Nya regler om cybersäkerhet

Delbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven

Stockholm 2024

STATENS OFFENTLIGA UTREDNINGAR

SOU 2024:18

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2024

ISBN 978-91-525-0878-7 (tryck)
ISBN 978-91-525-0879-4 (pdf)
ISSN 0375-250X

Till statsrådet Carl-Oskar Bohlin

Regeringen beslutade den 23 februari 2023 att tillkalla en särskild utredare med uppgift att föreslå de anpassningar av svensk rätt som är nödvändiga för att EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) och EU:s direktiv om kritiska entiteters motståndskraft (CER-direktivet) ska kunna genomföras. Uppdraget skulle redovisas ett år senare.

Som särskild utredare förordnades dagen efter juristen Annette Norman.

Anställda som sekreterare i utredningen har varit strategen Andreas Häll från den 27 februari 2023, hovrättsassessorn Nina Nordengren mellan den 15 mars och 30 juni 2023 och därefter som huvudsekreterare, samt seniore analytikern Love de Besche från den 1 september 2023.

Som sakkunniga förordnades den 14 april 2023 rättssakkunniga Lisa Wilander, Försvarsdepartementet, departementssekreteraren Tommy Forsell, Försvarsdepartementet, rättssakkunniga Mathilda Klang, Justitiedepartementet, kanslirådet Anna Stenberg, Finansdepartementet, numera kanslirådet Shafagh Elhami, Finansdepartementet och departementssekreteraren Marina Fransson, Landsbygds- och infrastrukturdepartementet. Shafagh Elhami entledigades den 6 september 2023 och ersattes samma dag av departementssekreteraren Agata Uhlhorn, Finansdepartementet.

Som experter förordnades den 14 april 2023 verksamhetsstrategen Helena Andersson, Myndigheten för samhällsskydd och beredskap (MSB), seniore it- och informationssäkerhetsspecialisten Magnus Bergström, Integritetsskyddsmyndigheten (IMY), handläggaren Martin Carlsson, Statens energimyndighet, professorn Mads Dam, Kungliga Tekniska högskolan (KTH), NIS-informationssäkerhetsinspektören Kristin Eriksson, Transportstyrelsen, seniore juristen Sebastian Fichtel, Finansinspektionen, ingenjören Anders Franzén,

Post- och telestyrelsen (PTS), beredskapshandläggaren Per Gustavsson, Livsmedelsverket, it-säkerhetschefen Lars Hjelm, Försäkringskassan, förbundsjuristen Magnus Ljung, Sveriges Kommuner och Regioner (SKR), juristen Emmelie Pettersén Uggla, Socialstyrelsen, gruppchefen Karin Stoffel, Polismyndigheten och verksjuristen Robert Tolonen Scherman, Säkerhetspolisen. Den 28 april 2023 förordnades handläggaren Linda Avad, Försvarsmakten och verksjuristen Fredrik Qvist, Bolagsverket som experter. Linda Avad entledigades den 18 september och analytikern Erik Hansen, Försvarsmakten, förordnades som expert samma dag. Mathilda Klang entledigades den 16 februari 2024.

Som ledamöter i en till utredningen knuten referensgrupp förordnades fr.o.m. den 14 april 2023 seniora juristen Sarah Berwick, Svenskt vatten, avdelningschefen Johan Billow, Försvarets materielverk (FMV), enhetschefen Cem Göcgören, Affärsverket svenska kraftnät, ansvarige för säkerhet och beredskap Emma Johansson, Energiföretagen, handläggaren inom rymdlägesbild Kristina Pålsson, Rymdstyrelsen, näringspolitiska experten Fredrik Sand, TechSverige, näringspolitiska experten Patrik Sandgren, Teknikföretagen, beredskapshandläggaren Fredrik Toreheim, Naturvårdsverket och juristen Åsa Wiklund Fredström, Kemikalieinspektionen. Fredrik Toreheim entledigades den 21 september 2023 och säkerhetsspecialisten Line Zandén förordnades att ingå i referensgruppen samma dag. Cem Göcgören entledigades den 23 oktober 2023 och säkerhetsskyddsspecialisten Elin Devonport Wretman, Affärsverket svenska kraftnät, förordnades att ingå i referensgruppen samma dag. Fredrik Sand entledigades den 22 januari 2024 från uppdraget att ingå i referensgruppen och förordnades att vara expert i utredningen samma dag.

Förordnandet för experterna är personligt. Likväl hänvisar utredningen till expertens myndighet eller motsvarande när det gäller redovisade synpunkter. Experterna och de sakkunniga har i allt väsentligt ställt sig bakom utredningens överväganden och förslag. De särskilda ståndpunkter som enskilda experter och sakkunniga kan ha haft i olika frågor har berörts i texterna eller som möjliga alternativa bedömningar.

Genom tilläggsdirektiv den 11 januari 2024 förlängdes utredningstiden för den del av uppdraget som avser anpassningar med anledning av CER-direktivet (dir. 2024:3).

Utredningen överlämnar härmed delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18). Uppdragets första del är med detta slutfört, men arbetet fortsätter.

Stockholm i mars 2024

Annette Norman

/ Nina Nordengren
Andreas Häll
Love de Besche

Innehåll

Sammanfattning **15**

Summary **23**

1 Författningsförslag **33**

1.1 Förslag till lag om cybersäkerhet 33

1.2 Förslag till lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet 50

1.3 Förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation 52

1.4 Förslag till förordning om cybersäkerhet 56

1.5 Förslag till förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen 66

1.6 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641) 68

1.7 Förslag till förordning om ändring i förordningen (2022:511) om elektronisk kommunikation 69

2 Utredningens uppdrag och arbete **71**

2.1 Analys av regeringens direktiv 71

2.1.1 Bakgrund 71

2.1.2 Utredningens övergripande utgångspunkt 72

2.1.3 Särskilt om NIS2-direktivet 72

2.1.4 Förhållandet till säkerhetsskyddsregleringen 75

2.1.5 Förhållandet till annan unionsrättslig och nationell regering 77

2.1.6 Utanför uppdraget ... 77
2.1.7 Konsekvensanalys ... 77

2.2 Utredningens arbete ... 78

2.3 Betänkandets disposition ... 78

3 NIS2-direktivet ... 81

3.1 NIS-direktivet ... 81
3.1.1 Gällande rätt ... 82
3.1.2 Gällande myndighetsstruktur och samarbete ... 85

3.2 NIS2-direktivet ... 86
3.2.1 Bakgrund och syfte ... 86
3.2.2 Tillämpningsområde och förteckning ... 87
3.2.3 Behöriga myndigheter och gemensamma kontaktpunkter ... 91
3.2.4 Cyberkrishanteringsmyndighet ... 92
3.2.5 CSIRT-enheter ... 92
3.2.6 Samarbete på nationell nivå ... 93
3.2.7 Samarbetsgrupp för strategiskt samarbete och informationsutbyte ... 93
3.2.8 CSIRT-nätverk ... 93
3.2.9 Det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) ... 94
3.2.10 Styrning ... 94
3.2.11 Riskhanteringsåtgärder för cybersäkerhet ... 94
3.2.12 Rapporteringsskyldigheter ... 96
3.2.13 Cybersäkerhetscertifiering och standardisering ... 98
3.2.14 Arrangemang för informationsutbyte om cybersäkerhet ... 98
3.2.15 Tillsyn och efterlevnadskontroll ... 99

4 Beskrivning av de nya sektorerna ... 103

4.1 Inledning ... 103

4.2 Energi ... 104

4.3 Hälso- och sjukvårdssektorn ... 106

4.4 Avloppsvatten ... 107
4.5 Digital infrastruktur ... 108
4.6 Förvaltning av IKT-tjänster (mellan företag) ... 110
4.7 Offentlig förvaltning ... 110
4.8 Rymden ... 111
4.9 Post- och budtjänster ... 112
4.10 Avfallshantering ... 112
4.11 Tillverkning, produktion och distribution av kemikalier ... 112
4.12 Produktion, bearbetning och distribution av livsmedel ... 113
4.13 Tillverkning ... 114
4.14 Digitala leverantörer ... 116
4.15 Forskning ... 117

5 Cybersäkerhetslagens tillämpningsområde ... 119

5.1 Direktivet ska i huvudsak genomföras genom ny NIS-lag ... 119
5.1.1 NIS-lagen ... 119
5.1.2 Ett vidare syfte ... 120

5.2 Direktivets tillämpningsområde ... 123
5.2.1 Utgångspunkter ... 123
5.2.2 Verksamhetsutövare ... 123
5.2.3 Högkritiska sektorer ... 126
5.2.4 Offentlig förvaltning enligt direktivet ... 127
5.2.5 Sveriges organisation – offentlig förvaltning ... 127
5.2.6 Utredningens analys ... 129
5.2.7 Andra kritiska sektorer ... 131
5.2.8 Storlekskravet ... 131
5.2.9 Myndigheter och regioner ... 133
5.2.10 Kommuner ... 134
5.2.11 Alternativt förslag ... 136
5.2.12 Enskilda verksamhetsutövare ... 138

5.2.13 Övriga särskilda kvalificeringsgrunder för enskilda verksamhetsutövare ... 140
5.2.14 Utbildningsinstitut ... 144

5.3 Jurisdiktion ... 146
5.3.1 Jurisdiktion för offentliga verksamhetsutövare ... 147
5.3.2 Jurisdiktion för enskilda verksamhetsutövare ... 147

5.4 Undantag för sektorsspecifika unionsrättsakter och andra författningar ... 150

5.5 Undantag för Sveriges säkerhet och brottsbekämpning ... 154
5.5.1 Bestämmelserna i direktivet ... 154
5.5.2 Säkerhetsskyddslagen ... 155
5.5.3 Undantag för säkerhetsskyddsklassificerade uppgifter ... 156
5.5.4 Undantag för offentliga verksamhetsutövare ... 157
5.5.5 Undantag för enskilda verksamhetsutövare ... 166

6 Klassificering och registrering ... 171

6.1 Väsentlig eller viktig ... 171

6.2 Register över väsentliga och viktiga verksamhetsutövare ... 177
6.2.1 Särskilt register över gränsöverskridande verksamhetsutövare ... 180

6.3 Domännamnsregistreringsuppgifter ... 182

7 Riskhantering och incidentrapportering ... 189

7.1 Övergripande lagreglering om riskhanteringsåtgärder ... 189
7.1.1 Övergripande om begrepp ... 191
7.1.2 Riskhanteringsåtgärder ... 192
7.1.3 Systematiskt informationssäkerhetsarbete ... 195

7.2 Ansvar och utbildning – riskhanteringsåtgärder ... 197

7.3 Incidentrapportering ... 198

7.4 Certifiering ... 203

8 Tillsyn 205

8.1 Inledning 205

8.2 Generella utgångspunkter för reglering om tillsyn 206

8.3 Tillsyn enligt NIS-direktivet 207
8.3.1 Utredningens enkät om tillsyn 207
8.3.2 Samarbetsforum 209
8.3.3 Utredningens slutsatser gällande nuvarande system för tillsyn 209

8.4 Utredningens överväganden och förslag 212
8.4.1 System för tillsyn 212
8.4.2 Tillsynsmyndigheter i Sverige 214
8.4.3 Tillsynsmyndighetens uppdrag 225
8.4.4 Tillsyn över viktiga verksamhetsutövare 226
8.4.5 Föreskrifter 226
8.4.6 Tillsynsmyndighetens undersökningsbefogenheter 233
8.4.7 Samordning och informationsutbyte 240

9 Ingripanden och sanktioner 249

9.1 Inledning 249
9.1.1 Bakgrund 249
9.1.2 Sammanfattning av utredningens förslag i denna del 249

9.2 Administrativa sanktioner eller straffrättsliga påföljder? ... 251

9.3 Vilka överträdelser kan läggas till grund för sanktioner? ... 252
9.3.1 Tillsynsmyndigheten ska kunna avstå från att ingripa i särskilda fall 253

9.4 Gemensamma bestämmelser för sanktionerna 254
9.4.1 Val av sanktion och generella krav på sanktionernas utformning 254
9.4.2 Vad ska beaktas särskilt vid val av sanktion och utformningen av dem? 255

9.5 Vilka administrativa sanktioner och andra möjligheter till ingripande ska finnas? ... 264
9.5.1 Föreläggande som kan förenas med vite ... 264
9.5.2 Informera användare om betydande cyberhot ... 265
9.5.3 Offentliggörande av överträdelser av direktivet ... 266
9.5.4 Utse övervakningsansvarig hos tillsynsmyndigheten ... 267
9.5.5 Tillfälligt upphävande av auktorisation eller certifiering ... 267
9.5.6 Förbud att utöva ledningsfunktion ... 272
9.5.7 Anmärkning ... 284

9.6 Sanktionsavgifter ... 285
9.6.1 För vilka överträdelser ska sanktionsavgifter införas och när får sanktionsavgift tas ut? ... 285
9.6.2 Sanktionsavgiftens storlek ska förändras ... 287
9.6.3 Hinder mot att ta ut sanktionsavgift ... 290
9.6.4 Betalning, verkställighet och preskription ... 291

9.7 Omedelbar verkställighet av förelägganden ... 292

9.8 Överklagande ... 293

10 Gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet ... 295

10.1 Gemensam kontaktpunkt ... 295
10.1.1 Inledning ... 295
10.1.2 Gemensam kontaktpunkt i Sverige ... 295
10.1.3 Den gemensamma kontaktpunktens uppgifter ... 296

10.2 Enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet) ... 299
10.2.1 Inledning ... 299
10.2.2 CSIRT-enhet i Sverige ... 299
10.2.3 CSIRT-enhetens uppgifter ... 300

10.3 Cyberkrishanteringsmyndighet ... 311
10.3.1 Inledning ... 311
10.3.2 Cyberkrishanteringsmyndighet i Sverige ... 311
10.3.3 Cyberkrishanteringsmyndighetens uppgifter ... 313

11 NIS2-direktivet och LEK 315

11.1 Inledning 315

11.2 Bestämmelserna i LEK, kodexen och NIS2 315
11.2.1 Allmänt 315
11.2.2 Kretsen som ska tillämpa kraven 316
11.2.3 Riskhanteringsåtgärder 316
11.2.4 Ramen för vad riskhanteringsåtgärderna kan avse 319
11.2.5 Säkerhetsrevision 320
11.2.6 Incidentbegreppet 321
11.2.7 Kravet på incidentrapportering 323
11.2.8 Informera allmänheten om incidenter 324
11.2.9 Informera om betydande cyberhot 324
11.2.10 Ingripanden, sanktioner och vissa tillsynsåtgärder 325
11.2.11 Föreskriftsrätt 326

11.3 Slutsatser och följdförslag 326

12 Konsekvensanalys 329

12.1 Allmänt 329

12.2 Jämställdhet och de integrationspolitiska målen 331

12.3 Regleringsalternativ 331

12.4 Vem berörs av förslagen? 332

12.5 Skyldigheterna för dem som omfattas 333

12.6 Ekonomiska konsekvenser för tillsynsmyndigheterna och Myndigheten för samhällsskydd och beredskap samt finansiering 333
12.6.1 Tillsynsmyndigheternas uppgifter 334
12.6.2 Uppgifter för Myndigheten för samhällsskydd och beredskap 336
12.6.3 Utgångspunkter och bedömning för Finansinspektionen 340
12.6.4 Ekonomiska konsekvenser för Bolagsverket och finansiering 342

12.6.5 Övriga tillsynsmyndigheter och Myndigheten för samhällsskydd och beredskap – bakgrund 342
12.6.6 Swecos uppdrag och rapport 347
12.6.7 Utredningens förslag – ekonomiska konsekvenser för tillsynsmyndigheterna och för Myndigheten för samhällsskydd och beredskap 351

12.7 Ekonomiska konsekvenser för offentliga verksamhetsutövare 356

12.8 Ekonomiska konsekvenser för enskilda verksamhetsutövare 357

12.9 Förslagens konsekvenser för det kommunala självstyret .. 358

13 Ikraftträdande med mera 361

13.1 Cybersäkerhetsregleringen 361

13.2 Följdändringar i annan författning 363
13.2.1 Hänvisningar i författning 363
13.2.2 Bestämmelser som upphävs eller ändras 363

14 Författningskommentar 365

14.1 Förslaget till lag om cybersäkerhet 365

14.2 Förslaget till lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet 391

14.3 Förslaget till lag om ändring i lagen (2022:482) om elektronisk kommunikation 394

Bilagor

Bilaga 1 Kommittédirektiv 2023:30 395

Bilaga 2 Kommittédirektiv 2024:3 419

Bilaga 3 NIS2-direktivet 421

Bilaga 4 Swecos rapport 495

Bilaga 5 Jämförelsetabell 517

Sammanfattning

Direktivet

Europaparlamentet och rådet antog den 14 december 2022 två nya EU-direktiv, NIS2-direktivet, se bilaga 3 och CER-direktivet. Utredningen redovisar i detta delbetänkande förslag om införlivning av NIS2-direktivet och kommer att i sitt slutbetänkande i september 2024 att lämna förslag om införlivning av CER-direktivet.

NIS2-direktivet ställer krav på säkerhet i nätverks- och informationssystem. Det ersätter det tidigare NIS-direktivet från 2016, som genomfördes i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Utredningen föreslår att NIS2-direktivet i huvudsak införlivas genom en ny lag, cybersäkerhetslagen och att den tidigare lagen upphävs.

NIS2-direktivet skärper kraven jämfört med det tidigare direktivet för verksamhetsutövare och innehåller bestämmelser om ett mer långtgående samarbete inom unionen. Syftet är att uppnå en högre cybersäkerhet. Det är ett minimidirektiv med innebörd att den svenska lagstiftningen skulle kunna innehålla längre gående skyldigheter. Utredningen föreslår med något undantag inte några skyldigheter utöver vad som följer av direktivet.

Vem omfattas av cybersäkerhetsregleringen?

Det finns två viktiga skillnader mellan gällande lagstiftning och förslaget till cybersäkerhetsreglering. Den första är att cybersäkerhetslagen föreslås omfatta betydligt fler aktörer, eftersom antalet sektorer utökas från sju till 18. Den andra viktiga skillnaden är att kraven kommer att gälla för hela verksamheten inte bara för samhällsviktiga och digitala tjänster.

De sektorer som kommer att omfattas är:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvårdssektorn
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av IKT-tjänster (mellan företag)
- Offentlig förvaltning
- Rymden
- Post- och budtjänster
- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning
- Digitala leverantörer
- Forskning

Innebörden är att den som bedriver verksamhet inom någon av sektorerna som utgångspunkt omfattas av kraven i cybersäkerhetsregleringen. Det gäller för såväl offentliga som enskilda verksamhetsutövare.

Som framgår av uppräkningen av sektorer är offentlig förvaltning en egen sektor. Det får till följd att nästan hela den offentliga sektorn omfattas av lagens krav. Utredningen föreslår att cybersäkerhetslagen ska gälla för de flesta statliga myndigheter i Sverige. De som är undantagna är regeringen, Regeringskansliet, myndigheter som lyder under Riksdagen, och domstolar. Detsamma gäller för sammanlagt

16 myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning.

Vidare omfattas samtliga regioner och kommuner av lagens krav. Undantag gäller enbart för region- eller kommunfullmäktige. Utredningen föreslår också att lärosäten med examenstillstånd ska omfattas av regleringen.

För enskilda verksamhetsutövare gäller som huvudregel ett storlekskrav med innebörd att verksamheten måste sysselsätta minst 50 personer eller ha en årsomsättning som överstiger 10 miljoner euro för att omfattas av lagen. Det betyder att små företag som utgångspunkt inte kommer att beröras. Vissa särskilt utpekade enskilda verksamhetsutövare omfattas dock oavsett storlek. Myndigheten för samhällsskydd och beredskap (MSB) kommer också att ha möjlighet att peka ut vissa särskilt kritiska mindre verksamheter. Enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet, brottsbekämpning eller erbjuder tjänster till myndigheter som gör det, är undantagna.

Därutöver kommer lagen att gälla i begränsad utsträckning för offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpning, men där den delen inte utgör en väsentlig andel. Motsvarande kommer att gälla för enskilda verksamhetsutövare som bedriver annan verksamhet tillsammans med säkerhetskänslig verksamhet eller brottsbekämpning. För den säkerhetskänsliga delen av verksamheten eller den delen av verksamheten som avser brottsbekämpning kommer det endast att gälla en anmälnings- och uppgiftsskyldighet. Detsamma gäller för verksamheter som redan omfattas av skyldigheter med motsvarande verkan som kraven i cybersäkerhetslagen. Så kommer vara fallet för exempelvis finansiella verksamhetsutövare som omfattas av Dora-förordningen.

Kraven i direktivet

Den nya regleringen ställer krav på verksamhetsutövarna. En verksamhetsutövare som omfattas av lagen ska anmäla sig till sin tillsynsmyndighet och lämna uppgifter om bland annat identitet, kontaktuppgift och verksamhet.

Därutöver ska verksamhetsutövare vidta riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från en riskanalys, vara proportionella i förhållande till risken och de ska utvärderas. Det ställs också krav på att verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete samt krav på att verksamhetens ledning ska genomgå utbildning och att anställda ska erbjudas utbildning.

Slutligen gäller en skyldighet för verksamhetsutövare att rapportera betydande incidenter till MSB i egenskap av CSIRT-enhet (se nedan) inom bestämda tidsgränser. Det betyder att en varning ska lämnas inom 24 timmar efter det att verksamhetsutövaren fått kännedom om den betydande incidenten. Vidare ska en incidentanmälan göras inom 72 timmar och en slutrapport inom en månad.

De uppgifter verksamhetsutövarna lämnar till sin tillsynsmyndighet ovan ska myndigheten använda för att klassificera verksamhetsutövarna som väsentliga eller viktiga och registrera dem.

Det ska också finnas ett särskilt register för gränsöverskridande verksamhetsutövare. Registret ska sedan vidarebefordras till MSB i egenskap av gemensam kontaktpunkt (se nedan) som i sin tur ska informera kommissionen.

Tillsyn

I kommittédirektivet anges att systemet för tillsyn bör utgå från den struktur som finns enligt dagens regelverk. Enligt den nu gällande NIS-lagen finns det för varje sektor och för de digitala tjänster som omfattas av lagen en utpekad tillsynsmyndighet som utövar tillsyn över att regelverket följs. Utredningen föreslår att det även fortsatt ska finnas en tillsynsmyndighet för varje sektor. I de sektorer som är oförändrade i förhållande till det första NIS-direktivet är utredningens förslag att befintliga tillsynsmyndigheter fortsätter att ansvara för dessa. Den kompetens som finns hos befintliga tillsynsmyndigheter bör så långt möjligt även nyttjas för de nya sektorer som omfattas av reglering. Flera tillsynsmyndigheter föreslås därför få utökade ansvarsområden. Utredningen föreslår också fem nya tillsynsmyndigheter. Dessa är länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län samt Läkemedelsverket.

Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som meddelats i anslutning till lagen följs. Tillsynsåtgärder för viktiga verksamhetsutövare får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att regleringen inte följs.

Verksamhetsutövarna ska tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen. Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten. Tillsynsmyndigheten får också låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av cybersäkerhetslagen.

MSB ska även fortsättningsvis leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet

För att säkerställa gränsöverskridande samarbete ska varje medlemsstat utse en gemensam kontaktpunkt. Den gemensamma kontaktpunkten ska utöva en sambandsfunktion och bland annat lämna sammanfattande rapporter om betydande incidenter, cyberhot och tillbud till Enisa samt underrätta kommissionen och samarbetsgruppen om antalet verksamhetsutövare i Sverige.

Mot bakgrund av att MSB i dag fullgör de uppgifter som följer av att vara gemensam kontaktpunkt samt myndighetens uppgift att stödja och samordna arbetet med samhällets informationssäkerhet anser utredningen att MSB även fortsatt ska vara gemensam kontaktpunkt i Sverige.

Varje medlemsstat ska också utse eller inrätta en eller flera CSIRT-enheter (Computer Security Incident Response Team). CSIRT-enheten ska bland annat övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå och tillhandahålla varningar och information. Vidare ska varje medlemsstat utse eller inrätta en eller flera myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter).

Mot bakgrund av de uppdrag MSB har i dag och den kompetens som finns inom myndigheten bedömer utredningen att MSB även fortsatt ska vara CSIRT-enhet samt vara cyberkrishanteringsmyndighet i Sverige.

Varje medlemsstat ska anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Planen ska bland annat innehålla cyberkrishanteringsmyndighetens uppgifter och ansvarsområden. Utformningen av den nationella planen ingår inte i utredningens uppdrag.

Ingripanden och sanktioner

Nuvarande ingripanden och sanktioner

Enligt NIS-lagen får en tillsynsmyndighet ingripa mot överträdelser av vissa skyldigheter i lagen. Tillsynsmyndighetens möjligheter att ingripa beror på vilken skyldighet som har överträtts, men består av förelägganden som kan förenas med vite, eller sanktionsavgifter. Sanktionsavgifterna ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor. Tillsynsmyndigheten ska ta särskild hänsyn till vissa omständigheter vid bestämmandet av sanktionsavgiftens storlek.

De nuvarande ingripandena och sanktionerna behålls och kompletteras

Tillsynsmyndighetens möjligheter att besluta om förelägganden (vid vite) och sanktionsavgifter behålls. Tillsynsmyndigheten ska även kunna förelägga en verksamhetsutövare att (1) offentliggöra information om överträdelser av lagens bestämmelser, och att (2) informera användare som kan påverkas av ett betydande cyberhot.

Vidare föreslås tillsynsmyndigheten få ansöka hos allmän förvaltningsdomstol om att en person med ledningsansvar hos en väsentlig verksamhetsutövare ska förbjudas att utöva ledningsfunktioner där. Det krävs särskilda omständigheter för att sådant förbud ska kunna meddelas.

Anmärkning införs som sanktion och ska alltid beslutas vid överträdelser om ingen annan sanktion har använts av tillsynsmyndigheten.

Sanktionsavgifternas maximinivå ska höjas

Lägstanivåerna för sanktionsavgifter behålls på 5 000 kronor. Högstanivåerna höjs väsentligt i jämförelse med gällande nivåer och uppgår:

För väsentliga verksamhetsutövare till det högsta av:

1. Två procent av den väsentliga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 10 000 000 euro.

För viktiga verksamhetsutövare till det högsta av:

1. 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 7 000 000 euro.

För offentliga verksamhetsutövare till 10 000 000 kronor.

Tillsynsmyndigheten ska ingripa mot alla överträdelser och beakta fler omständigheter vid val och utformning av sanktioner

Utredningen föreslår att tillsynsmyndigheten ska ingripa mot alla överträdelser av lagen. Den ska i vissa särskilda fall ha möjlighet att avstå från att ingripa, till exempel för att inte bryta mot det s.k. dubbelprövningsförbudet.

Om tillsynsmyndigheten inte avstår från att ingripa ska den åtminstone meddela en anmärkning. Om den ingriper med någon annan sanktion behöver den inte meddela anmärkning.

När tillsynsmyndigheten ingriper ska den alltid beakta alla relevanta omständigheter, men fler omständigheter görs obligatoriska att beakta än vad som tidigare gällt.

Ekonomiska konsekvenser

Utredningens förslag medför ekonomiska konsekvenser för tillsynsmyndigheterna, MSB och verksamhetsutövarna. För tillsynsmyndigheterna handlar det om att betydligt fler verksamhetsutövare kommer att omfattas av lagen. Tillsynsmyndigheterna är enligt utredningens

förslag elva. Sex av dem bedriver redan tillsyn enligt gällande lagstiftning, men fem myndigheter är som framgår ovan nya. Utredningen har som underlag för konsekvensanalysen inhämtat en rapport från Sweco Aktiebolag, som intervjuat de föreslagna tillsynsmyndigheterna och MSB. Av rapporten följer att det varit förenat med svårigheter för myndigheterna att uppskatta de framtida kostnaderna.

Utredningen föreslår att de tillsynsmyndigheter som redan bedriver tillsyn med undantag av Finansinspektionen får ett förstärkt anslag med två miljoner kronor vardera för 2025 avseende löpande kostnader. Skälet är att tillsynsmyndigheterna bör ha utökade resurser för att kunna identifiera vilka verksamhetsutövare som omfattas av den nya lagen, utfärda nya föreskrifter och nya vägledningar utan att samtidigt behöva minska ambitionen med tillsyn. Även MSB bör tillföras motsvarande belopp. De myndigheter som inte redan har tillsynsuppdrag bör få ett förstärkt anslag med fem miljoner kronor vardera för 2025 för att bygga upp tillsynsverksamheten.

Samtidigt föreslår utredningen att regeringen ger Statskontoret i uppdrag att vidare utreda de ekonomiska konsekvenserna för tillsynsmyndigheterna och MSB samt att det för de första åren införs ett återrapporteringskrav för myndigheterna.

För de offentliga verksamhetsutövarna föreslår utredningen att kostnaderna ska finansieras inom befintlig ram. Skälen är att det är rimligt att offentliga verksamhetsutövare vidtar grundläggande säkerhetsåtgärder. Genom förslagen erhåller verksamhetsutövarna också stöd. Vidare kan åtgärder för att förebygga incidenter medföra besparingar.

Förslagen medför även kostnader för enskilda verksamhetsutövare, men även dessa får stöd genom förslagen och det förebyggande arbetet kan medföra besparingar. Som framgått omfattas som huvudregel inte små företag. Kraven kommer att gälla inom hela unionen. Utredningen bedömer därför att regleringen inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

Ikraftträdande

Utredningen föreslår att förslagen ska träda i kraft den 1 januari 2025.

Summary

Terms of reference

On 14 December 2022, the European Parliament and the Council adopted two new EU Directives: the Directive on measures for a high common level of cybersecurity across the Union (NIS 2) – see Annex 3 – and the Critical Entities Resilience Directive (CER). The Inquiry has outlined the proposals on incorporating the NIS 2 Directive in this interim report and will present proposals on incorporating the CER Directive in its final report in September 2024.

The NIS 2 Directive sets out requirements on network and information systems (NIS) security. It replaces the previous NIS Directive of 2016, which was implemented in Swedish law through the Act on information security for essential and digital services (2018:1174) (NIS Act). The Inquiry proposes implementing the NIS 2 Directive primarily through a new cyber security act that would replace the existing Act.

The NIS 2 Directive sets out stricter requirements on operators than those in the previous directive, and contains provisions on farther-reaching cooperation within the Union. The aim is to achieve a higher level of cybersecurity. This is a minimum directive, which means that Swedish legislation could contain more extensive obligations. With a few exceptions, the Inquiry does not propose any obligations beyond those set out in the Directive.

Who would be covered by the proposed regulation of cybersecurity?

There are two important differences between the current legislation and the proposed regulation of cybersecurity. Firstly, it is proposed that the cybersecurity act cover significantly more actors, as the number of sectors would be expanded from 7 to 18. Secondly, the requirements would apply to their entire operations rather than only essential and digital services.

The following sectors should be covered:

- energy
- transport
- banking
- financial market infrastructures
- health
- drinking water
- wastewater
- digital infrastructure
- Information and communication technology (ICT) service management (business to business)
- public administration
- space
- postal and courier services
- waste management
- chemicals
- food
- manufacturing
- digital services
- research

Under the proposed regulation of cybersecurity, operators carrying out activities in any of these sectors would be subject to the new requirements. This applies to both public and private operators.

As indicated by the list above, public administration would be considered its own sector. Consequently, almost the entire public sector would be subject to the act's requirements. The Inquiry proposes that the cybersecurity act apply to most central government agencies in Sweden. The Government, the Government Offices, government agencies under the Riksdag and the courts would be exempted. The same would apply for the 16 government agencies that primarily carry out security-sensitive activities or law enforcement.

All regions and municipalities would also be subject to the act's requirements. The only exceptions would be regional or municipal councils. The Inquiry further proposes that regulation of cybersecurity cover higher education institutions authorised to award degrees.

As regards private operators, the act's requirements would, as a general rule, apply only to operations that employ at least 50 people or have a minimum annual turnover of EUR 10 million. This means that most small enterprises would not be affected. However, certain specifically identified individual operators would be covered by the act regardless of size. In addition, the Swedish Civil Contingencies Agency would be empowered to identify certain especially critical smaller activities. Individual operators that strictly carry out security-sensitive activities or law enforcement, or offer services to government agencies that do so, would be exempted.

The act would also apply to a limited extent to public sector operators that carry out security-sensitive activities or law enforcement, but only if that part of their activities is not a substantial share of their overall operations. The same would apply to individual operators that carry out other activities together with security-sensitive activities or law enforcement. For the security-sensitive part of the activities or the part concerning law enforcement, only an incident reporting and notification obligation would apply. The same would apply to activities already subject to obligations that have an effect equivalent to that of the requirements of the cybersecurity act. For example, this would be the case for financial operators covered by the Regulation on digital operational resilience for the financial sector.

Requirements in the Directive

The proposed regulation of cybersecurity would set out requirements on operators. An operator covered by the act would have to register with their supervisory authority and provide information including their identity, contact details and activities.

The operator would also have to take risk management measures to protect network and information systems and their physical environments against incidents. These measures would be based on a risk analysis, be proportional to the risk and be subject to evaluation. The operator would also be required to carry out systematic, risk-based information security work, require its management to undergo training and offer training to employees.

Finally, operators would be obliged to report significant incidents to the Swedish Civil Contingencies Agency in its capacity as Computer Security Incident Response Team (CSIRT) (see below) within a specified timeframe. This means that an operator would have to report a warning to the CSIRT within 24 hours of having become aware of a significant incident. Moreover, an incident report would have to be submitted within 72 hours, and a final report within one month.

The information that the operators would be required to submit to their supervisory authority as specified above would be used by the authority to classify the operators as essential or important, and register them. There would also be a separate register for cross-border operators. This register would then be forwarded to the Swedish Civil Contingencies Agency in its capacity as the single point of contact (see below), which would in turn notify the European Commission.

Supervision

The committee terms of reference stipulate that the system for supervision should be based on the existing structure under the current regulatory framework. Under the currently applicable NIS Act, a specific supervisory authority responsible for each sector and for the digital services covered by the Act carries out supervision to ensure compliance with the regulatory framework. The Inquiry proposes that a supervisory authority continue to have responsibility for each

sector. In those sectors where the requirements would remain unchanged in relation to the first NIS Directive, the Inquiry proposes that the currently responsible supervisory authorities continue to have responsibility. The expertise in the current supervisory authorities should be utilised as far as possible for supervision of the additional sectors that would be covered by the proposed regulation. It is therefore proposed that several supervisory authorities gain expanded areas of responsibility. The Inquiry further proposes establishing five new supervisory authorities: the county administrative boards of Stockholm, Skåne, Västra Götaland and Norrbotten, and the Medical Products Agency.

Supervisory authorities should be tasked with carrying out supervision to ensure compliance with the cybersecurity act and regulations announced in connection with it. Supervisory measures against important operators would only be taken if a supervisory authority had reason to believe that the regulation was being not followed.

The operators would have to provide supervisory authorities with the information needed for supervision. If there are special grounds for doing so, a supervisory authority would be empowered to require an operator to arrange and pay for an independent body to conduct a targeted security audit and present the results to the supervisory authority. The supervisory authority would also be empowered to carry out security scans on the premises of operators covered by the cybersecurity act.

The Swedish Civil Contingencies Agency would continue to lead a cooperation forum of supervisory authorities. The purpose of the forum is to facilitate coordination and achieve effective and equivalent supervision.

Single point of contact, CSIRT and cyber crisis management authority

To ensure cross-border cooperation, each Member State must appoint a single point of contact. It is the task of the single point of contact to exercise a liaison function and submit summary reports on significant incidents, cyber threats and near misses to the European Network and Information Security Agency, and notify the Commis-

sion and the Cooperation Group of the number of operators in Sweden.

As it is currently the Swedish Civil Contingencies Agency's mandate to carry out the tasks associated with serving as a single point of contact and to support and coordinate work on society's information security, the Inquiry proposes that the Agency continue to serve as the single point of contact in Sweden.

Each Member State must also designate or establish one or multiple CSIRTs. A CSIRT's mandate includes monitoring and analysing cyber threats, vulnerabilities and incidents at national level, issuing warnings and providing information. Each Member State must also designate or establish one or more authorities with responsibility for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities).

In consideration of the Swedish Civil Contingencies Agency's current mandate and expertise, the Inquiry proposes that the Agency remain the CSIRT and serve as the cyber crisis management authority in Sweden.

Each Member State must adopt a large-scale national cybersecurity incident and crisis response plan. The plan must outline the tasks and responsibilities of the cyber crisis management authority. The formulation of this national plan is not part of the Inquiry's remit.

Enforcement measures and penalties

Current enforcement measures and penalties

According to the NIS Act, a supervisory authority may intervene against infringements of certain obligations under the Act. Depending on which obligation has been violated, a supervisory authority's enforcement measures consist of issuing orders – possibly in combination with a financial penalty – or administrative fines. The administrative fines should be set at no less than SEK 5 000 and no more than SEK 10 000 000. A supervisory authority should give special consideration to certain circumstances when determining the amount of the administrative fine.

Current enforcement measures and penalties should be retained and supplemented

Supervisory authorities should retain the power to issue orders (as regards financial penalties) and administrative fines. They should also be able to order an operator to (1) announce information about infringements of the act's provisions and (2) inform individuals who are potentially affected by a significant cyber threat.

The Inquiry also proposes empowering supervisory authorities to apply to a general administrative court to prohibit an individual at chief executive officer or legal representative level from exercising managerial functions at an essential operator. Special circumstances would be required to issue such a prohibition.

A reprimand should be introduced as a penalty and always be issued in connection with infringements unless another penalty has been issued by the supervisory authority.

The maximum amount of an administrative fine should be increased

The minimum level of administrative fines should remain at SEK 5 000. The maximum level should be increased substantially in comparison with current levels as follows:
for essential operators, a maximum of

1. 2 per cent of the essential operator's entire global turnover of the preceding fiscal year, or
2. EUR 10 000 000;

for important operators, a maximum of:

1. 1.4 per cent of the operator's entire global turnover of the preceding fiscal year, or
2. EUR 7 000 000; and

for public sector operators, SEK 10 000 000.

A supervisory authority should intervene against all infringements and take account of additional circumstances when determining penalties

The Inquiry proposes that supervisory authorities intervene against all infringements of the act. In certain cases, they should have the option to refrain from intervening, e.g. to avoid double jeopardy situations.

If a supervisory authority does not refrain from intervening, it should, at a minimum, issue a reprimand. If it issues some other penalty, it need not issue a reprimand.

When a supervisory authority intervenes, it should always consider all relevant circumstances. However, it should be obliged to consider more circumstances than is currently the case.

Financial impact

If adopted, the Inquiry's proposals would have a financial impact on the supervisory authorities, the Swedish Civil Contingencies Agency and the operators. This would be due to the new act covering significantly more operators. The Inquiry proposes designating 11 supervisory authorities. Six of these already carry out supervision under currently applicable legislation. The other five authorities mentioned above would be newly empowered. As a basis for its consequence analysis, the Inquiry has examined a report from Sweco Aktiebolag, which interviewed the proposed supervisory authorities and the Swedish Civil Contingencies Agency. The report indicates that it is difficult for those authorities to estimate the future costs.

The Inquiry proposes that the supervisory authorities that already carry out supervision, with the exception of the Swedish Financial Supervisory Authority, each receive an additional SEK 2 million in funding for 2025 to cover running costs. This would provide the supervisory authorities with additional resources, thus enabling them to identify which operators are covered by the new act and issue new regulations and new guidelines without simultaneously diminishing the efficacy of the supervision. The Swedish Civil Contingencies Agency should also be allocated an equivalent amount. The supervisory authorities that do not currently have a supervisory mandate

should each receive an additional SEK 5 million for 2025 to build their supervisory organisation.

At the same time, the Inquiry proposes that the Government instruct the Swedish Agency for Public Management to investigate the financial impact on the supervisory authorities and the Swedish Civil Contingencies Agency, and that the authorities be required to report the financial impact for the first few years.

For public sector operators, the Inquiry proposes financing the costs within existing frameworks. This is because it is reasonable to require public sector operators to take basic security measures. Through these proposals, the operators also receive support. Measures to prevent incidents also result in savings.

The proposals would also entail additional costs for individual operators, but they would also receive support through the proposals, and the preventive work could result in savings. As stated earlier, the act would not cover small enterprises in general. The new requirements will apply throughout the Union. The Inquiry has therefore concluded that the proposed regulation would not have a significant impact on businesses' working conditions, competitiveness or other conditions.

Entry into force

The Inquiry proposes that the proposals enter into force on 1 January 2025.

1 Författningsförslag

1.1 Förslag till lag om cybersäkerhet

Härigenom föreskrivs följande.

1 kap. Inledande bestämmelser

Lagens syfte

1 § Syftet med denna lag är att uppnå en hög cybersäkerhetsnivå.

Uttryck i lagen

2 § I lagen avses med

1. allmän dataskyddsförordning: Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG,

2. allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster: begreppen har samma innebörd som i lagen (2022:482) om elektronisk kommunikation,

3. betrodda tjänster: begreppet har samma innebörd som i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG,

4. betydande cyberhot: ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en verksamhetsutövares nätverks- och informationssystem eller

användarna av verksamhetsutövarens tjänster genom att vålla betydande materiell eller immateriell skada,

5. cyberhot: ett cyberhot enligt definitionen i artikel 2.8 i Cybersäkerhetsakten,

6. cybersäkerhet: cybersäkerhet enligt definitionen i artikel 2.1 i Cybersäkerhetsakten,

7. Cybersäkerhetsakten: Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013,

8. datacentraltjänst: en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll,

9. domännamnsregistreringstjänster: registrar eller en annan verksamhetsutövare som verkar som ombud eller återförsäljare av domännamn,

10. domännamnssystem (DNS): ett hierarkiskt distribuerat namnsystem som möjliggör identifieringen av tjänster och resurser på internet,

11. domännamnssystemtjänster (DNS-tjänster): allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare, eller auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar,

12. Dora-förordning: Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011,

13. EES: Europeiska ekonomiska samarbetsområdet,

14. enskilda verksamhetsutövare: fysiska och juridiska personer som inte är en myndighet, region eller en kommun och som bedriver verksamhet,

15. forskningsorganisation: en verksamhetsutövare vars främsta mål är att bedriva tillämpad forskning i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner,

16. hanterade säkerhetstjänster: en verksamhet som utför eller tillhandahåller stöd för annan verksamhet gällande hantering av tjänster som hanterar cybersäkerhetsrisker,

17. hanterade tjänster: en verksamhet som erbjuder tjänster som rör installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans,

18. IKT-produkt, IKT-tjänst och IKT-process: enligt begreppens definitioner i artiklarna 2.12, 2.13 och 2.14 i Cybersäkerhetsakten,

19. incident: en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom nätverks- och informationssystem,

20. kommissionens rekommendation 2003/361/EG: bilagan till kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag,

21. kvalificerade tillhandahållare av betrodda tjänster: begreppet har samma innebörd som i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG,

22. marknadsplatser online: en marknadsplats online enligt definitionen i artikel 2 n i Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder),

23. molntjänst: en digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma beräkningstjänster, inbegripet när sådana resurser är distribuerade på flera platser,

24. NIS2-direktivet: Europaparlamentets och rådets direktiv av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148,

25. nätverk för leverans av innehåll: ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning.

26. nätverks- och informationssystem:

1. ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen (2022:482) om elektronisk kommunikation,

2. en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller

3. digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av 1 och 2 för att de ska kunna driftas, användas, skyddas och underhållas,

27. partnerföretag och anknutna företag: begreppen har samma innebörd som i artikel 3 i rekommendation 2003/361/EG,

28. plattformar för sociala nätverkstjänster: en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, särskilt genom chattar, inlägg, videor och rekommendationer.

29. registreringsenhet för toppdomäner: en verksamhet som har delegerats en specifik toppdomän och som ansvarar för att administrera, förvalta, sköta teknisk drift samt registrering av domännamn under en specifik toppdomän, dock inte om toppdomänen endast avses för eget bruk,

30. risk: risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att en sådan incident inträffar,

31. sökmotor: en sökmotor enligt definitionen i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av online baserade förmedlingstjänster,

32. tillbud: en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod,

33. verksamhetsutövare: juridisk eller fysisk person som bedriver verksamhet. Samlingsterm i denna lag för bland annat leverantör, producent, vårdgivare, leverantör eller tillhandahållare.

Lagens tillämpningsområde

Offentliga verksamhetsutövare

3 § Denna lag gäller för

1. statliga myndigheter i Sverige med undantag för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och Sveriges domstolar,
2. regioner i Sverige med undantag för regionfullmäktige, och
3. kommuner i Sverige med undantag för kommunfullmäktige.

Enskilda verksamhetsutövare

4 § Denna lag gäller för enskilda verksamhetsutövare om

1. verksamheten omfattas av bilaga 1 eller 2 i NIS2-direktivet eller är ett lärosäte med examenstillstånd,
2. inte annat följer av 5 och 6 §§, verksamheten är etablerad i Sverige, och
3. inte annat följer av 7 och 8 §§, verksamheten uppfyller kraven för medelstort företag enligt artikel 2 och 3.1–3.3 i bilagan till kommissionens rekommendation 2003/361/EG.

Regeringen eller den myndighet regeringen bestämmer får i föreskrifter meddela undantag för 3 avseende partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet.

5 § Verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster behöver inte vara etablerade i Sverige för att omfattas av lagen utan det är tillräckligt att verksamhetsutövaren erbjuder tjänster i Sverige.

6 § Gränsöverskridande verksamhetsutövare är verksamhetsutövare som erbjuder:

1. DNS-tjänster,
2. registreringsenheter för toppdomäner,
3. domännamnsregistrering,
4. molntjänster,
5. datacentraltjänster,
6. nätverk för leverans av innehåll,
7. hanterade tjänster,
8. hanterade säkerhetstjänster, eller
9. marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster.

Gränsöverskridande verksamhetsutövare som erbjuder tjänster inom EES, men saknar etablering där ska utse en företrädare med etablering i något av de länder där tjänster erbjuds.

För gränsöverskridande verksamhetsutövare krävs det i stället för etablering att Sverige är huvudsakligt etableringsställe eller att företrädaren är etablerad i Sverige för att verksamhetsutövaren ska omfattas av lagen.

För gränsöverskridande verksamhetsutövare som erbjuder tjänster i Sverige, men inte utser en företrädare gäller kap. 5.

Regeringen får meddela föreskrifter om vad som utgör huvudsakligt etableringsställe.

7 § Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 och som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner, DNS-tjänster eller domännamnsregistrering omfattas av lagen.

8 § Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 omfattas också av lagen om,

1. verksamheten är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner,
2. en störning kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet, folkhälsa eller medföra betydande systemrisker särskilt om det får gränsöverskridande konsekvenser, eller

3. verksamheten är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av denna verksamhet.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter.

Undantag från lagens tillämpningsområde

Krav i andra författningar

9 § Om annan författning innehåller bestämmelser om krav på riskhanteringsåtgärder eller incidentrapportering för en verksamhetsutövare med motsvarande verkan gäller inte kraven i 3 kap. för verksamhetsutövaren.

Vid jämförelsen av verkan mellan författningarna ska hänsyn tas till bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till bestämmelserna.

Regeringen får i föreskrifter ange vilka andra bestämmelser om riskhanteringsåtgärder och incidentrapportering som har motsvarande verkan.

10 § Lagen ska inte tillämpas på verksamheter som undantagits enligt artikel 2.4 i Dora-förordningen.

Sveriges säkerhet eller brottsbekämpning

11 § Lagen gäller inte statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) eller brottsbekämpning.

Regeringen får i föreskrifter ange vilka statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning.

12 § För andra statliga myndigheter som utövar säkerhetskänslig verksamhet eller brottsbekämpning än de som avses i 11 § gäller inte kraven i 6 § andra och fjärde stycket samt kap. 3 för den del av verksamheten som är säkerhetskänslig eller utgör brottsbekämpning. För den övriga delen av verksamheten gäller lagen i dess helhet.

Vad som anförs i första stycket gäller även regioner och kommuner.

13 § Lagen gäller inte för enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet, brottsbekämpning eller som enbart erbjuder tjänster till statliga myndigheter som avses i 11 §.

Om en enskild verksamhetsutövare bedriver även annan verksamhet gäller för den säkerhetskänsliga verksamheten, brottsbekämpningen och verksamheten som avser tjänster till statliga myndigheter enligt 11 § inte kraven i 6 § andra och fjärde stycket samt kap. 3. För den övriga delen av verksamheten gäller lagen i dess helhet.

Vad som anförs ovan i andra stycket gäller inte om verksamhetsutövaren är en tillhandahållare av betrodda tjänster. För dessa verksamhetsutövare gäller lagen i dess helhet.

14 § Skyldighet att lämna uppgifter enligt denna lag gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585).

2 kap. Klassificering och registrering

1 § Följande verksamhetsutövare är väsentliga:

1. Statliga myndigheter,

2. verksamhetsutövare som bedriver verksamhet enligt bilaga 1 till NIS2-direktivet, är en kommun eller ett lärosäte med examenstillstånd och vars verksamhet överstiger trösklarna för medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,

3. verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och vars verksamhet är medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,

4. kvalificerade tillhandahållare av betrodda tjänster,

5. registreringsenheter för toppdomäner,
6. verksamhetsutövare som erbjuder DNS-tjänster och
7. verksamhetsutövare som anges i 1 kap. 8 § och identifierats som väsentliga enligt 33 § förordning om cybersäkerhet.

Verksamhetsutövare som inte är väsentliga är viktiga verksamhetsutövare.

2 § Verksamhetsutövare ska i en anmälan till tillsynsmyndigheten lämna uppgift om identitet, kontaktuppgift, IP-adressintervall, verksamhet och uppgift om i vilka länder verksamheten bedrivs. Gränsöverskridande verksamhetsutövare ska även lämna uppgift om huvudsakligt etableringsställe och i förekommande fall kontaktuppgift till företrädaren.

Ändras uppgifterna ska verksamhetsutövaren anmäla förändringen inom 14 dagar.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om uppgifterna.

3 kap. Riskhanteringsåtgärder och incidentrapportering

1 § Verksamhetsutövaren ska vidta tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken. De ska utvärderas och särskilt innefatta följande:

1. Incidenthantering,
2. kontinuitetshantering,
3. säkerhet i leveranskedjan,
4. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation,
5. strategier och förfaranden för användning av kryptografi och kryptering,
6. personalsäkerhet,
7. strategier för åtkomstkontroll och tillgångsförvaltning,
8. säkrade lösningar för kommunikation, och
9. lösningar för autentisering.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om riskhanteringsåtgärder.

2 § Verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete.

3 § Ledningen i enskilda och offentliga verksamheter ska genomgå utbildning om riskhanteringsåtgärder och anställda ska erbjudas sådan utbildning.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om utbildning.

4 § Med betydande incident avses

1. En incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller

2. en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande incident.

5 § Verksamhetsutövaren ska som en varning underrätta CSIRT-enheten om betydande incidenter inom 24 timmar efter det att verksamhetsutövaren fått kännedom om den. Det ska anges om att det finns misstanke om incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter.

6 § Verksamhetsutövaren ska också inom 72 timmar från tidpunkten från kännedom göra en incidentanmälan till CSIRT-enheten om betydande incidenter. Den ska innehålla en inledande bedömning av hur allvarlig den betydande incidenten är, konsekvenserna av den och förekomsten av angreppsindikatorer. Vidare ska tidigare varning enligt 5 § uppdateras.

För verksamhetsutövare som erbjuder betrodda tjänster ska en incidentanmälan göras inom 24 timmar.

CSIRT-enheten får begära ytterligare information av verksamhetsutövaren.

Verksamhetsutövaren ska samtidigt även informera kunder som kan antas påverkas av den betydande incidenten. Kunderna ska vid behov informeras om avhjälpande åtgärder. Detsamma gäller betydande cyberhot.

7 § Verksamhetsutövaren ska inom en månad från incidentanmälan i 5 § lämna en slutrapport till CSIRT-enheten. Om incidenten fortfarande är pågående ska i stället en lägesrapport lämnas som ska kompletteras med en slutrapport en månad efter det att incidenten har hanterats. Slutrapporten eller lägesrapporten ska innehålla en beskrivning av

1. Incidenten och dess konsekvenser,
2. hur allvarlig incidenten bedöms vara,
3. vad som sannolikt utlöst incidenten,
4. åtgärderna för att begränsa incidenten, och
5. incidentens möjliga gränsöverskridande effekter.

8 § Regeringen eller den myndigheten regeringen bestämmer får meddela föreskrifter om incidentrapporteringen enligt 5–7 §§.

4 kap. Tillsyn

Tillsynsmyndighet

1 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Tillsynsmyndighetens uppdrag

2 § Tillsynsmyndigheten ska utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

3 § Tillsynsåtgärder för viktiga verksamhetsutövare får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att denna lag eller föreskrifter som meddelats i anslutning till lagen inte följs.

Tillsynsmyndighetens undersökningsbefogenheter

4 § Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten den information som behövs för tillsyn.

5 § Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamheten.

6 § Tillsynsmyndigheten får förelägga den som står under tillsyn att tillhandahålla information och ge tillträde enligt 4 och 5 §§.

Ett sådant föreläggande får förenas med vite.

7 § Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att genomföra de åtgärder som avses i 4 och 5 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Säkerhetsrevision

8 § Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten.

Tillsynsmyndigheten får även anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare.

Regeringen får meddela föreskrifter om säkerhetsrevisioner.

Säkerhetsskanning

9 § Tillsynsmyndigheten får låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av denna lag.

En säkerhetsskanning ska ske i samarbete med verksamhetsutövaren.

5 kap. Ingripanden och sanktioner

Inledande bestämmelser

1 § Tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter enligt denna lag, eller föreskrifter som har meddelats med stöd av bestämmelserna om

1. skyldighet att utse företrädare enligt 1 kap. 6 §,
2. anmälningsskyldighet enligt 2 kap. 2 §,
3. riskhanteringsåtgärder enligt 3 kap. 1 §,
4. utbildning enligt 3 kap. 3 §, eller
5. incidentrapportering enligt 3 kap. 5–7 §§.

2 § Ingripanden sker genom att tillsynsmyndigheten

1. meddelar föreläggande enligt 6 §,
2. ansöker om förbud att utöva ledningsfunktion enligt 7 §, eller
3. meddelar sanktionsavgift enligt 11 §.

Om tillsynsmyndigheten inte finner skäl att ingripa enligt första stycket ska den i stället meddela verksamhetsutövaren en anmärkning.

Tillsynsmyndigheten får avstå från att ingripa enligt första och andra stycket om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren eller den fysiska personen med anledning av överträdelsen, och tillsynsmyndigheten bedömer att dessa åtgärder är tillräckliga.

Omständigheter som ska beaktas vid ett ingripande

3 § Vid val och utformning av ingripandeåtgärder enligt 2 § ska hänsyn tas till hur allvarlig överträdelsen är, hur länge den har pågått, samt den skada eller risk för skada som uppstått till följd av överträdelsen.

Vid bedömningen ska särskilt beaktas

1. de åtgärder verksamhetsutövaren vidtagit för att förhindra eller minska skadan,
2. verksamhetsutövarens samarbete med tillsynsmyndigheten,
3. om överträdelsen begåtts med uppsåt eller oaktsamhet, och
4. den ekonomiska fördel som verksamhetsutövaren fått till följd av överträdelsen.

4 § Utöver vad som anges i 3 § ska det beaktas som försvårande om verksamhetsutövaren tidigare har begått en överträdelse.

I förmildrande riktning ska beaktas om verksamhetsutövaren har följt godkända uppförandekoder eller godkända certifieringsmekanismer.

5 § En överträdelse ska betraktas som allvarlig om verksamhetsutövaren

1. har begått upprepade överträdelser,
2. inte har rapporterat eller avhjälpt en betydande incident,
3. inte har följt ett tidigare föreläggande från en tillsynsmyndighet,
4. har hindrat säkerhetsrevisioner eller tillsynsåtgärder som tillsynsmyndigheten beslutat om, eller
5. har lämnat oriktiga uppgifter avseende riskhanteringsåtgärder eller rapporteringsskyldigheter enligt 3 kap. 1 eller 5–7 §§.

Förelägganden

6 § Tillsynsmyndigheten får meddela de förelägganden som behövs för att verksamhetsutövare ska uppfylla skyldigheterna som följer av 1 §.

Förelägganden enligt denna paragraf får förenas med vite.

7 § Tillsynsmyndigheten får förelägga en verksamhetsutövare att offentliggöra information på det sätt som tillsynsmyndigheten beslutar rörande överträdelser av denna lag och föreskrifter som har meddelats med stöd av lagen.

Tillsynsmyndigheten får förelägga en verksamhetsutövare att informera de användare som kan påverkas av ett betydande cyberhot om hotet och vilka skydds- eller motåtgärder de kan vidta.

Förelägganden enligt denna paragraf får förenas med vite.

Förbud att utöva ledningsfunktion

8 § Om ett föreläggande enligt 6 § inte följts får tillsynsmyndigheten ingripa mot en person som ingår i verksamhetsutövarens ledning. Ingripande sker genom att tillsynsmyndigheten ansöker hos

allmän förvaltningsdomstol om att en person inte ska få vara befattningshavare hos en viss verksamhetsutövare (förbud).

Ett sådant ingripande får riktas mot den som är befattningshavare enligt 3 § andra stycket lagen (2014:836) om näringsförbud.

Ett ingripande får endast göras om överträdelsen som ligger till grund för föreläggandet är allvarlig och om personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

9 § Ett beslut om förbud enligt 8 § fattas av förvaltningsrätten på ansökan från tillsynsmyndigheten. En ansökan ska innehålla uppgifter om

1. den person som ansökan avser,
2. verksamhetsutövaren,
3. överträdelsen och de omständigheter som behövs för att kännetecknа den, och
4. de bestämmelser som är tillämpliga på överträdelsen.

Ett förbud ska tidsbegränsas till lägst ett år och högst tre år och ska upphävas omedelbart när föreläggandet har följts.

Förbud får inte riktas mot offentliga verksamhetsutövare.

Ansökan ska prövas skyndsamt av domstolen.

10 § Ett beslut om förbud ska upphävas om det inte längre finns förutsättningar för förbudet.

11 § Förvaltningsrätten ska pröva om ett beslutat förbud ska upphävas om tillsynsmyndigheten eller den enskilde begär det, eller om det annars finns skäl för det. Den enskilde ska upplysas om sin rätt att begära att ett förbud ska upphävas.

Om tillsynsmyndigheten bedömer att det inte längre finns förutsättningar för förbudet ska den omedelbart begära att förvaltningsrätten ska upphäva förbudet.

Sanktionsavgift

12 § Tillsynsmyndigheten får besluta att en verksamhetsutövare ska betala en sanktionsavgift till följd av en överträdelse enligt 1 §.

Sanktionsavgiftens storlek

13 § Sanktionsavgiften ska för väsentliga verksamhetsutövare bestämmas till lägst 5 000 kr och högst till det högsta av:

1. Två procent av den väsentliga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 10 000 000 euro.

14 § Sanktionsavgiften ska för viktiga verksamhetsutövare bestämmas till lägst 5 000 kr och högst till det högsta av:

1. 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 7 000 000 euro.

15 § Sanktionsavgiften ska för offentliga verksamhetsutövare bestämmas till lägst 5 000 kr och högst 10 000 000 kr.

Hur sanktionsavgiften ska bestämmas

16 § När sanktionsavgiftens storlek bestäms ska tillsynsmyndigheten särskilt beakta de omständigheter som följer av 3–5 §§.

Hinder mot att ta ut sanktionsavgift

17 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

En sanktionsavgift får inte heller beslutas för samma överträdelse som lett till att verksamhetsutövaren har påförts en sanktionsavgift enligt Allmänna dataskyddsförordningen.

Betalning, verkställighet och preskription

18 § En sanktionsavgift får endast tas ut om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Beslut om sanktionsavgift ska delges.

19 § Sanktionsavgiften ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning ska verkställighet få ske enligt utsökningsbalken.

Sanktionsavgift tillfaller staten.

20 § En beslutad sanktionsavgift ska falla bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Förordnande om att beslut ska gälla omedelbart

21 § Tillsynsmyndigheten får bestämma att ett beslut om föreläggande enligt denna lag ska gälla omedelbart.

6 kap. Överklagande

1 § Tillsynsmyndighetens beslut enligt denna lag eller anslutande föreskrifter får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

---

1. Denna lag träder i kraft den 1 januari 2025.

2. Genom lagen upphävs lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagen ska dock fortfarande gälla för överträdelser som har skett före ikraftträdandet.

1.2 Förslag till lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet

Härigenom föreskrivs att rubriken till lag (2006:24) om nationella toppdomäner för Sverige på internet samt 1, 2 och 6 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Lag om *nationella* toppdomäner *för Sverige* på internet	**Lag om toppdomäner på internet**
1 §	
Denna lag gäller teknisk drift av *nationella* toppdomäner *för* Sverige på *I*nternet *samt* tilldelning och registrering av domännamn under dessa toppdomäner.	Denna lag gäller teknisk drift av toppdomäner *med huvudsakligt etableringsställe i* Sverige på *i*nternet. *Vidare omfattar lagen* tilldelning och registrering av domännamn under dessa toppdomäner.
2 §	
I denna lag avses med	
domännamnssystemet: det internationella hierarkiska system som för befordringsändamål på Internet används för att tilldela domännamn,	
domän: nivå i domännamnssystemet och del av domännamn,	
domännamn: unikt namn sammansatt av domäner, där en i domännamnssystemet lägre placerad domän står före en domän som är högre placerad i systemet,	
toppdomän: den domän som återfinns sist i ett domännamn,	
nationell toppdomän: toppdomän som betecknar en nation eller en region,	
administration: teknisk drift av en toppdomän samt tilldelning och registrering av domännamn under denna,	
domänadministratör: den som ansvarar för administration av en *nationell* toppdomän *för Sverige*,	domänadministratör: den som ansvarar för administration av en toppdomän,

namnserver: dator i ett elektroniskt kommunikationsnät som programmerats så att den lagrar och distribuerar information om domännamn samt tar emot och svarar på frågor om domännamn.

6 §

En domänadministratör *skall* föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna	En domänadministratör *ska* föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna
Registret *skall* innehålla	Registret *ska* innehålla
1. domännamnet,	
2. namnet på domännamnsinnehavaren och dennes postadress, telefonnummer och adress för elektronisk post,	
3. namnet på den som tekniskt administrerar domännamnet och dennes postadress, telefonnummer och adress för elektronisk post,	
4. uppgifter om de namnservrar som är knutna till domännamnet, *samt*	4. uppgifter om de namnservrar som är knutna till domännamnet,
5. övrig teknisk information som behövs för att administrera domännamnet.	5. övrig teknisk information som behövs för att administrera domännamnet, *och*
	6. registreringsdatum.
Uppgifterna i registret *skall* kunna hämtas utan avgift via *I*nternet.	Uppgifterna i registret *ska* kunna hämtas utan avgift via *i*nternet. *Därutöver ska uppgifter även på begäran lämnas ut skyndsamt till myndigheter och andra med offentligrättsliga uppgifter inom EES.*
Personuppgifter får *dock* göras tillgängliga på *detta sätt endast* om den registrerade har samtyckt till det.	Personuppgifter får *endast* göras tillgängliga på *internet* om den registrerade har samtyckt till det.

Domänadministratören är personuppgiftsansvarig för behandling av personuppgifter i registret.

Denna lag träder i kraft den 1 januari 2025.

1.3 Förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2022:482) om elektronisk kommunikation

dels att 8 kap. 1–4 §§ ska upphöra att gälla,

dels att 12 kap. 1 § ska ha följande lydelse,

dels att rubriken närmast före 8 kap. 1 § ska utgå.

Nuvarande lydelse	*Föreslagen lydelse*
	12 kap.
	1 §[1]
Tillsynsmyndigheten ska besluta att ta ut en sanktionsavgift av den som	
1. inte tillhandahåller en sammanfattning av avtalet i enlighet med 7 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 102.3 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,	
2. inte tillämpar villkor om bindningstid eller uppsägningstid i enlighet med 7 kap. 8, 13 eller 14 §,	
3. inte uppfyller kraven på nummerportabilitet i enlighet med 7 kap. 19 och 20 §§ eller föreskrifter om nummerportabilitet som har meddelats med stöd av 7 kap. 21 § första stycket,	
4. inte vidtar åtgärder för att hantera risker som hotar säkerheten i nät och tjänster i enlighet med 8 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,	
5. inte rapporterar om säkerhetsincidenter i enlighet med 8 kap. 3 §, föreskrifter som har meddelats	

[1] Senaste lydelse 2023:411.

med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

6. inte informerar om hot om säkerhetsincidenter i enlighet med 8 kap. 4 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

7. inte vidtar skyddsåtgärder i enlighet med 8 kap. 5 § eller föreskrifter som har meddelats med stöd av den paragrafen,

8. inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. 6 § eller föreskrifter som har meddelats med stöd av den paragrafen,

9. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,

10. inte underrättar om integritetsincidenter i enlighet med 8 kap. 8 § eller kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig

4. inte vidtar skyddsåtgärder i enlighet med 8 kap. 5 § eller föreskrifter som har meddelats med stöd av den paragrafen,

5. inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. 6 § eller föreskrifter som har meddelats med stöd av den paragrafen,

6. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,

7. inte underrättar om integritetsincidenter i enlighet med 8 kap. 8 § eller kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig

integritet och elektronisk kommunikation,

11. inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,

12. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket eller föreskrifter som har meddelats i anslutning till det stycket,

13. inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand i enlighet med 9 kap. 29 b § andra stycket eller föreskrifter som har meddelats i anslutning till det stycket,

14. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § eller föreskrifter som har meddelats med stöd av den paragrafen, eller

15. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §.

integritet och elektronisk kommunikation,

8. inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,

9. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket eller föreskrifter som har meddelats i anslutning till det stycket,

10. inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand i enlighet med 9 kap. 29 b § andra stycket eller föreskrifter som har meddelats i anslutning till det stycket,

11. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § eller föreskrifter som har meddelats med stöd av den paragrafen, eller

12. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §.

En sanktionsavgift enligt första stycket 2 ska, när det är fråga om ett paket enligt 7 kap. 26 §, tas ut endast om överträdelsen avser en allmänt tillgänglig elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst eller en överföringstjänst som används för tillhandahållande av maskin-till-maskin-tjänster.

1. Denna lag träder i kraft den 1 januari 2025.
2. Äldre bestämmelser gäller fortfarande för överträdelser som skett före ikraftträdandet.

1.4 Förslag till förordning om cybersäkerhet

Härigenom föreskrivs följande.

Inledande bestämmelser

1 § Denna förordning kompletterar lagen om cybersäkerhet.

Uttryck i förordningen

2 § Uttryck som används i förordningen har samma innebörd som i lagen om cybersäkerhet.

Huvudsakligt etableringsställe

3 § Vid bedömningen av vad som utgör huvudsakligt etableringsställe enligt 1 kap. 6 § tredje stycket lagen om cybersäkerhet ska följande omständigheter beaktas i angiven rangordning:

1. Plats för beslut om riskhanteringsåtgärder för cybersäkerhet,
2. plats för cybersäkerhetsverksamhet, eller
3. plats där verksamhetsutövaren har flest anställda.

Enskilda verksamhetsutövare

4 § Enskilda verksamhetsutövare får ansöka hos tillsynsmyndighet om att undantas från 1 kap. 4 § första stycket 3 lagen om cybersäkerhet. Myndigheten får meddela ett sådant undantag om verksamheten inte i sig uppfyller storlekskravet i paragrafen, men gör det som partnerföretag eller anknutet företag om ett undantag är skäligt med hänsyn till den lagens syfte.

Verksamhetsutövare som omfattas av krav om cybersäkerhet i andra författningar

5 § I bilaga till denna förordning anges de lagar och andra författningar som innehåller krav på riskhanteringsåtgärder och incidentrapportering med verkan som sammantaget motsvarar skyldigheterna enligt lagen om cybersäkerhet.

Verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpning till övervägande del

6 § Fortifikationsverket, Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Försvarsunderrättelsedomstolen, Statens inspektion för försvarsunderrättelseverksamheten, Säkerhetspolisen, Totalförsvarets forskningsinstitut och Totalförsvarets plikt- och prövningsverk bedriver säkerhetskänslig verksamhet till övervägande del.

7 § Brottsförebyggande rådet, Brottsoffermyndigheten, Ekobrottsmyndigheten, Kriminalvården, Polismyndigheten, Rättsmedicinalverket, Säkerhetspolisen och Åklagarmyndigheten bedriver brottsbekämpning till övervägande del.

Tillsynsmyndighet

8 § Följande myndigheter ska vara tillsynsmyndighet enligt lagen om cybersäkerhet och denna förordning för angivna tillsynsområden.

Tillsynsmyndighet	**Sektor**
Statens energimyndighet	Energi
Transportstyrelsen	Transporter
	Tillverkning av motorfordon, släpfordon, påhängsvagnar och andra transportmedel
Finansinspektionen	Bankverksamhet
	Finansmarknadsinfrastruktur

Inspektionen för vård och omsorg	Vårdgivare[1] i Hälso- och sjukvårdssektorn
Läkemedelsverket	Hälso- och sjukvårdssektorn, med undantag för vårdgivare Tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik
Livsmedelsverket	Avloppsvatten Dricksvatten Produktion, bearbetning och distribution av livsmedel
Post- och telestyrelsen	Digital infrastruktur Digitala leverantörer Förvaltning av IKT-tjänster Post- och budtjänster Rymden
Länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län	Avfallshantering Forskning Lärosäten med examenstillstånd Offentlig förvaltning Tillverkning, produktion och distribution av kemikalier Tillverkning av datorer, elektronikvaror och optik Tillverkning av elapparatur Tillverkning av övriga maskiner

9 § Länsstyrelsen i Norrbottens län ska vara tillsynsmyndighet för kommuner och regioner som hör till Västernorrlands, Jämtlands, Västerbottens eller Norrbottens län och verksamhetsutövare som har sitt säte i något av dessa län samt Länsstyrelsen i Stockholms län.

10 § Länsstyrelsen i Skåne län ska vara tillsynsmyndighet för kommuner och regioner som hör till Kronobergs, Blekinge, Kalmar eller Skåne län och verksamhetsutövare som har sitt säte i något av dessa län samt Länsstyrelsen i Västra Götalands län.

[1] Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård.

11 § Länsstyrelsen i Stockholms län ska vara tillsynsmyndighet för kommuner och regioner som hör till Stockholms, Uppsala, Södermanlands, Västmanlands, Värmlands, Gotlands, Örebro, Dalarnas eller Gävleborgs län och verksamhetsutövare som har sitt säte i något av dessa län samt Länsstyrelsen i Norrbottens län.

12 § Länsstyrelsen i Västra Götalands län ska vara tillsynsmyndighet för kommuner och regioner som hör till Hallands, Jönköpings, Västra Götalands eller Östergötlands län och verksamhetsutövare som har sitt säte i något av dessa län samt Länsstyrelsen i Skåne län.

13 § Om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive tillsynsmyndighet inte utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde i 8 §.

Tillsynsmyndighetens uppgifter

14 § Tillsmyndigheten ska upprätta ett register över väsentliga och viktiga verksamhetsutövare. Registret ska ges in till den gemensamma kontaktpunkten senast den 1 mars 2025. Därefter ska det ske en uppdatering och ny rapportering i vart fall vartannat år.

15 § Tillsynsmyndigheten ska samarbeta med Integritetsskyddsmyndigheten vid hantering av incidenter som även utgör personuppgiftsincidenter.

Om tillsynsmyndigheten, när den bedriver tillsyn enligt lagen om cybersäkerhet, får kännedom om en omständighet som kan innebära en personuppgiftsincident som ska anmälas enligt den allmänna dataskyddsförordningen ska tillsynsmyndigheten utan onödigt dröjsmål informera Integritetsskyddsmyndigheten.

16 § Om tillsynsmyndigheten bedriver tillsyn över en verksamhetsutövare som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster enligt artikel 31 i Dora-förordningen ska tillsynsmyndigheten informera det tillsynsforum som inrättats enligt artikel 32 i samma förordning.

17 § Tillsynsmyndigheten ska samarbeta med och bistå tillsynsmyndigheter i andra medlemsstater inom EES avseende verksamhetsutövare som erbjuder tjänster i mer än en medlemsstat eller erbjuder tjänster i en eller flera medlemsstater och dess nätverks- och informationssystem finns i en eller flera medlemsstater.

18 § Tillsynsmyndigheten får avslå en begäran om bistånd enligt 17 § om myndigheten inte är behörig att tillhandahålla biståndet, om biståndet inte är proportionerligt i förhållande till tillsynsmyndighetens uppgifter eller om begäran avser information eller omfattar verksamhet som om den skulle lämnas ut eller utförs, skulle inverka skadligt på Sveriges säkerhetsintressen, allmänna säkerhet eller försvar.

Innan tillsynsmyndigheten avslår en begäran om bistånd ska tillsynsmyndigheten samråda med övriga berörda behöriga myndigheter samt, på begäran av de berörda medlemsstaterna, med kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa).

19 § Tillsynsmyndigheten ska lämna stöd till Sveriges representant i den samarbetsgrupp som inrättats enligt artikel 14 i NIS2-direktivet.

Gemensam kontaktpunkt

20 § Myndigheten för samhällsskydd och beredskap ska vara gemensam kontaktpunkt.

Gemensamma kontaktpunktens uppgifter

21 § Den gemensamma kontaktpunkten ska utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete med myndigheter i andra medlemsstater, kommissionen och Enisa samt ett sektorsövergripande samarbete med tillsynsmyndigheterna.

22 § Den gemensamma kontaktpunkten är Sveriges representant i den samarbetsgrupp som inrättats enligt artikel 14 i NIS2-direktivet.

23 § Den gemensamma kontaktpunkten ska på begäran av CSIRT-enheten vidarebefordra incidentrapporter till de gemensamma kontaktpunkterna i andra medlemsstater.

24 § Den gemensamma kontaktpunkten ska var tredje månad lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud.

25 § Den gemensamma kontaktpunkten ska senast den 17 april 2025 och därefter vartannat år underrätta kommissionen och samarbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare som förtecknats för varje sektor och delsektor.

Den gemensamma kontaktpunkten ska informera kommissionen och samarbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare samt deras verksamhet som identifierats enligt 1 kap. 8 § lagen om cybersäkerhet.

26 § Den gemensamma kontaktpunkten ska upprätta ett särskilt register över gränsöverskridande verksamhetsutövare och ge in det skyndsamt till Enisa. Vidare ska den gemensamma kontaktpunkten löpande underrätta Enisa om uppgifter avseende gränsöverskridande verksamhetsutövare.

CSIRT-enhet

27 § Myndigheten för samhällsskydd och beredskap ska vara CSIRT-enhet.

CSIRT-enhetens uppgifter

28 § När CSIRT-enheten utför sina uppgifter ska den,

1. säkerställa en hög nivå av tillgänglighet för sina kommunikationskanaler,
2. ha lokaler och informationssystem på säkra platser,
3. ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar,
4. vara ständigt tillgänglig och säkerställa att personalen har fått lämplig utbildning,
5. ha redundanta system och reservlokaler för att säkerställa kontinuiteten i tjänsterna, och

6. ha en säker och motståndskraftig kommunikations- och informationsstruktur för utbyte av information med verksamhetsutövare och andra relevanta intressenter.

29 § CSIRT-enheten ska,

1. övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå och tillhandahålla varningar och information,
2. erbjuda stöd avseende realtidsövervakning av nätverks- och informationssystem,
3. ta emot incidentrapporter, vidta åtgärder och erbjuda stöd,
4. om en incident kan antas ha sin grund i en brottslig gärning skyndsamt uppmana verksamhetsutövaren att anmäla incidenten till Polismyndigheten,
5. tillgängliggöra informationen i incidentrapporter utan dröjsmål för tillsynsmyndigheten,
6. samla in och analysera forensiska uppgifter,
7. tillhandahålla dynamiska risk- och incidentanalyser samt lägesuppfattning,
8. på begäran av en verksamhetsutövare utföra en proaktiv skanning av den berörda verksamhetsutövarens nätverks- och informationssystem,
9. delta i det nätverk som inrättats enligt artikel 15 i NIS2-direktivet (CSIRT-nätverket),
10. vara samordnare för samordnad delgivning av information om sårbarheter, och
11. upprätta samarbetsförbindelser med relevanta intressenter inom privat och offentlig sektor samt bidra till samverkan rörande cybersäkerhet.

30 § CSIRT-enheten får utföra proaktiva, icke-inkräktande skanningar av verksamhetsutövarnas allmänt tillgängliga nätverks- och informationssystem i syfte att upptäcka sårbara eller osäkert konfigurerade system.

Cyberkrishanteringsmyndighet

31 § Myndigheten för samhällsskydd och beredskap ska vara cyberkrishanteringsmyndighet.

32 § Myndigheten för samhällsskydd och beredskap ska delta i det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe).

Rätt att meddela föreskrifter

33 § Myndigheten för samhällsskydd och beredskap får i föreskrifter ange vilka verksamhetsutövare som omfattas av 1 kap. 8 § lagen om cybersäkerhet och om verksamhetsutövaren är väsentlig. Tillsynsmyndigheten ska ges tillfälle att yttra sig.

34 § Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om anmälningsskyldigheten i 2 kap. 2 § lagen om cybersäkerhet.

35 § Tillsynsmyndigheten får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning enligt 3 kap. 1–3 §§ lagen om cybersäkerhet. Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig.

För sektorn offentlig förvaltning och lärosäten med examenstillstånd får Myndigheten för samhällsskydd och beredskap i stället för länsstyrelserna i 8 § meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning enligt 3 kap. 1–3 §§ lagen om cybersäkerhet.

36 § Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om vad som utgör en betydande incident enligt 3 kap. 4 § och om incidentrapportering enligt 3 kap. 5–7 §§ lagen om cybersäkerhet. Tillsynsmyndigheten ska ges tillfälle att yttra sig.

Samarbetsforum för effektiv och likvärdig tillsyn

37 § Myndigheten för samhällsskydd och beredskap ska leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Begäran om information

38 § När tillsynsmyndigheten begär information enligt 4 kap. 4 § lagen om cybersäkerhet ska myndigheten ange syftet med begäran och precisera vilken information som krävs.

Säkerhetsrevision

39 § Ett beslut om riktad säkerhetsrevision enligt 4 kap. 8 § lagen om cybersäkerhet ska baseras på riskbedömningar som utförts av tillsynsmyndigheten, verksamhetsutövaren eller på annan tillgänglig riskrelaterad information.

Beslut om förbud

40 § När ett beslut enligt 5 kap. 8 § lagen om cybersäkerhet har fått laga kraft ska domstolen underrätta Bolagsverket och verksamhetsutövaren om beslutet och dess innehåll. Om verksamhetsutövaren är en stiftelse ska den länsstyrelse som är registreringsmyndighet för stiftelsen underrättas i stället för Bolagsverket.

Domstolen ska skicka motsvarande underrättelser om ett sådant förbud upphävs.

41 § När Bolagsverket eller en länsstyrelse som är registreringsmyndighet har fått en underrättelse enligt 40 § ska de avregistrera personen som befattningshavare hos verksamhetsutövaren i det aktuella registret.

Bolagsverket eller en länsstyrelse som är registreringsmyndighet ska säkerställa att personen inte registreras på nytt som befattningshavare hos verksamhetsutövaren under förbudstiden.

---

1. Denna förordning träder i kraft den 1 januari 2025.

2. Genom förordningen upphävs förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Förordningen ska dock fortfarande gälla för överträdelser som har skett före ikraftträdandet.

Bilaga

Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

1.5 Förslag till förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen

Härigenom föreskrivs i fråga om förordningen (2007:951) med instruktion för Post- och telestyrelsen att 4 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

4 §[1]

Post- och telestyrelsen har till uppgift att

1. främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att se till att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska kommunikationstjänster,

2. främja utbyggnaden av och följa tillgången till bredband och mobiltäckning i alla delar av landet, inbegripet att skapa förutsättningar för samverkan mellan myndigheter som kan bidra till utbyggnaden av bredband,

3. svara för att möjligheterna till radiokommunikation och andra användningar av radiovågor utnyttjas effektivt,

4. svara för att nummer ur nationella nummerplaner utnyttjas på ett effektivt sätt,

5. främja en effektiv konkurrens,

6. övervaka pris- och tjänsteutvecklingen,

7. bedriva informationsverksamhet riktad till konsumenter,

8. följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation och uppkomsten av eventuella miljö- och hälsorisker,

9. pröva frågor om tillstånd och skyldigheter, fastställa och analysera marknader samt utöva tillsyn och pröva tvister enligt lagen (2022:482) om elektronisk kommunikation,

10. meddela föreskrifter enligt förordningen (2022:511) om elektronisk kommunikation,

11. upprätta och offentliggöra planer för frekvensfördelning till ledning för radioanvändningen samt offentliggöra information av allmänt intresse om rättigheter, villkor, förfaranden och avgifter som rör radiospektrumanvändningen,

[1] Senaste lydelse 2022:531.

12. tillhandahålla information om frekvensanvändning till Europeiska radiokommunikationskontorets frekvensinformationssystem (EFIS),

13. vara marknadskontrollmyndighet enligt radioutrustningslagen (2016:392),

14. vara tillsynsmyndighet enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och ge stöd och information till myndigheter och enskilda när det gäller betrodda tjänster,

15. följa utvecklingen när det gäller toppdomäner med geografiska namn som har anknytning till Sverige,

16. vara tillsynsmyndighet enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet samt meddela föreskrifter enligt förordningen (2006:25) om nationella toppdomäner för Sverige på internet,

17. verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, och verka för ökad krishanteringsförmåga,

18. verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer,

19. lämna råd och stöd till myndigheter, kommuner och regioner och till företag, organisationer och andra enskilda i frågor om nätsäkerhet,

20. vara tvistlösnings- och tillsynsmyndighet enligt lagen (2016:534) om åtgärder för utbyggnad av bredbandsnät och ansvara för informationstjänsten för utbyggnad av bredbandsnät enligt samma lag, och

21. vara tillsynsmyndighet enligt lagen *(2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.*	21. vara tillsynsmyndighet enligt lagen *(2024:XXX) om cybersäkerhet.*

Denna förordning träder i kraft den 1 januari 2025.

1.6 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

Härigenom föreskrivs att bilagan till offentlighets- och sekretessförordningen (2009:641) ska ha följande lydelse.

Nuvarande lydelse

Bilaga[1]

Verksamheten består i	Särskilda begränsningar i sekretessen
153. tillsyn enligt *lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*	

Föreslagen lydelse

Bilaga

Verksamheten består i	Särskilda begränsningar i sekretessen
153. tillsyn enligt *lagen (2025:000) om cybersäkerhet*	*Gäller ej beslut i ärenden*

Denna förordning träder i kraft den 1 januari 2025.

[1] Senaste lydelse 2023:742.

1.7 Förslag till förordning om ändring i förordningen (2022:511) om elektronisk kommunikation

Härigenom föreskrivs i fråga om förordningen (2022:511) om elektronisk kommunikation

dels att 1 kap. 2 § fjortonde strecksatsen ska upphöra att gälla,
dels att 8 kap. 1 och 5 §§ ska upphöra att gälla,
dels att 1 kap. 2 § femtonde strecksatsen ska ha följande lydelse,
dels att 8 kap. 4 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §[1]	
– –	
8 kap. *4–6 §§* i samma lag i fråga om 8 kap. 4 §,	8 kap. *5 och 6 §§* i samma lag i fråga om 8 kap. 4 §,
– –	
8 kap.	
4 §[2]	
Post- och telestyrelsen får meddela	
1. ytterligare föreskrifter om säkerhetsåtgärder enligt 8 kap. 1 § lagen (2022:482) om elektronisk kommunikation	
2. ytterligare föreskrifter om rapportering av säkerhetsincidenter enligt 8 kap. 3 § i samma lag,	
3. ytterligare föreskrifter om information till användare enligt 8 kap. 4 § i samma lag,	
4. ytterligare föreskrifter om skyddsåtgärder enligt 8 kap. 5 § i *samma lag*, och	*1.* ytterligare föreskrifter om skyddsåtgärder enligt 8 kap. 5 § i *lagen (2022:482) om elektronisk kommunikation*, och

[1] Senaste lydelse 2023:583.
[2] Senaste lydelse 2023:583.

5. föreskrifter om skyddsåtgärder enligt 8 kap. 6 § i samma lag.	*2.* föreskrifter om skyddsåtgärder enligt 8 kap. 6 § i samma lag.

1. Denna förordning träder i kraft den 1 januari 2025.
2. Äldre bestämmelser gäller fortfarande för överträdelser som skett före ikraftträdandet.

2 Utredningens uppdrag och arbete

I detta kapitel ska utredningens uppdrag och arbete beskrivas. Under 2.1 analyseras uppdraget, i 2.2 redovisas arbetet och 2.3 beskriver delbetänkandets disposition.

2.1 Analys av regeringens direktiv

2.1.1 Bakgrund

Europaparlamentet och rådet antog den 14 december 2022 två nya EU-direktiv: NIS2-direktivet[1], se bilaga 2 och CER-direktivet.[2] NIS2-direktivet ställer krav på säkerhet i nätverk och informationssystem. Det ersätter det tidigare NIS-direktivet från 2016, som genomfördes i svensk rätt genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, NIS-lagen.

NIS2-direktivet ersätter det tidigare direktivet och skärper kraven. Fler områden pekas ut.

Medlemsländerna ska senast den 17 oktober 2024 anta de nationella bestämmelser som krävs för att följa direktivet.

Regeringen beslutade den 23 februari 2023 att utse en särskild utredare med uppdrag att föreslå hur de två direktiven ska genomföras i svensk rätt, se bilaga 1. I uppdraget ingår att analysera hur den nya regleringen förhåller sig till säkerhetsskyddsregleringen och att föreslå en sammanhållen systematik mellan regelverken. Vidare ska

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet).
[2] Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

utredningen även klarlägga om det behövs ett starkare sekretesskydd för uppgifter till följd av direktivens krav. Uppdraget skulle genomföras under en tid om ett år. I tilläggsdirektiv beslutade regeringen att utredningens förslag avseende införlivning av NIS2-direktivet skulle redovisas i ett delbetänkande den 5 mars 2024 och övriga delar i ett slutbetänkande i september 2024.

2.1.2 Utredningens övergripande utgångspunkt

Direktiven är s.k. minimidirektiv, varför medlemsstaterna får anta mer långtgående bestämmelser. Det betyder att utredningen skulle kunna lämna förslag om att exempelvis fler sektorer än vad som följer av direktivet skulle kunna omfattas av en reglering. Utgångspunkten enligt regeringen ska dock vara att förslagen utformas så att regelbördan och administrationen minimeras för berörda verksamhetsutövare. Om utredningen lämnar mer långtgående förslag ska utredningen motivera varför det är nödvändigt och göra en analys om förslagen är samhällsekonomiskt effektiva och hur svenska företags konkurrenskraft skulle påverkas.

2.1.3 Särskilt om NIS2-direktivet

Vem omfattas?

Det tidigare direktivet omfattade leverantörer av samhällsviktiga tjänster och gav medlemsländerna relativ stor frihet att bestämma vem som skulle innefattas i detta. NIS2-direktivet anger som huvudregel att alla verksamhetsutövare som uppfyller vissa kriterier omfattas.

En särskild fråga är i vilken utsträckning kommuner ska omfattas. Kommunal verksamhet kan redan omfattas enligt det tidigare NIS-direktivet om kommuner bedriver verksamhet inom något av de sju utpekade områdena. Eftersom ett tillkommande område är offentlig förvaltning kommer dock offentliga verksamhetsutövare att omfattas i mycket större omfattning. Direktivet kan enligt regeringen tolkas så att statliga myndigheter och regioner omfattas, men överlåter åt medlemsstaterna att bestämma om kommuner ska omfattas. Ett annat nytt område i NIS2-direktivet är forskning. Utbildningsinstitutioner är undantagna från direktivets tillämpningsområde, men medlems-

staterna får föreskriva att direktivet även ska tillämpas på dem, vilket enligt regeringen kan vara särskilt relevant om de utför kritisk forskningsverksamhet. Utredningen ska överväga om universitet och högskolor ska omfattas eller ett urval av dem och därvid beakta principer om akademisk frihet, institutionell autonomi och forskningsintegritet samt excellens och öppenhet. Det ankommer förstås på utredningen att ta ställning till det.

Klassificering och registrering

De som omfattas av direktivet ska klassificeras antingen som väsentliga eller viktiga utifrån betydelse och storlek. Medlemsstaterna ska upprätta en förteckning, som uppdateras regelbundet. Underlag för förteckningen ska lämnas av verksamhetsutövarna till behöriga myndigheter, som i sin tur ska underrätta kommissionen. Medlemsländerna får alternativt inrätta ett system för självregistrering.

Riskhantering och rapportering

NIS2-direktivet ställer krav om tekniska, operationella och organisatoriska riskhanteringsåtgärder. Dessa ska vara proportionella utifrån bland annat storlek, sannolikhet för incidenter och möjlig påverkan. Direktivet uppställer minimikrav.

Direktivet innehåller också en rapporteringsskyldighet till CSIRT-enheten eller nationell myndighet. Enligt den nuvarande ordningen sker rapportering till CSIRT-enheten, dvs. MSB. Detta bör vara utgångspunkt även framöver.

Myndigheternas ansvarsfördelning

På samma sätt som enligt tidigare NIS-direktiv ska enligt det nya direktivet en eller flera behöriga myndigheter utöva tillsyn på nationell nivå. De nuvarande tillsynsmyndigheterna är Statens energimyndighet, Transportstyrelsen, Finansinspektionen, IVO, Livsmedelsverket och PTS. Därutöver ska det precis som tidigare finnas en nationell gemensam kontaktpunkt. Den ska utgöra en sambandsfunktion som säkerställer samarbete mellan de nationella myndigheterna och sam-

arbetet med myndigheter i andra medlemsländer. MSB är nationell gemensam kontaktpunkt. Oförändrat är även att det även fortsättningsvis ska finnas en eller flera s.k. CSIRT-enheter som ska ansvara för it-säkerhetsincidenter. MSB är för närvarande CSIRT-enhet. Myndigheten leder också ett samarbetsforum mellan tillsynsmyndigheter, där även Socialstyrelsen ingår.

Genom NIS2-direktivet införs några nyheter. En är att medlemsländerna ska utse en eller flera myndigheter som cyberkrishanteringsmyndighet med ansvar för storskaliga cybersäkerhetsincidenter och cyberkriser. Samarbetet mellan medlemsländerna förstärks såväl i samarbetsgruppen som mellan CSIRT-enheter. Det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) med företrädare för cyberkrishanteringsmyndigheter ska vara stödjande vid storskaliga incidenter och cyberkriser. Det finns redan ett frivilligt samarbete med MSB som svensk representant. En utgångspunkt är att den nya tillsynsstrukturen bör utgå från den tidigare.

Av det anförda följer att utredningen behöver utse tillsynsmyndigheter för de tillkommande områdena. Vidare behöver utredningen utse en cyberkrishanteringsmyndighet. Enligt regeringens direktiv är det en utgångspunkt att MSB behåller ansvaret som gemensam kontaktpunkt och CSIRT-enhet samt även utses till cyberkrishanteringsmyndighet. Det utredningen behöver klarlägga i denna del är om mandatet för MSB behöver förändras.

Det som därutöver anförs i regeringens direktiv i denna del är att det kan finnas skäl för en mer effektiv tillsyn, varför utredningen ska göra en utvärdering av den tillsyn som har bedrivits enligt tidigare reglering. En slutsats kan vara att detta i första hand bör ha bäring på myndigheternas arbete och samarbete, eftersom nuvarande struktur ska vara utgångspunkt.

Utredningen har vidare noterat att Försvarsberedningen i betänkandet *Kraftsamling* (Ds 2023:34), som överlämnades i december 2023, framför att det kan övervägas att ansvaret för cyber- och informationssäkerhet som i dag finns på MSB organiseras som ny myndighet. Utredningen har dock att förhålla sig till det av regeringen beslutade kommittédirektivet, där det bland annat anges att MSB ska ha vissa av de uppgifter som följer av NIS2-direktivet. Det kan dock konstateras att en utbrytning av cyber- och informationssäkerhetsfrågorna från MSB skulle behöva utredas närmare. Utredningen noterar också att frågan om Nationellt cybersäkerhetscenters ledning,

organisering och styrning utreds inom Försvarsdepartementet med inriktning att ett huvudmannaskap ska ligga hos Försvarets radioanstalt. Eftersom utredningen om cybersäkerhetscentret inte färdigställts när detta betänkande lämnas får eventuella förslag kring organisatoriska förändringar för myndigheterna som ingår i Nationellt cybersäkerhetscenter beaktas i den fortsatta beredningen av denna utrednings förslag.

Myndigheternas befogenheter

NIS2-direktivet uppställer detaljerade krav på befogenheter för tillsynsmyndigheterna och innehåller sanktioner. Flera åtgärder saknar direkt motsvarighet i svensk rätt. Det gäller kravet om att tillfälligt upphäva certifiering eller tillstånd för verksamhet och att tillfälligt förbjuda personer i ledningen att utöva ledningsfunktioner. I denna del ska utredningen analysera hur en sådan reglering förhåller sig till relevant reglering inom andra områden i svensk rätt, till exempel associationsrättsliga regler eller sektorsspecifika regler som innehåller krav om certifiering eller tillstånd.

Det är enligt direktivet upp till medlemsstaterna att avgöra om bestämmelser om straffansvar ska införas för den nationella regleringen. Vid genomförandet av det tidigare NIS-direktivet gjordes bedömningen att överträdelser inte skulle vara straffsanktionerade. Skälen var att kriminalisering som metod bör användas med försiktighet. Vidare skulle straff inte heller vara den effektivaste sanktionen, eftersom de som skulle kunna göra sig skyldiga till överträdelser skulle vara myndigheter, kommuner, landsting och företag. Straff kan enligt svensk rätt endast ådömas en fysisk person. Det saknas enligt regeringen nu skäl att frångå den bedömningen. Utredningens inriktning ska därför vara att sanktioner ska vara av administrativt slag. Det handlar då om sanktionsavgifter. En förändring i förhållande till NIS-lagen är att dessa ska ligga på en högre nivå.

2.1.4 Förhållandet till säkerhetsskyddsregleringen

Säkerhetsskyddsregleringens, dvs. säkerhetshetsskyddslagen (2018:585), och säkerhetsskyddsförordning (2021:955), huvudsyfte är att skydda verksamheter som har betydelse för Sveriges säkerhet ur ett natio-

nellt perspektiv. Det finns möjlighet att helt undanta offentliga och enskilda verksamhetsutövare som i hög grad bedriver verksamhet inom områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, medan de verksamhetsutövare som bedriver sådan verksamhet i mindre utsträckning inte i sin helhet kan undantas från direktivet.

I stället får medlemsstaterna för dessa på olika sätt för specifika verksamheter besluta om undantag från vissa krav. Detta rimmar dock inte med den nuvarande svenska lagsystematiken.

Säkerhetsskyddslagen omfattar enligt 1 § den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet). NIS-lagens 8 § anger att lagen inte gäller för verksamhet som omfattas av säkerhetsskyddslagen. Av 2 kap. 1 § säkerhetsskyddslagen följer sedan att den som till någon del bedriver säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd (säkerhetsskyddsanalys).

Innebörden är enligt regeringen att en verksamhetsutövare själv ska bedöma vilka delar av verksamheten som omfattas av säkerhetsskyddslagen respektive NIS-lagen. Problemet skulle nu vara att detta mer generella system inte skulle rimma med NIS2-direktivets krav om specifika undantag för vissa verksamheter.

I regeringens direktiv anförs att det skulle vara naturligt att utgå från gällande tillsynsstruktur i säkerhetsskyddslagen. Tillsynsansvaret är fördelat bland annat mellan Försvarsmakten och Säkerhetspolisen. Dessa ska sedan genom systematisk kartläggning identifiera verksamhetsutövare inom myndigheternas respektive tillsynsområde. Dessa skulle då också kunna besluta om specifika undantag från kraven i direktiven. Regeringens utgångspunkt är alltså att de nya kraven i NIS2-direktivet i denna del skulle regleras genom en anpassning av säkerhetsskyddsregleringen. Det anges också uttryckligen att inriktningen ska vara att säkerhetskänslig verksamhet undantas från den nya regleringen så långt det är möjligt. I regeringens direktiv anges dock också att utredningen kan föreslå andra lösningar.

Utredningen bedömer att skäl för andra lösningar kan vara att undantag i säkerhetsskyddslagen kan bli komplicerat att genomföra. En inledande åtgärd för utredningen kan vara att ingående analysera i vilken utsträckning direktiven ställer tvingande krav om beslut om specifika undantag för verksamhetsutövare. En annan komplikation

är att det inte kommer att vara tillräckligt att undanta verksamhetsutövare som bedriver säkerhetskänslig verksamhet helt eller delvis från rapporteringskravet om incidenter. Det behöver därutöver exempelvis införas undantag för uppgifter som rör säkerhetskänslig verksamhet så att de inte registreras i den europeiska sårbarhetsdatabasen som enligt NIS2-direktivet ska upprättas.

2.1.5 Förhållandet till annan unionsrättslig och nationell regering

Utredningen behöver beakta annan sektorsspecifik unionsrättslig reglering. Det gäller särskilt för sektorerna bankverksamhet och finansmarknadsinfrastruktur. Även annan nationell reglering ska förstås beaktas. När det gäller verksamhetsutövares säkerhetsarbete ska målet vara att samordningsvinster uppnås. Regelbördan och administrationen ska minimeras och kostnadseffektivitet eftersträvas.

2.1.6 Utanför uppdraget

Vissa saker som regleras i direktivet faller utanför uppdraget, eftersom det ska behandlas i särskild ordning. Det handlar om införandet av ett system för sakkunnigbedömningar samt om nationell strategi för cybersäkerhet och nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter. Dessa ämnen ska därför inte behandlas av utredningen.

2.1.7 Konsekvensanalys

En viktig uppgift för utredningen är att göra en konsekvensanalys för förslagen. Det handlar särskilt om ekonomiska konsekvenser för myndigheter och företag samt påverkan på den kommunala självstyrelsen.

Kostnadsökningar för det allmänna ska utredningen föreslå en finansiering för.

Med hänsyn till att ett stort antal myndigheter kan förväntas få nya tillsynsuppgifter kan konsekvensanalysen behöva bli omfattande. En utgångspunkt med hänsyn till komplexiteten krävs konsultstöd för att upprätta i vart fall delar av analysen.

2.2 Utredningens arbete

Utredningens arbete har bedrivits på sedvanligt sätt med regelbundna möten med sakkunniga och experter samt med deltagarna i en till utredningen knuten referensgrupp. Utredningen har haft sex protokollförda möten med expert- och sakkunniggruppen och två med referensgruppen. Utredningen har också haft enskilda möten med deltagarna i expert- och sakkunniggruppen samt referensgruppen.

Utredningen har också träffat Tele2 Sverige AB, Netnod Internet Exchange i Sverige AB, Svenska Bankföreningen, Säkerhets- och försvarsföretagen, Inspektionen för vård och omsorg samt Försvarets radioanstalt. Utredningen har vidare träffat de myndigheter som föreslås som nya tillsynsmyndigheter, dvs. Läkemedelsverket, och länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län.

Utredningen har löpande hållit Regeringskansliet informerat om arbetet.

Utredningen har i enlighet med direktiven också hållit sig informerad om arbetet i *Fastighetsregisterlagsutredningen* (Ju 2022:09), *Operativ krisledning vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur* (Fi2023/01842), *Uppdrag att lämna förslag på hur en ändamålsenlig och effektiv ledning, organisering och styrning av Nationellt cybersäkerhetscenter ska utformas* (Fö 2023:A) och *Utredningen om säker och tillgänglig digital identitet* (I 2022:04).

2.3 Betänkandets disposition

Betänkandet inleds med en övergripande beskrivning av NIS2-direktivet (kapitel 3). Därefter följer en beskrivning av de nya sektorer som följer av direktivet (kapitel 4). I kapitel 5 behandlas cybersäkerhetslagens tillämpningsområde. I kapitel 6 behandlas klassificering och registrering av verksamhetsutövare. Riskhantering och incidentrapportering behandlas i kapitel 7. Kapitlen därefter behandlar till-

syn (kapitel 8) och ingripanden och sanktioner (kapitel 9). I kapitel 10 behandlas funktionerna gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet. Kapitel 11 analyserar hur NIS2-direktivet påverkar lagen (2022:482) om elektronisk kommunikation. Kapitel 12 innehåller utredningens konsekvensanalys. Ikraftträdandet behandlas i kapitel 13. Slutligen följer en författningskommentar till de lämnade författningsförslagen (kapitel 14). Kommittédirektivet finns i sin helhet i bilaga 1. Utredningens tilläggsdirektiv finns i bilaga 2. I bilaga 3 finns NIS2-direktivet. Bilaga 4 är en av utredningen beställd konsultrapport. Bilaga 5 innehåller en parallelluppställning över direktivets artiklar och de bestämmelser i gällande rätt eller i utredningens författningsförslag som genomför varje artikel.

3 NIS2-direktivet

3.1 NIS-direktivet

Den 6 juli 2016 antog Europaparlamentet och rådet NIS-direktivet om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

NIS-direktivet omfattar leverantörer av samhällsviktiga tjänster inom sju sektorer: energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten och digital infrastruktur. Vidare omfattas leverantörer av vissa digitala tjänster.

Syftet med direktivet är att förbättra den inre marknadens funktion genom att skapa tillit och förtroende och att fastställa åtgärder för att uppnå en gemensam hög nivå på säkerhet i nätverks- och informationssystem inom unionen. Flera av åtgärderna syftar till att säkerställa kontinuiteten i de samhällsviktiga och digitala tjänster som omfattas av direktivet.

Direktivet innebär bland annat att leverantörer som omfattas ska vidta säkerhetsåtgärder för att hantera risker och incidenter i nätverks- och informationssystem som de är beroende av för att kunna tillhandahålla tjänsterna.

Medlemsstaterna ska enligt direktivet utse myndigheter med särskilda uppgifter, till exempel tillsynsmyndigheter, nationella kontaktpunkter och enheter för hantering av incidenter, så kallade CSIRT-enheter.

3.1.1 Gällande rätt

NIS-direktivet har i Sverige genomförts genom NIS-lagen och förordning (2018:1175) om informationssäkerhet för samhällsviktiga tjänster samt föreskrifter utfärdade av MSB, Statens energimyndighet, Transportstyrelsen, Livsmedelsverket och Post- och telestyrelsen.

Lagen (2018:1174) om samhällsviktiga och digitala tjänster

NIS-lagen ställer krav på vissa leverantörer av samhällsviktiga och digitala tjänster. Kraven innebär bland annat skyldigheter att vidta säkerhetsåtgärder och att rapportera incidenter som påverkar kontinuiteten i tjänsten.

I lagen finns bestämmelser om tillsyn. Tillsynsmyndigheten ska kunna besluta om vitesföreläggande och sanktionsavgift mot den som inte följer bestämmelserna i lagen eller i föreskrifter som meddelats med stöd av lagen. Vidare finns bestämmelser om nationell kontaktpunkt, CSIRT-enhet och ett samarbetsforum för en effektiv och likvärdig tillsyn.

I lagen bemyndigas regeringen eller den myndighet regeringen bestämmer att meddela föreskrifter bland annat om vilka tjänster som är samhällsviktiga, säkerhetsåtgärder och incidentrapportering.

Lagen trädde i kraft den 1 augusti 2018.

Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster

Förordningen kompletterar NIS-lagen och specificerar närmare de aspekter som ska beaktas av leverantörer av digitala tjänster när de hanterar risker som hotar säkerheteten i deras nät- och informationssystem samt parametrarna för fastställande av om en incident har avsevärd inverkan.

Förordningen innehåller också bemyndigande för MSB att meddela föreskrifter om vilka tjänster som är samhällsviktiga enligt NIS-lagen. Därutöver innehåller förordningen även faktorer som ska beaktas vid bedömningen av vad som avses med en betydande störning och bemyndigar MSB att meddela ytterligare föreskrifter för att precisera detta.

Vidare innehåller förordningen bestämmelser om säkerhetsåtgärder och bemyndiganden för MSB, Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Livsmedelsverket, Post- och telestyrelsen och Socialstyrelsen att meddela ytterligare föreskrifter om säkerhetsåtgärder.

Förordningen anger även vad som särskilt ska beaktas vid bedömningen av om en incident har en betydande inverkan på kontinuiteten i en samhällsviktig tjänst samt bemyndigande för MSB att meddela ytterligare föreskrifter om vad som avses med betydande inverkan.

MSB är CSIRT-enhet och ska ta emot incidentrapporter och får enligt förordningen meddela ytterligare föreskrifter om vilken information en sådan rapport ska innehålla, inom vilken tid den ska göras och de närmare formerna för rapporteringen.

MSB får också meddela föreskrifter om anmälningsskyldighet för leverantörer av samhällsviktiga tjänster. Föreskrifterna får avse när i tiden en anmälan ska ske, vilken information en anmälan ska innehålla och de närmare formerna för fullgörandet av anmälningsskyldigheten.

Vidare pekar förordningen ut vilka myndigheter som är tillsynsmyndigheter för vilka sektorer samt listar särskilda uppgifter för tillsynsmyndigheterna.

Enligt förordningen ska MSB vara nationell kontaktpunkt och leda ett samarbetsforum där tillsynsmyndigheterna och Socialstyrelsen ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn. MSB är också Sveriges representant i den samarbetsgrupp som inrättats enligt NIS-direktivet och ska tillhandahålla information om genomförandet av direktivet till kommissionen.

Myndighetsföreskrifter

MSB har meddelat följande föreskrifter och allmänna råd för leverantörer av samhällsviktiga och digitala tjänster:

- Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2021:9) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. Föreskrifterna trädde i kraft den 1 mars 2022 när MSBFS 2018:7 upphörde att gälla.

- Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.
- Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd (MSBFS 2018:9) om rapportering av incidenter för leverantörer av samhällsviktiga tjänster.
- Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd (MSBFS 2018:10) om rapportering av incidenter för leverantörer av digitala tjänster.
- Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd (MSBFS 2018:11) om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet.

Statens energimyndighet har meddelat följande föreskrifter och allmänna råd för leverantörer av samhällsviktiga tjänster inom energisektorn:

- Statens energimyndighets föreskrifter och allmänna råd (STEMFS 2021:3) om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn. Föreskrifterna trädde i kraft den 1 mars 2021.

Post- och telestyrelsen har meddelat följande föreskrifter och allmänna råd för leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur:

- Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2021:3) om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur. Föreskrifterna trädde i kraft den 1 juni 2021.

Transportstyrelsen har meddelat följande föreskrifter och allmänna råd om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom transportsektorn:

- Transportstyrelsens föreskrifter och allmänna råd (TFFS 2022:14) om säkerhetsåtgärder för leverantörer inom transportsektorn. Föreskrifterna trädde i kraft den 1 juli 2022.

Livsmedelsverket har meddelat följande föreskrifter om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn leverans och distribution av dricksvatten:

- Livsmedelsverkets föreskrifter (LIVFS 2022:2) om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn leverans och distribution av dricksvatten. Föreskrifterna trädde i kraft den 1 september 2022.

3.1.2 Gällande myndighetsstruktur och samarbete

Det svenska genomförandet av NIS-direktivet innebär alltså att uppgifter fördelats på ett flertal myndigheter. MSB är nationell kontaktpunkt och CSIRT-enhet. Myndigheten leder också ett nationellt samarbetsforum och tar emot incidentrapporter. Som framgått ovan har myndigheten även föreskriftsrätt på flera områden.

Tillsynsansvaret är fördelat enligt följande.

Tabell 3.1 Tillsyn

Sektor	Tillsynsmyndighet
Energi	Statens energimyndighet
Transporter	Transportstyrelsen
Bankverksamhet	Finansinspektionen
Finansmarknadsinfrastruktur	Finansinspektionen
Hälso- och sjukvård	Inspektionen för vård och omsorg
Leverans och distribution av dricksvatten	Livsmedelsverket
Digital infrastruktur	Post- och telestyrelsen
Digitala tjänster	Post- och telestyrelsen

Tillsynsmyndigheterna får meddela föreskrifter om säkerhetsåtgärder enligt 12–14 §§ NIS-lagen för sina respektive tillsynsområden. Socialstyrelsen får meddela sådana föreskrifter för Inspektionen för vård och omsorgs tillsynsområde. Innan föreskrifterna meddelas ska MSB ges tillfälle att yttra sig. MSB ska lämna råd och stöd till tillsynsmyndigheterna och Socialstyrelsen när de tar fram föreskrifterna.

3.2 NIS2-direktivet

3.2.1 Bakgrund och syfte

Syftet med NIS2-direktivet är att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen.

Sedan NIS-direktivet trädde i kraft har betydande framsteg gjorts för att öka unionens nivå av cyberresiliens. Trots dessa framsteg har översynen av NIS-direktivet avslöjat brister som hindrar direktivet från att effektivt hantera befintliga och framväxande utmaningar på cybersäkerhetsområdet.

Nätverks- och informationssystem har utvecklats till ett centralt inslag i vardagslivet genom den snabba digitala omställningen och sammankopplingen av samhället. Denna utveckling har lett till en utvidgad hotbild och fört med sig nya utmaningar som kräver anpassade, samordnade och innovativa svarsåtgärder i alla medlemsstater. Incidenter, som blir allt fler och mer omfattande, sofistikerade och vanliga utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Därför kan sådana incidenter hindra utövandet av ekonomisk verksamhet på den inre marknaden, generera ekonomisk förlust, undergräva användarnas förtroende och orsaka allvarlig skada för unionens ekonomi och samhälle. Beredskap och ändamålsenlighet på cybersäkerhetsområdet är därför nu viktigare än någonsin för att den inre marknaden ska fungera väl. Cybersäkerhet är dessutom en viktig förutsättning för att många kritiska sektorer ska kunna tillgodogöra sig den digitala omställningen och fullt ut utnyttja digitaliseringens ekonomiska, sociala och hållbarhetsmässiga fördelar.

De cybersäkerhetskrav som åläggs verksamhetsutövare som tillhandahåller tjänster eller utför verksamhet som är ekonomiskt betydelsefull varierar avsevärt mellan medlemsstaterna avseende typen av krav och tillsynsmetod. Dessa skillnader medför extra kostnader och gör det svårt för verksamhetsutövarna att erbjuda varor och tjänster över gränserna. Krav som ställs av en medlemsstat och som skiljer sig från, eller till och med står i strid med, krav som ställs av en annan medlemsstat kan väsentligt påverka sådan gränsöverskridande verksamhet. Det är dessutom sannolikt att otillräckligt utformade eller genomförda cybersäkerhetskrav i en medlemsstat kommer att påverka cybersäkerhetsnivån i andra medlemsstater. Översynen av NIS-direk-

tivet har också visat på stora skillnader i medlemsstaternas genomförande när det gäller dess tillämpningsområde.

Alla dessa skillnader medför en fragmentering av den inre marknaden vilket kan ha en skadlig inverkan på dess funktion och påverkar tillhandahållandet av tjänster över gränserna samt nivån av cyberresiliens. Dessa skillnader kan också leda till att vissa medlemsstater har större sårbarhet för cyberhot, med potentiella spridningseffekter i hela unionen. Direktivets mål är att undanröja dessa stora skillnader mellan medlemsstaterna, särskilt genom att föreskriva minimiregler för ett fungerande samordnat regelverk, genom att fastställa mekanismer för effektivt samarbete mellan de ansvariga myndigheterna i varje medlemsstat, genom att uppdatera vilka sektorer och verksamheter som omfattas av skyldigheter och genom att föreskriva effektiva rättsmedel och efterlevnadskontrollåtgärder.

I och med upphävandet av NIS-direktivet bör tillämpningsområdet utvidgas till en större del av ekonomin så att det ger en omfattande täckning av sektorer och tjänster som är av avgörande betydelse för viktiga samhälleliga och ekonomiska verksamheter på den inre marknaden. (artikel 1.1 och skäl 2–6).

3.2.2 Tillämpningsområde och förteckning

Direktivet är tillämpligt på offentliga eller privata verksamhetsutövare av den typ som avses i direktivets bilaga 1 eller 2 och som betecknas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG eller överstiger de trösklar för medelstora företag som avses i punkt 1 i den artikeln och som tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen. Verksamhetsutövarna finns inom 18 sektorer som delas upp i högkritiska och andra kritiska sektorer. De högkritiska sektorerna är följande:

- Energi, med delsektorerna elektricitet, fjärrvärme eller fjärrkyla, olja, gas och vätgas
- Transporter, med delsektorerna lufttransport, järnvägstransport, sjöfart och vägtransport
- Bankverksamhet
- Finansmarknadsinfrastruktur

- Hälso- och sjukvårdssektorn
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av IKT-tjänster (mellan företag)
- Offentlig förvaltning
- Rymden

Till detta kommer de andra kritiska sektorerna som är:

- Post- och budtjänster
- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning, med delsektorerna
  - tillverkning av medicintekniska produkter och medicintekniska produkter för *in vitro*-diagnostik
  - tillverkning av datorer, elektronikvaror och optik
  - tillverkning av elapparatur
  - tillverkning av övriga maskiner
  - tillverkning av motorfordon, släpfordon och påhängsvagnar
  - tillverkning av andra transportmedel
- Digitala leverantörer
- Forskning

Oavsett verksamhetsutövarnas storlek är direktivet också tillämpligt på verksamhetsutövare av en typ som avses i bilaga 1 eller 2 i följande fall:

- Om tjänster tillhandahålls av
  - tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster,
  - tillhandahållare av betrodda tjänster,
  - registreringsenheter för toppdomäner och leverantörer av domännamnssystemtjänster.
- Om verksamhetsutövaren är den enda leverantören i en medlemsstat av en tjänst som är väsentlig för att upprätthålla kritisk eller samhällelig eller ekonomisk verksamhet.
- Om en störning av den tjänst som verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa.
- Om en störning av den tjänst som verksamhetsutövaren tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser.
- Verksamhetsutövaren är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer i medlemsstaten som är beroende av denna verksamhetsutövare.
- Om verksamhetsutövaren är en offentlig förvaltningsenhet
  - på statlig nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, eller
  - på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, som enligt en riskbaserad bedömning tillhandahåller tjänster vars störning kan ha betydande effekt på kritisk samhällelig eller ekonomisk verksamhet.

Oavsett verksamhetsutövarnas storlek är direktivet också tillämpligt på verksamhetsutövare som identifierats som kritiska verksamhetsutövare enligt CER-direktivet och på verksamhetsutövare som tillhandahåller domännamnsregistreringstjänster.

Medlemsstaterna får föreskriva att direktivet även ska tillämpas på offentliga förvaltningsenheter på lokal nivå och utbildningsinstitut, särskilt om de utför kritisk forskningsverksamhet.

Direktivet påverkar inte medlemsstaternas ansvar för att skydda nationell säkerhet och deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning.

Direktivet är inte tillämpligt på offentliga verksamhetsutövare som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott. Medlemsstaterna får undanta särskilda verksamhetsutövare som bedriver verksamhet på dessa områden, eller som uteslutande tillhandahåller tjänster till en offentlig verksamhetsutövare som bedriver verksamhet på dessa områden, från skyldigheterna rörande riskhantering och rapportering med avseende på sådan verksamhet eller sådana tjänster. I sådana fall ska inte heller tillsyns- och efterlevnadskontrollåtgärder tillämpas på denna specifika verksamhet eller dessa specifika tjänster. Om verksamhetsutövarna bedriver verksamhet uteslutande på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning får medlemsstaten besluta att befria dessa verksamhetsutövare också från skyldigheterna om registrering.

Om det i sektorsspecifika unionsrättsakter föreskrivs att verksamhetsutövare ska anta riskhanteringsåtgärder för cybersäkerhet eller underrätta om betydande incidenter, och dessa krav har minst samma verkan, ska de relevanta bestämmelserna i NIS2-direktivet inte tillämpas på sådana verksamhetsutövare.

Verksamhetsutövare som omfattas av direktivet ska delas upp i väsentliga och viktiga verksamhetsutövare. Följande verksamhetsutövare är enligt direktivet väsentliga:

- Verksamhetsutövare av en typ som avses i bilaga 1 och som överstiger trösklarna för medelstora företag.
- Kvalificerade tillhandahållare av betrodda tjänster och registreringsenheter för toppdomäner samt leverantörer av DNS-tjänster, oavsett storlek.
- Tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som betraktas som medelstora företag.

- Offentliga verksamhetsutövare på statlig nivå.
- Alla andra verksamhetsutövare av en typ som avses i bilaga 1 eller 2 som av en medlemsstat identifierats som väsentliga.
- Verksamhetsutövare som identifierats som kritiska verksamhetsutövare enligt CER-direktivet.
- Verksamhetsutövare som medlemsstaterna före den 16 januari 2023 har identifierat som leverantörer av samhällsviktiga tjänster enligt NIS-direktivet, om så föreskrivs av medlemsstaten.

Alla verksamhetsutövare av en typ som avses i bilaga 1 eller 2 och som inte är väsentliga ska betraktas som viktiga verksamhetsutövare. Detta inkluderar verksamhetsutövare som en medlemsstat identifierat som viktiga i enlighet med artikel 2.2 b–e.

Senast den 17 april 2025 ska medlemsstaterna upprätta en förteckning över väsentliga och viktiga verksamhetsutövare samt verksamhetsutövare som tillhandahåller domännamnsregistreringstjänster. Medlemsstaterna ska regelbundet och minst vartannat år se över förteckningen och när det är lämpligt uppdatera den. Medlemsstaterna får inrätta nationella mekanismer som gör det möjligt för verksamhetsutövarna att registrera sig själva.

Senast den 17 april 2025 och därefter vartannat år ska de behöriga myndigheterna underrätta kommissionen och samarbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare för varje sektor och delsektor och lämna relevant information om väsentliga och viktiga verksamhetsutövare som identifierats oavsett storlek (artikel 2–4).

3.2.3 Behöriga myndigheter och gemensamma kontaktpunkter

Varje medlemsstat ska utse en eller flera behöriga myndigheter med ansvar för cybersäkerhet och tillsyn. De behöriga myndigheterna ska övervaka genomförandet av direktivet på nationell nivå. Varje medlemsstat ska också utse en gemensam kontaktpunkt. Den ska utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och myndigheter i andra medlemsstater och, när det är lämpligt, kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa). Den behöriga myndig-

heten ska också säkerställa ett sektorsövergripande samarbete med andra behöriga myndigheter i medlemsstaten (artikel 8).

3.2.4 Cyberkrishanteringsmyndighet

Varje medlemsstat ska utse en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter). Om en medlemsstat utser mer än en cyberkrishanteringsmyndighet ska den ange vilken av dessa myndigheter som ska samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Enligt direktivet ska medlemsstaten även anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser där mål och villkor för hanteringen av sådana incidenter och kriser fastställs. Utformningen av den nationella planen omfattas enligt kommittédirektivet inte av utredarens uppdrag (artikel 9).

3.2.5 CSIRT-enheter

Medlemsstaterna bör ha både den tekniska och organisatoriska kapaciteten som krävs för att förebygga, upptäcka, vidta åtgärder mot och begränsa incidenter och risker. Varje medlemsstat ska därför utse en eller flera CSIRT-enheter. I direktivet ställs uttryckliga krav som CSIRT-enheter ska uppfylla. Direktivet anger också ett antal uppgifter för CSIRT-enheter. Medlemsstaterna ska säkerställa att deras CSIRT-enheter har nödvändig kapacitet att utföra dessa uppgifter och att tillräckliga resurser anslås för att säkerställa en tillräcklig personalstyrka för att göra det möjligt för CSIRT-enheterna att utveckla sin tekniska kapacitet (artikel 10 och 11).

Varje medlemsstat ska utse en av sina CSIRT-enheter till samordnare för den samordnade delgivningen av information om sårbarheter. Den CSIRT-enhet som utsetts till samordnare ska fungera som betrodd mellanhand och vid behov underlätta interaktionen mellan den som rapporterar en sårbarhet och tillverkaren eller leverantören av de potentiellt sårbara produkterna eller tjänsterna (artikel 12).

3.2.6 Samarbete på nationell nivå

Om den behöriga myndigheten, den gemensamma kontaktpunkten och CSIRT-enheten i en medlemsstat är separata ska de samarbeta när det gäller fullgörandet av skyldigheterna enligt direktivet. Medlemsstaterna ska säkerställa att antingen CSIRT-enheten eller de behöriga myndigheterna tar emot underrättelser om incidenter, cyberhot och tillbud som lämnas enligt direktivet. Den gemensamma kontaktpunkten ska informeras om de underrättelser som lämnas in. Medlemsstaterna ska också säkerställa att de behöriga myndigheterna, CSIRT-enheterna och den gemensamma kontaktpunkten samarbetar med bland annat brottsbekämpande myndigheter, dataskyddsmyndigheter och behöriga myndigheter enligt andra sektorsspecifika unionsrättsakter (artikel 13).

3.2.7 Samarbetsgrupp för strategiskt samarbete och informationsutbyte

Genom NIS-direktivet inrättades en samarbetsgrupp för att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna och skapa förtroende och tillit. Samarbetsgruppen utökas i NIS2-direktivet genom att fler aktörer har möjlighet att delta i samarbetsgruppen som dessutom får fler uppgifter som återges i artikel 14.

3.2.8 CSIRT-nätverk

Genom NIS-direktivet inrättades ett nätverk för nationella CSIRT-enheter för att bidra till utvecklingen av förtroende och tillit och för att främja ett snabbt och ändamålsenligt operativt samarbete i unionen. Nätverket ska enligt NIS2-direktivet i princip fortsätta att fungera på samma sätt men får en del nya uppgifter, till exempel att samarbeta och utbyta information med säkerhetscentrum (SOC) på regional och unionsnivå (artikel 15).

3.2.9 Det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe)

EU-CyCLONe inrättas för att stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser och säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer. En storskalig cybersäkerhetsincident definieras i direktivet som en incident som orsakar störningar som är så omfattande att den berörda medlemsstaten inte kan hantera den eller som har en betydande påverkan på minst två medlemsstater. EU-CyCLONe ska bestå av företrädare för medlemsstaternas cyberkrishanteringsmyndigheter och i vissa fall kommissionen. EU-CyCLONe ska bland annat öka beredskapen för hantering av storskaliga cybersäkerhetsincidenter och kriser samt samordna hanteringen och ge stöd till beslutsfattande på politisk nivå i samband med sådana incidenter och kriser (artikel 16).

3.2.10 Styrning

Medlemsstaterna ska säkerställa att väsentliga och viktiga verksamhetsutövares ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som verksamhetsutövaren vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för överträdelser av den artikeln. Medlemsstaterna ska också säkerställa att medlemmar i ledningsorganen är skyldiga att genomgå utbildning, och ska uppmuntra verksamhetsutövare att regelbundet erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på verksamhetsutövarens tjänster (artikel 20).

3.2.11 Riskhanteringsåtgärder för cybersäkerhet

Medlemsstaterna ska säkerställa att de väsentliga och viktiga verksamhetsutövare som beskrivits i avsnitt 3.2.2 vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhanda-

hålla sina tjänster. Åtgärderna ska också vidtas för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken. Åtgärderna ska baseras på en allriskansats som syftar till att skydda verksamhetsutövarens nätverks- och informationssystem och dessa systems fysiska miljö från incidenter och minst inbegripa

- strategier för riskanalys och informationssystemens säkerhet,
- incidenthantering,
- driftskontinuitet,
- säkerhet i leveranskedjan,
- säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem,
- strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,
- grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,
- strategier och förfaranden för användning av kryptografi,
- personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning, och
- användning av, när så är lämpligt, lösningar för multifaktorsautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.

Medlemsstaterna ska säkerställa att verksamhetsutövare beaktar de sårbarheter som är specifika för varje direktleverantör och tjänsteleverantör och den övergripande kvaliteten på deras leverantörers och tjänsteleverantörers produkter och cybersäkerhetspraxis. Medlemsstaterna ska också säkerställa att verksamhetsutövare är skyldiga att beakta resultatet av de samordnade säkerhetsbedömningar säkerhetsriskbedömningar av kritiska leveranskedjor som utförs i enlighet med direktivet.

Kommissionen ska senast den 17 oktober 2024 anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna för åtgärderna ovan när det gäller vissa verksamhetsutövare.[1] Kommissionen får även anta genomförandeakter för att fastställa tekniska och metodologiska krav samt, vid behov, sektorskrav med avseende på andra verksamhetsutövare (artikel 21).

3.2.12 Rapporteringsskyldigheter

Varje medlemsstat ska säkerställa att väsentliga och viktiga verksamhetsutövare utan onödigt dröjsmål underrättar sin CSIRT-enhet eller behöriga myndighet om alla incidenter som har en betydande inverkan på tillhandahållandet av deras tjänster (betydande incident). En incident ska anses vara betydande om den har orsakat eller kan orsaka allvarliga driftstörningar för tjänsterna, ekonomiska förluster för den berörda verksamhetsutövaren eller har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

Enligt direktivet ska verksamhetsutövarna utan onödigt dröjsmål, men senast inom 24 timmar efter att ha fått kännedom om den betydande incidenten, lämna en *tidig varning* som ska ange om incidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller kan ha gränsöverskridande verkningar. Utan onödigt dröjsmål men senast inom 72 timmar ska verksamhetsutövaren sedan lämna en *incidentanmälan* som ska innehålla en inledande bedömning av incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer. Senast en månad efter inlämningen av incidentanmälan ska en *slutrapport* lämnas. Slutrapporten ska enligt direktivet innehålla en detaljerad beskrivning av incidenten, den typ av hot eller grundorsak som sannolikt har utlöst incidenten, tillämpade och pågående begränsande åtgärder samt incidentens gränsöverskridande verkningar.

[1] Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer och för plattformar för sociala nätverkstjänster samt kvalificerade tillhandahållare av betrodda tjänster.

CSIRT-enheten eller den behöriga myndigheten ska utan onödigt dröjsmål och om möjligt inom 24 timmar från mottagandet av en tidig varning lämna ett svar till den rapporterande verksamhetsutövaren, inbegripet initial återkoppling om incidenten och, på verksamhetsutövarens begäran, vägledning eller operativa råd om genomförandet av möjliga begränsande åtgärder. CSIRT-enheten ska tillhandahålla ytterligare tekniskt stöd om den berörda verksamhetsutövaren begär det. Om incidenten misstänks vara av brottslig art ska CSIRT-enheten eller den behöriga myndigheten också tillhandahålla vägledning om rapportering av incidenten till de brottsbekämpande myndigheterna.

När så är lämpligt, och särskilt om incidenten berör två eller flera medlemsstater, ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten utan dröjsmål informera andra berörda medlemsstater och Enisa om incidenten. Vid en sådan underrättelse ska verksamhetsutövarens säkerhets- och affärsintressen samt informationens konfidentialitet bevaras, i enlighet med unionsrätten eller nationell rätt.

På begäran av CSIRT-enheten eller den behöriga myndigheten ska den gemensamma kontaktpunkten vidarebefordra incidentrapporter till de gemensamma kontaktpunkterna i andra berörda medlemsstater.

Den gemensamma kontaktpunkten ska var tredje månad lämna en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud som rapporterats enligt direktivet.

CSIRT-enheterna eller, i tillämpliga fall, de behöriga myndigheterna ska förse de behöriga myndigheterna enligt CER-direktivet med information om rapportering som gjorts av verksamhetsutövare som identifierats som kritiska i enlighet med CER-direktivet.

Kommissionen får anta genomförandeakter som närmare anger typen av information i och formatet och förfarandet för underrättelser som lämnas enligt direktivet.

Senast den 17 oktober 2024 ska kommissionen, med avseende på vissa verksamhetsutövare[2] anta genomförandeakter som närmare anger i vilka fall en incident ska anses vara betydande enligt direktivet. Kommissionen får även anta sådana genomförandeakter med avseende på andra väsentliga och viktiga verksamhetsutövare (artikel 23).

[2] Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer eller av plattformar för sociala nätverkstjänster.

3.2.13 Cybersäkerhetscertifiering och standardisering

Medlemsstaterna får ålägga väsentliga och viktiga verksamhetsutövare att använda särskilda IKT-produkter, IKT-tjänster och IKT-processer, som har utvecklats av den väsentliga eller viktiga verksamhetsutövaren eller upphandlats från tredje parter, som är certifierade enligt europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med cybersäkerhetsakten[3]. Medlemsstaterna ska dessutom uppmuntra väsentliga och viktiga verksamhetsutövare att använda kvalificerade betrodda tjänster. Kommissionen får anta delegerade akter som anger vilka kategorier av väsentliga eller viktiga verksamhetsutövare som ska vara skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhålla ett certifikat enligt en ordning för cybersäkerhetscertifiering som antagits enligt cybersäkerhetsakten.

Medlemsstaterna ska, utan att föreskriva eller gynna användning av viss typ av teknik, uppmuntra användningen av europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem (artikel 24 och 25).

3.2.14 Arrangemang för informationsutbyte om cybersäkerhet

Medlemsstaterna ska säkerställa att det är möjligt för verksamhetsutövare att på frivillig basis utbyta relevant information om cybersäkerhet om sådant informationsutbyte syftar till att förebygga, upptäcka, reagera på eller återhämta sig från incidenter, begränsa deras inverkan eller höja cybersäkerhetsnivån. Medlemsstaterna ska underlätta inrättandet av sådana arrangemang för informationsutbyte. Medlemsstaterna ska också säkerställa att väsentliga och viktiga verksamhetsutövare underrättar de behöriga myndigheterna om sitt deltagande i sådana arrangemang (artikel 29).

[3] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

3.2.15 Tillsyn och efterlevnadskontroll

Medlemsstaterna ska säkerställa att deras behöriga myndigheter på ett ändamålsenligt sätt övervakar och vidtar de åtgärder som krävs för att säkerställa att direktivet efterlevs. Medlemsstaterna får tillåta sina behöriga myndigheter att prioritera sin tillsyn utifrån en riskbaserad metod. De behöriga myndigheterna ska ha ett nära samarbete med tillsynsmyndigheterna för dataskyddsförordningen[4] när de behandlar incidenter som medför personuppgiftsincidenter.

Tillsyns- och efterlevnadskontroller i fråga om väsentliga verksamhetsutövare

Medlemsstaterna ska säkerställa att de tillsyns- eller efterlevnadskontroller som åläggs väsentliga verksamhetsutövare är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall. Medlemsstaterna ska säkerställa att behöriga myndigheter, när de utövar sina tillsynsuppgifter, har befogenhet att åtminstone underställa dessa verksamhetsutövare

- inspektioner på plats och distansbaserad tillsyn,
- regelbundna och riktade säkerhetsrevisioner,
- ad hoc-revisioner,
- säkerhetsskanningar,
- begäranden om sådan information som behövs för att bedöma de riskhanteringsåtgärder för cybersäkerhet som antagits av verksamhetsutövaren,
- begäranden om tillgång till uppgifter, handlingar och information som behövs för att de ska kunna utföra sina tillsynsuppgifter, och
- begäranden om bevis på genomförandet av cybersäkerhetsstrategier.

[4] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Kostnaderna för riktade säkerhetsrevisioner som utförs av ett oberoende organ ska betalas av verksamhetsutövaren, om inte den behöriga myndigheten beslutar något annat.

Medlemsstaterna ska vidare säkerställa att behöriga myndigheter, när de utövar efterlevnadskontroll, åtminstone har befogenhet att

- utfärda varningar,
- anta bindande instruktioner,
- ålägga de berörda verksamhetsutövarna att upphöra med och att avstå från att upprepa beteenden som utgör en överträdelse av direktivet,
- ålägga de berörda verksamhetsutövarna att säkerställa riskhanteringsåtgärder och incidentrapportering överensstämmer med direktivet,
- ålägga de berörda verksamhetsutövarna att informera de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller utför verksamheter som potentiellt kan beröras av ett betydande cyberhot om hotets karaktär och om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa kan vidta som svar på hotet,
- ålägga de berörda verksamhetsutövarna att genomföra rekommendationer som lämnats till följd av en säkerhetsrevision,
- utse en övervakningsansvarig för att övervaka att verksamhetsutövaren efterlever skyldigheter om riskhanteringsåtgärder och incidentrapportering,
- ålägga de berörda verksamhetsutövarna att offentliggöra aspekter av överträdelser av direktivet, och
- påföra eller begära att relevanta organ eller domstolar i enlighet med nationell rätt påför administrativa sanktionsavgifter.

Om efterlevnadskontrollåtgärderna är ineffektiva ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenhet att fastställa en tidsfrist inom vilken en väsentlig verksamhetsutövare ska vidta nödvändiga åtgärder för att avhjälpa bristerna. Om de begärda åtgärderna inte vidtas inom den fastställda tidsfristen ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenhet att

- tillfälligt upphäva eller begära att ett certifierings- eller auktorisationsorgan, eller en domstol, i enlighet med nationell rätt, tillfälligt upphäver en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls eller verksamheter som utövas av verksamhetsutövaren,
- begära att relevanta organ eller domstolar, i enlighet med nationell rätt, inför ett tillfälligt förbud för varje fysisk person som på nivån verkställande direktör eller juridiskt ombud har ledningsansvar i verksamhetsutövaren att utöva ledningsfunktioner.

Tillfälliga upphävanden och förbud är inte tillämpliga på offentliga verksamhetsutövare som omfattas av direktivet.

Medlemsstaterna ska säkerställa att varje fysisk person som ansvarar för eller agerar som juridiskt ombud för en verksamhetsutövare har befogenhet att säkerställa att verksamhetsutövaren efterlever direktivet. Medlemsstaterna ska också säkerställa att dessa fysiska personer kan hållas ansvariga för överträdelser av sitt uppdrag att säkerställa att direktivet efterlevs. När det gäller offentliga verksamhetsutövare påverkar detta inte nationell rätt avseende det ansvar som åligger statligt anställda och valda eller utnämnda tjänstepersoner.

Medlemsstaterna ska säkerställa att deras behöriga myndigheter informerar relevanta behöriga myndigheter enligt CER-direktivet när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll mot en verksamhetsutövare som identifierats som en kritisk verksamhetsutövare enligt det direktivet (artikel 32).

Tillsyns och efterlevnadskontroller i fråga om viktiga verksamhetsutövare

När medlemsstaterna får bevis, indikationer på eller information om att en viktig verksamhetsutövare påstås underlåta att fullgöra direktivet ska de säkerställa att de behöriga myndigheterna vid behov vidtar åtgärder i form av tillsynsåtgärder i efterhand. Medlemsstaterna ska säkerställa att dessa åtgärder är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de utövar sina tillsynsuppgifter avseende viktiga verksamhetsutövare, har i princip samma befogenheter som de har gällande väsentliga

verksamhetsutövare, med skillnaden att tillsyn ska ske i efterhand. Medlemsstaterna ska också säkerställa att de behöriga myndigheterna har i stora delar samma befogenheter när det gäller efterlevnadskontroll som de har gällande väsentliga verksamhetsutövare. Dock finns inte bestämmelser om möjlighet att utse en övervakningsansvarig när det gäller viktiga verksamhetsutövare. Det finns inte heller bestämmelser om att upphäva certifiering eller auktorisation eller införa förbud för personer att utöva ledningsansvar (artikel 33).

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella åtgärder som antagits enligt direktivet och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska anmäla dessa regler och åtgärder till kommissionen senast den 17 januari 2025.

Medlemsstaterna ska säkerställa att väsentliga verksamhetsutövare som överträder artikel 21 eller 23 påförs administrativa sanktionsavgifter på högst 10 000 000 euro eller högst 2 procent av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den väsentliga verksamhetsutövaren tillhör, beroende på vilken siffra som är högst.

Medlemsstaterna ska säkerställa att viktiga verksamhetsutövare som överträder artikel 21 eller 23 påförs administrativa sanktionsavgifter på högst 7 000 000 euro eller högst 1,4 procent av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den viktiga verksamhetsutövaren tillhör, beroende på vilken siffra som är högst.

Medlemsstaterna får föreskriva befogenhet att förelägga viten för att tvinga en verksamhetsutövare att upphöra med en överträdelse av direktivet.

Medlemsstaterna får också fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga verksamhetsutövare. Kommissionen ska underrättas om lagar som medlemsstaten antar gällande administrativa sanktionsavgifter senast den 17 oktober 2024 (artikel 34 och 36).

4 Beskrivning av de nya sektorerna

4.1 Inledning

NIS2-direktivet innebär som framgått ovan att tillämpningsområdet utvidgas i jämförelse med det första NIS-direktivet. Ett flertal nya sektorer har tillkommit och inom befintliga sektorer har nya delsektorer samt nya typer av verksamhetsutövare lagts till. Nedan följer en beskrivning av de nya sektorer, delsektorer och typer av verksamhetsutövare som omfattas av NIS2-direktivets tillämpningsområde. Leverantörer av molntjänster, marknadsplatser online och sökmotorer var enligt NIS1-direktivet digitala tjänster. Dessa beskrivs nedan under den sektor de tillhör i NIS2-direktivet. För en beskrivning av övriga verksamhetsutövare se SOU 2017:36.[1] Medlemsstaterna får föreskriva att direktivet ska tillämpas på utbildningsinstitut vilket utredningen behandlar i avsnitt 5.2.14.

NIS2-direktivets bilaga 1 och 2 innehåller en omfattande uppräkning av sektorer, delsektorer och verksamhetsutövare. I många fall hänvisas till andra EU-rättsakter där ytterligare definitioner finns. I andra fall finns definitionen endast i NIS2-direktivet. Detta innebär att det i vissa sektorer kan finnas ett tolkningsutrymme för vilken typ av verksamhetsutövare som faktiskt omfattas i sektorn eller delsektorn. Utredningen återkommer till detta i avsnitt 5.2.12.

[1] SOU 2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, s. 65 ff.

4.2 Energi

Elektricitet

- Producenter enligt definitionen i artikel 2.38 i direktiv (EU) 2019/944[2].

Med producent avses en fysisk eller juridisk person som framställer el.

- Nominerade elmarknadsoperatörer enligt definitionen i artikel 2.8 i Europaparlamentets och rådets förordning (EU) 2019/943[3].

Med nominerad elmarknadsoperatör avses en marknadsoperatör som av den behöriga myndigheten utsetts att utföra arbetsuppgifter i samband med gemensam dagen före- eller intradagskoppling.

- Marknadsaktörer enligt definitionen i artikel 2.25 i förordning (EU) 2019/943 och som tillhandahåller aggregering, efterfrågeflexibilitet eller energilagringstjänster enligt definitionen i artikel 2.18, 2.20 och 2.59 i direktiv (EU) 2019/944.

Med marknadsaktör avses en fysisk eller juridisk person som producerar, köper eller säljer el, efterfrågeflexibilitet eller lagringstjänster, inklusive lägger handelsorder, på en eller flera elmarknader, däribland energibalansmarknader.

Aggregering avser en funktion som fullgörs av en fysisk eller juridisk person som kombinerar flera kundlaster eller producerad el för försäljning, inköp eller auktionering på alla slags organiserade elmarknader.

Med efterfrågeflexibilitet avses förändringar i belastningen i fråga om el från slutkunder, jämfört med deras normala eller nuvarande konsumtionsmönster, som svar på marknadssignaler, inbegripet som svar på tidsvarierande elpriser eller ekonomiska incitament, eller som svar på antagandet av slutkundens bud om att sälja efterfrågeminskning eller ökning till ett visst pris på organiserade marknader enligt definitionen i artikel 2.4 i kommissionens genomförandeförordning (EU) nr 1348/2014, enskilt eller genom aggregering.

[2] Europaparlamentets och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU.
[3] Europaparlamentets och rådets förordning (EU) 2019/943 av den 5 juni 2019 om den inre marknaden för el.

Energilagring innebär i elsystemet en uppskjutning av den slutliga användningen av el till en senare tidpunkt än produktionstillfället, eller omvandlingen av elenergi till en form av energi som kan lagras, lagringen av den energin, och den därpå följande återomvandlingen av den energin till elenergi eller användningen som en annan energibärare.

- Laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt och som tillhandahåller en laddningstjänst till slutanvändare, även när detta utförs på uppdrag av en leverantör av mobilitetstjänster och i dess namn.

Fjärrvärme eller fjärrkyla

- Operatörer av fjärrvärme eller fjärrkyla enligt definitionen i artikel 2.19 i Europaparlamentets och rådets direktiv (EU) 2018/2001[4].

Med fjärrvärme eller fjärrkyla avses distribution av värmeenergi i form av ånga, hetvatten eller kylda vätskor från centrala eller decentraliserade produktionskällor, via ett nät, till flera byggnader eller anläggningar i syfte att värma eller kyla ner utrymmen eller processer.

Olja

- Centrala lagringsenheter enligt definitionen i artikel 2 f i rådets direktiv 2009/119/EG[5].

Med central lagringsenhet (CSE) avses organ eller tjänst som anförtrotts uppgiften att förvärva, vidmakthålla eller sälja oljelager, inbegripet beredskapslager och särskilda lager.

[4] Europaparlamentets och rådets direktiv (EU) 2018/2001 av den 11 december 2018 om främjande av användningen av energi från förnybara energikällor.
[5] Rådets direktiv 2009/119/EG av den 14 september 2009 om skyldighet för medlemsstaterna att inneha minimilager av råolja och/eller petroleumprodukter.

Vätgas

- Operatörer av anläggningar för produktion, lagring och överföring av vätgas.

4.3 Hälso- och sjukvårdssektorn

- EU-referenslaboratorier som avses i artikel 15 i Europaparlamentets och rådets förordning (EU) 2022/2371[6].

Med EU-referenslaboratorier avses de EU-referenslaboratorier som kommissionen enligt förordningen, genom genomförandeakter, får utse och som ska ge stöd till nationella referenslaboratorier för att främja god praxis och medlemsstaternas frivilliga harmonisering av diagnostik, testmetoder och användning av vissa tester för medlemsstaternas enhetliga övervakning, anmälan och rapportering av sjukdomar.

- Verksamhetsutövare som bedriver forskning och utveckling avseende läkemedel enligt definitionen i artikel 1.2 i Europaparlamentets och rådets direktiv 2001/83/EG[7].

Med läkemedel avses varje substans eller kombination av substanser som tillhandahålls för att behandla eller förebygga sjukdom hos människor och varje substans eller kombination av substanser som är avsedd att tillföras människor i syfte att ställa diagnos eller att återställa, korrigera eller modifiera fysiologiska funktioner.

- Verksamhetsutövare som tillverkar farmaceutiska basprodukter och läkemedel som avses i avsnitt C huvudgrupp 21 i Nace Rev. 2.

Tillverkning av farmaceutiska basprodukter avser bland annat tillverkning av medicinskt aktiva substanser som används i tillverkningen av läkemedel, till exempel antibiotika.

Tillverkning av läkemedel avser bland annat tillverkning av immunsera, preventivmedel och vacciner.

[6] Europaparlamentets och rådets förordning (EU) 2022/2371 av den 23 november 2022 om allvarliga gränsöverskridande hot mot människors hälsa och om upphävande av beslut nr 1082/2013/EU.
[7] Europaparlamentets och rådets direktiv 2001/83/EG av den 6 november 2001 om upprättande av gemenskapsregler för humanläkemedel.

- Verksamhetsutövare som tillverkar medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan i den mening som avses i artikel 22 i Europaparlamentets och rådets förordning (EU) 2022/123[8].

Efter det att ett hot mot folkhälsan erkänts enligt förordningen ska det upprättas en förteckning över kategorier av kritiska medicintekniska produkter som betraktas som kritiska under hotet mot folkhälsan. Europeiska läkemedelsmyndigheten ska i samband med detta offentliggöra förteckningen på en särskild sida på sin webbportal.

4.4 Avloppsvatten

- Företag som samlar ihop, släpper ut och renar avloppsvatten från tätbebyggelse, hushållsspillvatten eller industrispillvatten enligt definitionen i artikel 2.1–2.3 i rådets direktiv 91/271/EEG[9], undantaget företag som samlar ihop, släpper ut eller renar avloppsvatten från tätbebyggelse, hushållsspillvatten eller industrispillvatten som en icke väsentlig del av sin allmänna verksamhet.

Med avloppsvatten från tätbebyggelse avses spillvatten från hushåll eller en blandning av hushållsspillvatten och industrispillvatten eller dagvatten.

Hushållsspillvatten avser spillvatten från bostäder och serviceinrättningar, vilket till övervägande del härrör från människans metabolism och hushållsaktiviteter. Med industrispillvatten avses allt spillvatten som släpps ut från områden som används för kommersiell eller industriell verksamhet och som inte är hushållsspillvatten eller dagvatten.

[8] Europaparlamentets och rådets förordning (EU) 2022/123 av den 25 januari 2022 om en förstärkt roll för Europeiska läkemedelsmyndigheten vid krisberedskap och krishantering avseende läkemedel och medicintekniska produkter.
[9] Rådets direktiv 91/271/EEG av den 21 maj 1991 om rening av avloppsvatten från tätbebyggelse.

4.5 Digital infrastruktur

- Leverantörer av molntjänster.

Molntjänst avser en digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma beräkningstjänster, inbegripet när sådana resurser är distribuerade på flera platser.

- Leverantörer av datacentraltjänster.

Datacentraltjänst avser en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll.

- Leverantörer av nätverk för leverans av innehåll.

Nätverk för leverans av innehåll avser ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för, tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning.

- Tillhandahållare av betrodda tjänster.

Betrodd tjänst avser enligt NIS2-direktivet en betrodd tjänst enligt definitionen i artikel 3.16 i förordning (EU) nr 910/2014[10]. I den förordningen definieras betrodd tjänst som en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av

– skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller

– skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller

[10] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

– bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster.

- Tillhandahållare av allmänna elektroniska kommunikationsnät.

Allmänna elektroniska kommunikationsnät avser enligt NIS2-direktivet ett allmänt elektroniskt kommunikationsnät enligt definitionen i artikel 2.8 i direktiv (EU) 2018/1972[11]. I det direktivet definieras allmänt elektroniskt kommunikationsnät som ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stöder informationsöverföring mellan nätanslutningspunkter.

- Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster.

Allmänt tillgängliga elektroniska kommunikationstjänster avser enligt NIS2-direktivet en elektronisk kommunikationstjänst enligt definitionen i artikel 2.4 i direktiv (EU) 2018/1972. I det direktivet definieras en elektronisk kommunikationstjänst som en tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som omfattar, med undantag av tjänster i form av tillhandahållande av innehåll som överförts med hjälp av elektroniska kommunikationsnät och kommunikationstjänster eller utövande av redaktionellt ansvar över sådant innehåll, följande typer av tjänster:

– internetanslutningstjänst enligt definitionen i artikel 2.2 i förordning (EU) 2015/2120[12],

– interpersonell kommunikationstjänst, och

– tjänster som helt eller huvudsakligen utgörs av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin till maskin-tjänster och för utsändningstjänster.

[11] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.
[12] Europaparlamentets och rådets förordning (EU) 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster och förordning (EU) nr 531/2012 om roaming i allmänna mobilnät i unionen.

4.6 Förvaltning av IKT-tjänster (mellan företag)

IKT-tjänst avser enligt NIS2-direktivet en IKT-tjänst enligt definitionen i förordning (EU) 2019/881[13]. I den förordningen definieras IKT-tjänst som en tjänst som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via nätverks- och informationssystem.

- Leverantörer av hanterade tjänster.

Leverantör av hanterade tjänster definieras i NI2-direktivet som en verksamhetsutövare som tillhandahåller tjänster som rör installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans.

- Leverantörer av hanterade säkerhetstjänster.

Leverantör av hanterade säkerhetstjänster definieras i NIS2-direktivet som en leverantör av hanterade tjänster som utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker.

4.7 Offentlig förvaltning

- Offentliga förvaltningsentiteter hos nationella regeringar såsom de definieras av en medlemsstat i enlighet med nationell rätt.
- Offentliga förvaltningsentiteter på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt.

Offentlig förvaltningsentitet avser enligt NIS2-direktivet en entitet som erkänts som sådan i en medlemsstat i enlighet med nationell rätt, med undantag för rättsväsendet, parlamentet och centralbanker, som uppfyller följande kriterier:

[13] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

a) Den har inrättats för att tillgodose behov i det allmännas intresse och har inte industriell eller kommersiell karaktär.

b) Den har ställning som juridisk person eller har lagstadgad rätt att agera för en annan entitet som har ställning som juridisk person.

c) Den finansieras till största delen av staten, regionala myndigheter eller andra offentligrättsliga organ, står under administrativ tillsyn av dessa myndigheter eller organ, eller har ett förvaltnings-, lednings- eller kontrollorgan där mer än hälften av ledamöterna utses av staten, regionala myndigheter eller andra offentligrättsliga organ.

d) Den har befogenhet att rikta administrativa eller reglerande beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.

Medlemsstaterna får föreskriva att direktivet även ska tillämpas på offentliga förvaltningsentiteter på lokal nivå.

Se vidare om offentliga förvaltningsentiteter i avsnitt 5.2.

4.8 Rymden

- Operatörer av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter och som stöder tillhandahållandet av rymdbaserade tjänster, undantaget tillhandahållare av allmänna elektroniska kommunikationsnät.

NIS2-direktivet innehåller ingen ytterligare definition av rymdbaserade tjänster. En tolkning av ordalydelsen innebär enligt utredningen att rymdbaserade tjänster avser bland annat satellitkommunikation, positionerings- och tidstjänster samt jordobservation.

4.9 Post- och budtjänster

- Tillhandahållare av posttjänster enligt definitionen i artikel 2.1a i direktiv 97/67/EG[14], inbegripet tillhandahållare av budtjänster.

Med posttjänster avses tjänster som innefattar insamling, sortering, transport och utdelning av postförsändelser.

Med postförsändelser avses adresserad försändelse i den slutliga form i vilken den ska transporteras av en tillhandahållare av posttjänster. Sådana försändelser omfattar, förutom brevförsändelser, till exempel böcker, kataloger, tidningar och tidskrifter samt postpaket som innehåller varor med eller utan kommersiellt värde.

4.10 Avfallshantering

- Verksamhetsutövare som bedriver avfallshantering enligt definitionen i artikel 3.9 i Europaparlamentets och rådets direktiv 2008/98/EG[15], dock undantaget verksamhetsutövare vars huvudsakliga näringsverksamhet inte är avfallshantering.

Avfallshantering avser insamling, transport, återvinning och bortskaffande av avfall, inklusive kontroll av sådan verksamhet och efterbehandling av platser för bortskaffande av avfall, inklusive åtgärder som handlaren eller mäklaren vidtar.

4.11 Tillverkning, produktion och distribution av kemikalier

- Företag som tillverkar ämnen och distribuerar ämnen eller blandningar som avses i artikel 3.9 och 3.14 i Europaparlamentets och rådets förordning (EG) nr 1907/2006[16] samt företag som produ-

[14] Europaparlamentets och rådets direktiv 97/67/EG av den 15 december 1997 om gemensamma regler för utvecklingen av gemenskapens inre marknad för posttjänster och för förbättring av kvaliteten på tjänsterna.
[15] Europaparlamentets och rådets direktiv 2008/98/EG av den 19 november 2008 om avfall och om upphävande av vissa direktiv.
[16] Europaparlamentets och rådets förordning (EG) nr 1907/2006 av den 18 december 2006 om registrering, utvärdering, godkännande och begränsning av kemikalier (Reach), inrättande av en europeisk kemikaliemyndighet, ändring av direktiv 1999/45/EG och upphävande av rådets

cerar varor enligt definitionen i artikel 3.3 i den förordningen genom att använda ämnen och blandningar.

Med ämne avses kemiskt grundämne och föreningar av detta grundämne i naturlig eller tillverkad form, inklusive de eventuella tillsatser som är nödvändiga för att bevara dess stabilitet och sådana föroreningar som härrör från tillverkningsprocessen, men exklusive eventuella lösningsmedel som kan avskiljas utan att det påverkar ämnets stabilitet eller ändrar dess sammansättning. Med vara avses ett föremål som under produktionen får en särskild form, yta eller design, vilken i större utsträckning än dess kemiska sammansättning bestämmer dess funktion.

4.12 Produktion, bearbetning och distribution av livsmedel

- Livsmedelsföretag enligt definitionen i artikel 3.2 i Europaparlamentets och rådets förordning (EG) nr 178/2002[17] som bedriver grossisthandel och industriell produktion och bearbetning.

Med livsmedelsföretag avses varje privat eller offentligt företag som med eller utan vinstsyfte bedriver någon av de verksamheter som hänger samman med alla stadier i produktions-, bearbetnings- och distributionskedjan av livsmedel.

förordning (EEG) nr 793/93 och kommissionens förordning (EG) nr 1488/94 samt rådets direktiv 76/769/EEG och kommissionens direktiv 91/155/EEG, 93/67/EEG, 93/105/EG och 2000/21/EG.

[17] Europaparlamentets och rådets förordning (EG) nr 178/2002 av den 28 januari 2002 om allmänna principer och krav för livsmedelslagstiftning, om inrättande av Europeiska myndigheten för livsmedelssäkerhet och om förfaranden i frågor som gäller livsmedelssäkerhet.

4.13 Tillverkning

Tillverkning av medicintekniska produkter och medicintekniska produkter för *in vitro*-diagnostik

- Verksamhetsutövare som tillverkar medicintekniska produkter enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) 2017/745[18], och verksamhetsutövare som tillverkar medicintekniska produkter för *in vitro*-diagnostik enligt definitionen i artikel 2.2 i Europaparlamentet och rådets förordning (EU) 2017/746[19], med undantag av verksamhetsutövare som tillverkar sådana medicintekniska produkter som avses i punkt 5 femte strecksatsen i bilaga 1 i NIS2-direktivet.

Inom hälso- och sjukvården används ett mycket stort antal medicintekniska produkter av olika slag. Några exempel är kompresser, kontaktlinsprodukter, sprutor, kanyler, infusionsaggregat och pumpar för läkemedelstillförsel.

När det gäller medicintekniska produkter för in vitro-diagnostik så syftar termen på att biologiskt material studeras utanför sin normala biologiska kontext. In vitro-diagnostik innebär således diagnostik utanför kroppen och exempel på produkter är analysutrustning, provrör och olika tester avsedda att upptäcka medicinska tillstånd eller sjukdomar.

Tillverkning av datorer, elektronikvaror och optik

- Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 26 i Nace Rev. 2.

Huvudgrupp 26 omfattar tillverkning av datorer, kringutrustning för datorer, kommunikationsutrustning, och liknande elektroniska produkter, liksom tillverkning av komponenter för sådana produkter. Huvudgruppen innehåller också tillverkning av konsumentelek-

[18] Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG.
[19] Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU.

tronik, mät-, test- och navigationsutrustning, strålnings-, elektromedicinsk och elektroterapeutisk utrustning, optiska instrument och utrustning, samt tillverkning av magnetiska och optiska media.

Tillverkning av elapparatur

- Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 27 i Nace Rev. 2.

Huvudgrupp 27 omfattar tillverkning av produkter som alstrar, distribuerar och använder elkraft. Dessutom omfattar huvudgruppen tillverkning av elektrisk belysning, signalutrustning och elektriska hushållsapparater.

Tillverkning av övriga maskiner

- Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 28 i Nace Rev. 2.

Huvudgrupp 28 omfattar tillverkning av maskiner och utrustning som självständigt bearbetar material antingen mekaniskt eller med värme eller gör något med materialet (till exempel godshantering, sprutning, vägning eller förpackning) inklusive deras mekaniska komponenter som genererar och använder kraft, och specialtillverkade delar. Denna kategori omfattar fasta eller rörliga eller handmanövrerade anordningar, oberoende om de är avsedda för industrin, bygg- eller anläggningssektorn, jordbruket eller för hemmabruk. Tillverkning av särskild utrustning för passagerar- eller godstransporter inom avgränsade områden ingår även i denna huvudgrupp.

Tillverkning av motorfordon, släpfordon och påhängsvagnar

- Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 29 i Nace Rev. 2.

Huvudgrupp 29 omfattar tillverkning av motorfordon för transport av passagerare eller godsbefordran samt tillverkningen av olika delar och tillbehör, liksom tillverkning av släpfordon och påhängsvagnar.

Tillverkning av andra transportmedel

- Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 30 i Nace Rev. 2.

Huvudgrupp 30 omfattar tillverkning av transportmedel till exempel skepps- och båtbyggeri, tillverkning av rullande materiel för järnväg och lokomotiv, luftfartyg och rymdfarkoster samt tillverkning av delar till dessa.

4.14 Digitala leverantörer

- Leverantörer av marknadsplatser online.

Marknadsplats online avser enligt NIS2-direktivet en marknadsplats online enligt definitionen i artikel 2 n i Europaparlamentets och rådets direktiv (EU) 2005/29/EG[20]. I det direktivet definieras marknadsplats online som en tjänst som använder programvara, inbegripet en webbplats, en del av en webbplats eller en applikation, som administreras av en näringsidkare eller för dennas räkning, som ger konsumenterna möjlighet att ingå distansavtal med andra näringsidkare eller konsumenter.

[20] Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder).

- Leverantörer av sökmotorer.

Sökmotor avser enligt NIS2-direktivet en sökmotor enligt definitionen i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150[21]. I den förordningen definieras sökmotor som en digital tjänst som gör det möjligt för användare att mata in sökfraser för att göra sökningar på i princip alla webbplatser eller alla webbplatser på ett visst språk på grundval av en fråga om vilket ämne som helst i form av ett nyckelord, en röstbegäran, en fras eller någon annan inmatning och som returnerar resultat i vilket format som helst som innehåller information om det begärda innehållet.

- Leverantörer av plattformar för sociala nätverkstjänster.

Plattform för sociala nätverkstjänster definieras i NIS2-direktivet som en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, särskilt genom chattar, inlägg, videor och rekommendationer.

4.15 Forskning

- Forskningsorganisationer.

Forskningsorganisation definieras i NIS2-direktivet som en verksamhetsutövare vars främsta mål är att bedriva tillämpad forskning eller experimentell utveckling i syfte att utnyttja resultaten av denna forskning i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner.

Av skäl 36 framgår att forskningsorganisationer bör anses inbegripa verksamhetsutövare som riktar in större delen av sin verksamhet på tillämpad forskning eller experimentell utveckling i den mening som avses i Frascatimanualen 2015[22] i syfte att utnyttja sina resultat i kommersiella syften, såsom tillverkning eller utveckling av en produkt eller process, tillhandahållare av en tjänst, eller marknadsföring därav.

[21] Europaparlamentets och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster.
[22] OECD (2015), Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, The Measurement of Scientific, Technological and Innovation Activities, OECD Publishing, Paris.

5 Cybersäkerhetslagens tillämpningsområde

5.1 Direktivet ska i huvudsak genomföras genom ny NIS-lag

Utredningens förslag: NIS2-direktivet ska i huvudsak genomföras genom att NIS-lagen och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster upphävs och ersätts av ny lag och ny förordning med benämningarna cybersäkerhetslagen respektive cybersäkerhetsförordningen.

Som framgått av bakgrundsbeskrivningen i kapitel 3 genomfördes det tidigare NIS-direktivet genom NIS-lagen och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, NIS-förordningen. När det tidigare NIS-direktivet upphävs och ersätts av NIS2-direktivet är det givet att genomförandet behöver ske genom ändringar i dessa regelverk. Med hänsyn till de omfattande ändringarna bör den tidigare lagen och förordningen upphävas och ersättas av ny lag och ny förordning. Den tidigare lagen kan dock i flera avseenden tjäna som förebild utifrån genomarbetade lösningar för likartade frågor.

I detta kapitel ska tillämpningsområdet för en ändrad NIS-lag analyseras.

5.1.1 NIS-lagen

I NIS-lagens första paragraf anges att syftet med lagen är att uppnå en hög nivå på säkerheten i nätverk och informationssystem för samhällsviktiga tjänster inom de sju sektorerna energi, transport, bank-

verksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten och digital infrastruktur samt för digitala tjänster. Tillämpningsområdet är definierat i tredje paragrafen. Av den följer att flera olika kriterier måste vara uppfyllda.

Inledningsvis är det bara leverantörer av samhällsviktiga tjänster inom de sju områden och digitala tjänster som omfattas av lagen. De sju områden definieras i bilaga 2 till NIS-direktivet, vilket 3 § hänvisar till. Exempelvis anges där att området energi innefattar delområdena elektricitet, olja och gas. Det definieras vidare att exempelvis inom delområdet elektricitet avses elföretag och systemansvariga för distributionssystemet och överföringssystemet enligt definitioner i Europaparlamentets och rådets direktiv 2009/72/EG.[1] Därutöver krävs det att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem samt att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Vid bedömningen om vad som utgör en betydande störning ska bland annat beaktas antalet användare som är beroende av den samhällsviktiga tjänsten, leverantörens marknadsandel, storleken av det geografiska område som skulle kunna påverkas av en incident och hur beroende andra sektorer är av den samhällsviktiga tjänst som leverantören erbjuder. Leverantören behöver vara etablerad i Sverige. Såväl offentliga aktörer, dvs. statliga myndigheter, landsting som privata aktörer omfattas.[2]

5.1.2 Ett vidare syfte

Utredningens förslag: Syftet med denna lag är att uppnå en hög cybersäkerhetsnivå.

Som framgått av föregående avsnitt är NIS-lagens syfte som är uttryckt i 1 § att uppnå en hög nivå på säkerheten i nätverk och informationssystem för samhällsviktiga tjänster inom sju utpekade sektorer och digitala tjänster. Detta speglar med en anpassning till att det är nationell rätt. Artikel 1.1 i det tidigare NIS-direktivet anger att det i direktivet fastställs åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverks- och informationssystem. Regleringen

[1] Europaparlamentets och rådets direktiv 2009/72/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för el och om upphävande av direktiv 2003/54/EG.
[2] Prop. 2017/18:205 s. 90 och 91.

innehåller bland annat krav på ett systematiskt informationssäkerhetsarbete.

Med nätverk och informationssystem avses enligt lagens 2 § punkt 1 följande:

a) ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen (2022:482) om elektronisk kommunikation,

b) en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller

c) digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av a och b för att de ska kunna driftas, användas, skyddas och underhållas. Enligt samma paragraf punkt 2 avses med säkerhet i nätverks och informationssystem: nätverks och informationssystems förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem.

I NIS2-direktivet är syftet uttryckt på annat sätt. I artikel 1 är nivå på säkerhet i nätverks- och informationssystem utbytt till cybersäkerhetsnivå. I artikel 6.3 hänvisas för begreppet cybersäkerhet till definitionen i artikel 2.1 i förordning (EU) 2019/881[3]. Där anges att cybersäkerhet betyder all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot. Att nätverks- och informationssystem behåller sin tidigare betydelse framgår av samma artikel punkt 2, där det hänvisas till artikel 4.1 i NIS-direktivet.

Innebörden skulle vara att NIS2-direktivet delvis har samma syfte som det första NIS-direktivet. Formuleringen ”verksamhet som är nödvändig för att skydda nätverks- och informationssystem” i NIS2 betyder rimligen samma sak som att ”uppnå en hög nivå på säkerheten i nätverk och informationssystem”. Det som dock skiljer

[3] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

sig är att NIS2 genom definitionen av cybersäkerhet särskilt även pekar ut skyddet av användare av systemen och andra berörda personer.

En fråga är då vad detta betyder. Om nätverken och informationssystemen skyddas bör det innebära att även användare och andra berörda personer skyddas. Regeringens direktiv lyfter inte frågan och inte heller de inledande skälen 1–6 anger att en ändring är avsedd i denna del. I stället anges i skälen att det övergripande syftet med att ersätta det tidigare NIS-direktivet med ett nytt beror på att medlemsstaternas skydd skiljer sig åt, vilket ger en fragmentering av den inre marknaden. Skillnaderna medför att vissa medlemsstater har en större sårbarhet, vilket medför spridningseffekter. Direktivets mål är att undanröja skillnaderna, särskilt genom att föreskriva minimiregler och att fastställa mekanismer för ett effektivt samarbete mellan myndigheterna i medlemsländerna. Vidare bör sektorerna utökas och skillnaderna mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster utjämnas.[4]

Sammantaget drar utredningen den slutsatsen att syftet är något vidare uttryckt i NIS2-direktivet jämfört med NIS-direktivet, se även kapitel 11. Utredningen föreslår att det övergripande syftet i 1 § NIS-lagen följer EU-direktivet semantiskt.

En annan viktig skillnad är att NIS-lagen omfattar samhällsviktiga tjänster inom sju sektorer och digitala tjänster. NIS2-direktivet saknar begränsningen till samhällsviktiga och digitala tjänster. I stället omfattas som huvudregel alla verksamhetsutövare inom 18 sektorer, som också har undersektorer. Som kommer att framgå nedan finns det ett stort antal undantag och även möjligheter till att utsträcka tillämpningsområdet. Utredningen föreslår därmed att tillämpningsområdet definieras särskilt och att det inledningsvis är tillräckligt att ange att syftet med lagen är att uppnå en hög cybersäkerhetsnivå.

[4] Se särskilt skäl 5 och 6.

5.2 Direktivets tillämpningsområde

5.2.1 Utgångspunkter

Utredningens övergripande slutsats är att direktivet inte ska införlivas direktivnära utan att förslagen ska utformas utifrån den systematik och terminologi som används i svensk rätt. Ett normalt språkbruk ska eftersträvas.[5] Så är även det tidigare NIS-direktivet genomfört och det följer även uttryckligen att regeringens direktiv att den terminologi som används i direktiven ska anpassas till vedertagna begrepp i nationell reglering.

5.2.2 Verksamhetsutövare

Utredningens förslag: Begreppet entitet ersätts av verksamhetsutövare som definieras som juridisk eller fysisk person som bedriver verksamhet.

Den juridiska eller fysiska personens verksamhet omfattas i dess helhet av lagens krav.

NIS2-direktivets tillämpningsområde följer av artikel 2. I punkterna 1–5 definieras området för att följas av undantag under punkterna 6–12. Punkterna 13 och 14 avser sekretess och personuppgifter och kommer att behandlas i ett senare kapitel.

Av artikel 2.1 följer att direktivet är tillämpligt på offentliga eller privata entiteter av den typ som följer av bilaga 1 eller 2. Som framgått är det utredningens uppfattning att en ny NIS-lag på samma sätt som den tidigare ska präglas av ett tillgängligt språkbruk. Det betyder att utredningen behöver ersätta begreppet entitet. I artikel 6 punkt 38 definieras entitet som fysisk eller juridisk person som bildats och erkänts som sådan och som i eget namn får utöva rättigheter och ha skyldigheter. En entitet kan därmed inte vara en plats eller ett område. Av definitionen följer i stället att en entitet är en fysisk eller juridisk person, eftersom dessa enligt svensk rätt får utöva rättigheter och bära skyldigheter. Innebörden blir att det är fysiska eller

[5] Jämför Lagrådets yttrande 2023-04-11, *Ett granskningssystem för utländska direktinvesteringar till skydd för svenska säkerhetsintressen*, www.lagradet.se/wp-content/uploads/2023/04/Ett-granskningssystem-for-utlandska-direktinvesteringar-till-skydd-for-svenska-sakerhetsintressen.pdf, inhämtat 2023-05-02.

juridiska personer som bedriver en verksamhet som omfattas av lagen och bör lämpligen definieras så. Det framgår vidare av bilaga 1 eller 2 att det är fysiska eller juridiska personer, som bedriver verksamhet inom vissa områden, dvs. verksamhetsutövare. I direktivet används också en mängd olika begrepp för verksamhetsutövare, som exempelvis, producenter, vårdgivare, leverantörer eller tillhandahållare. För att möjliggöra en sammanhållen och stringent lag kommer utredningen genomgående att använda samlingstermen verksamhetsutövare. Detta kan dock inte ske undantagslöst. Exempelvis kommer utredningen att behöva använda begreppet kvalificerade tillhandahållare av betrodda tjänster, eftersom det begreppet behöver ha samma innebörd som i förordningen EU) nr 910/2014.[6]

Begreppet verksamhetsutövare används även i 2 kap. 1 § säkerhetsskyddslagen (2018:585), som där betyder den som till någon del bedriver säkerhetskänslig verksamhet.

Systematiken i artikel 2 punkt 1–5 är vidare att vissa högkritiska och kritiska verksamhetsutövare uttryckligen pekas ut i bilaga 1 respektive i bilaga 2 till direktivet. Dessa omfattas som huvudregel enligt artikel 1.1 av direktivets krav, dvs. de omfattas om de inte sedan faller under något undantag enligt punkt 6–12 under enda förutsättning att verksamheterna är av viss storlek. Därutöver är direktivet som huvudregel tillämpligt på utpekade verksamhetsutövare i bilaga 1 och 2 oavsett storlek om de uppfyller vissa kriterier som redovisas under punkterna 2–4. Slutligen får medlemsstaterna enligt punkten 5 även föreskriva att direktivet ska tillämpas på kommuner och utbildningsinstitut.

Innebörden av detta är att endast verksamhetsutövare inom områden som pekas ut i bilaga 1 och 2 omfattas av direktivet. Om verksamheterna är av viss storlek är det tillräckligt för att direktivets krav gäller. Är de inte tillräckligt stora behöver vissa kriterier vara uppfyllda och i de fallen krävs oftast en bedömning. Slutligen får medlemsstaterna utsträcka kraven.

En särskild fråga är om verksamhetsutövarens verksamhet i dess helhet omfattas eller om bara delar av verksamheten behöver uppfylla direktivets krav. Det är till exempel möjligt att ett elföretag som omfattas av bilaga 1 även bedriver annan verksamhet inom en annan

[6] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

sektor som inte finns upptagen i bilaga 1 eller 2. Omfattas då även denna andra verksamhet av direktivet? Som framgått är det den fysiska eller juridiska personen som exempelvis ett elföretag enligt angiven definition i bilaga 1 inom sektorn energi och delsektorn elektricitet som omfattas av direktivets krav. Det saknas en uttrycklig begränsning om att endast delar av den fysiska eller juridiska personens verksamhet skulle omfattas av direktivet.

Utredningens slutsats är med hänsyn härtill att hela verksamheten omfattas. Det betyder den fysiska eller juridisk personens verksamhet som helhet. För staten kommer dock särskilda regler att gälla i denna del, se nedan.

Det har ifrågasatts om detta skulle få allt för långtgående verkningar i praktiken, om exempelvis riskhanteringsåtgärderna enligt artikel 21 och tillsynen skulle behöva bli alltför omfattande.

Utredningen menar att det är svårt att tolka direktivet på annat sätt än att den fysiska eller juridiska personens verksamhet i sin helhet omfattas. Det framstår också med hänsyn till att nätverks- och informationssystem många gånger är sammankopplade inom hela verksamhet samt att incidenter inom en del kan påverka annan del att det skulle leda till gränsdragningsproblem att försöka dela upp verksamheten.

Slutsatsen förstärks av skäl 16. Här framgår att det förhållandet att en verksamhet har ett nära samband med en annan verksamhet kan leda till att tröskelvärden överstigs. Medlemsstaterna får under vissa förutsättningar undanta dessa från tillämpningsområdet. I skäl 16 anges att s.k. partnerföretag eller s.k. anknutna företag inte behöver omfattas när det skulle vara icke- proportionellt om de inte skulle omfattas om de varit självständiga. Det anges vissa kriterier när så får ske. Begreppen partnerföretag och anknutna företag definieras i artikel 3.1–3.3 i 2003/361/EG[7], se även avsnitt 5.2.8 avseende storlekskravet. Med anknutna företag avses företag som det finns förbindelse mellan. Fyra olika kriterier skapar en sådan förbindelse. Ett första är att ett företag ska ha ett stort inflytande över det andra genom majoritet av röster eller andelar. Detsamma gäller om företaget på grund av överenskommelser med andra förfogar ensamt över en majoritet av rösterna för aktierna eller andelarna. Andra kriterier är att företaget har rätt att utse eller entlediga en majoritet av leda-

[7] Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.

möter i styrelse, ledning eller tillsynsorgan eller rätt att utöva ett bestämmande inflytande över annat företag enligt avtal eller enligt bolagets stadgar. Utredningens bedömning är att kriterierna för anslutna företag överensstämmer med kriterierna för dotterbolag i bland annat 1 kap. 11 § aktiebolagslagen (2005:551) som kriterier för ett dotterbolag.

Därmed är bestämmelsen om anknutna företag i svensk rätt relevant för en koncern. En koncern består enligt 1 kap. 11 § aktiebolagslagen (2005:551) av ett moderbolag och ett eller flera dotterbolag. De är skilda juridiska personer. Innebörden är alltså att skäl 16 är mer långtgående.

Med partnerföretag avses företag som inte betecknas som anknutna, men som har en kapital- eller röstandel på minst 25 procent i ett annat företag eller om annat företag har samma kapital- eller röstandel i det företaget.[8] Innebörden av det anförda blir att även företag som inte når upp till storlekskravet som egen juridisk person kan göra det på grund av sambandet med exempelvis ett moderbolag. Detta behöver inte anges särskilt i lagen utan följer av artikel 3.1–3.3 i 2003/361/EG, alltså genom definitionen av storlekskravet. Det utredningen däremot behöver göra är att i enlighet med skäl 16 överväga om partnerföretag eller anknutna företag inte behöver omfattas när det inte skulle vara proportionellt om de inte skulle omfattas om de varit självständiga. Utredningen föreslår att detta ska vara möjligt. De närmare förutsättningarna ska följa av förordning, se vidare avsnitt 5.2.12.

5.2.3 Högkritiska sektorer

I bilaga 1 pekas de högkritiska sektorerna ut, vilka är 11. Dessa är energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, dricksvatten, avloppsvatten, digital infrastruktur, förvaltning av IKT-tjänster mellan företag, offentlig förvaltning och rymden. Jämfört med NIS-lagen, se ovan, motsvarar dessa högkritiska sektorer i hög grad de som i dag omfattas av NIS-lagen. Det finns sektorer som tillkommit samt andra förändringar som är redovisat i kapitel 4.

[8] Se även https://www.energimyndigheten.se/4a9cb5/globalassets/energieffektivisering_/lagar-och-krav/ekl/smf_guide.pdf, inhämtat 2023-05-16.

Sektorerna eller delsektorerna är också definierade i bilagorna. Exempelvis definieras fjärrvärme eller fjärrkyla som operatörer av fjärrvärme eller fjärrkyla enligt definitionen i artikel 2.19 i Europaparlamentets och rådets direktiv (EU) 2018/2001[9] och bankverksamhet definieras som kreditinstitut enligt definitionen i artikel 4.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013[10].

5.2.4 Offentlig förvaltning enligt direktivet

I bilaga 1 är offentlig förvaltning en egen utpekad sektor. Begreppet betyder i bilaga 1 två saker. Det betyder i första hand offentliga förvaltningsentiteter hos nationella regeringar såsom de definieras av en medlemsstat i enlighet med nationell rätt. Vidare innefattas offentliga förvaltningsentiteter på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt. Det ska också noteras att det finns en särskild definition av offentlig förvaltningsentitet i artikel 6 punkt 35. Här anges att en offentlig förvaltningsentitet är en entitet som erkänts som sådan i nationell rätt med undantag av rättsväsendet, parlament, och centralbanker. Det anges vidare som krav att fyra kriterier är uppfyllda, som innebär att 1. verksamheten har inrättats för att tillgodose behov i det allmännas intresse och inte har industriell eller kommersiell karaktär, 2. verksamheten har ställning som en juridisk person eller har lagstadgad rätt att företräda en annan entitet som har ställning som juridisk person, 3. verksamheten finansieras till största delen offentligt och 4. verksamheten har befogenhet att rikta administrativa eller reglerade beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.

5.2.5 Sveriges organisation – offentlig förvaltning

Sveriges statsskick följer av regeringsformen. Sammantaget gäller att med begreppet *myndighet* avses samtliga statliga och kommunala organ med undantag för beslutande politiska församlingar. Med

[9] Europaparlamentets och rådets direktiv (EU) 2018/2001 av den 11 december 2018 om främjande av användningen av energi från förnybara energikällor.
[10] Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och värdepappersföretag och om ändring av förordning (EU) nr 648/2012.

kommunala organ avses regioner och kommuner enligt 14 kap. 2 § regeringsformen.

Det betyder för staten att regeringen och Regeringskansliet är myndigheter. Riksdagen är inte en myndighet, eftersom det är en beslutande församling, men riksdagsförvaltningen, som biträder riksdagen är att betrakta som en myndighet.

Inom regioner och kommuner finns beslutande församlingar som benämns regionfullmäktige respektive kommunfullmäktige som motsvarar riksdagen och därför inte heller är myndigheter. Motsvarigheten till regeringen är regionstyrelsen respektive kommunstyrelsen, som då alltså är myndigheter.

I regeringsformen skiljer man sedan på rättskipning och offentlig förvaltning. För rättsskipning finns domstolar och för den offentliga förvaltningen statliga och kommunala förvaltningsmyndigheter. Begreppet *förvaltningsmyndighet* omfattar alla myndigheter utom regeringen och domstolarna. Även domstolarna är dock myndigheter, men alltså inte förvaltningsmyndigheter. Innebörden är att myndighet och förvaltningsmyndighet oftast betyder samma sak, enda skillnaden är att regeringen och domstolar faller utanför begreppet förvaltningsmyndighet, men ingår i begreppet myndighet. Även statliga affärsverk är en myndighet.

Det anförda betyder att organisationen utgår från organisationsformen, inte från vilken funktion organet har. Ett aktiebolag som till exempel AB Svensk Bilprovning, som alltså inte är en myndighet trots att bolaget utför förvaltningsuppgifter.

I Sverige finns det 346 statliga myndigheter, varav 342 lyder under regeringen. De är organisatoriskt fristående, men styrs av regeringen som ansvarar för myndigheternas verksamhet inför riksdagen. Domstolarna har en särställning som innebär att de är mer oberoende. Därutöver finns det fyra statliga myndigheter som i stället lyder under riksdagen. Dessa är Riksrevisionen, Riksdagens ombudsmän (JO), Sveriges Riksbank och Riksdagsförvaltningen.

Inom regionerna och kommunerna finns det nämnder som är regionala respektive kommunala förvaltningsmyndigheter.[11]

[11] https://www.statskontoret.se/fokusomraden/fakta-om-statsforvaltningen/myndigheterna-under-regeringen/, inhämtat 2023-07-07.

5.2.6 Utredningens analys

Enligt NIS2-direktivet är alltså offentlig förvaltning en egen sektor. Med offentlig förvaltning avses offentliga förvaltningsentiteter hos nationella regeringar såsom de definieras av en medlemsstat i nationell rätt. Offentliga förvaltningsentiteter hos nationella regeringar bör enligt utredningens bedömning i huvudsak avse statliga myndigheter inklusive statliga affärsverk. Eftersom det står ”hos” regeringen bör rimligen regeringen falla utanför, trots att även regeringen är en myndighet. Ordet ”hos” bör också exkludera myndigheter som lyder under riksdagen, dvs. Riksrevisionen, JO, Sveriges Riksbank och Riksdagsförvaltningen. Som framgått tidigare är Sveriges Riksbank även undantagen i sin egenskap av centralbank. Vidare innefattas länsstyrelserna som är statliga regionala myndigheter. Eftersom domstolar är statliga myndigheter ingår även de som utgångspunkt, men som framgår vidare ovan är rättsväsendet undantaget. Det bör betyda att domstolarna faller utanför, men att Domstolsverket som är en administrativ myndighet omfattas.

En särskild svårighet för analysen av tillämpningsområdet för begreppet offentlig förvaltning är kraven i artikel 6 punkt 35. Som framgått behöver fyra kriterier vara uppfyllda. Två av dem, att verksamheten har inrättats för att tillgodose behov i det allmännas intresse och inte har industriell eller kommersiell karaktär samt att verksamheten finansieras till största delen offentligt är självklara för offentlig verksamhet och behöver inte närmare beröras.

Det anges dock vidare som krav att verksamhetsutövaren har ställning som juridisk person eller lagstadgad rätt att agera för en annan entitet. Definitionen är motsägelsefull. Som tidigare berörts anges i samma artikel, punkt 38 att entitet betyder fysisk eller juridisk person. I punkt 35 anges nu att offentlig entitet betyder *entitet* som bland annat uppfyller kravet om att den har ställning som juridisk person eller lagstadgad rätt att agera för annan.

Utredningen tolkar artikel 6 punkt 35 på det sättet att kravet är att en verksamhetsutövare är en fysisk eller juridisk person, men att det för viss offentlig verksamhet är tillräckligt med företrädesrätt. När det gäller statliga myndigheter är det också så att de inte är egna juridiska personer utan den juridiska personen är staten, som sedan myndigheter kan företräda. Rimligen är det också detta som avses i kriteriet om att det är tillräckligt med företrädesrätt. En slutsats av

det anförda är att staten inte till skillnad från andra verksamhetsutövare som exempelvis bolag är en enhet som juridisk person utan att varje myndighet som omfattas är en egen enhet.

Vidare innefattas offentliga förvaltningsentiteter på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt. En region är en juridisk person och har som sådan också ett organisationsnummer enligt 1 § lag (1974:174) om identitetsbeteckning för juridiska personer med flera Här ingår då regionstyrelsen och nämnder. Med hänsyn till att begreppet är offentliga *förvaltnings*-entiteter bör rimligen regionfullmäktige falla utanför. Eftersom varje region är en juridisk person framstår det som rimligt att varje region på samma sätt som exempelvis varje bolag utgör en enhet, som verksamhetsutövaren ansvarar för.

En ytterligare svårighet utgör det fjärde kriteriet i artikel 6 punkt 35 för offentlig förvaltning om att verksamheten ska ha befogenhet att rikta administrativa eller reglerade beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital. Kravet har betydelse för all offentlig verksamhet, myndigheter, regioner och kommuner. Har alla dessa verksamhetsutövare möjlighet att rikta sådana beslut till fysiska eller juridiska personer?

Enligt utredningens bedömning är kriteriet oklart och svårt att förstå. Det är självklart att många myndigheter har befogenhet att rikta ingripande beslut mot fysiska och juridiska personer som påverkar i första hand dem, men som i förlängningen även påverkar deras gränsöverskridande förmåga. Klara exempel kan vara Polismyndigheten som kan frihetsberöva personer eller tullmyndigheten som kan omhänderta gods.

Som framgått har Sverige 346 myndigheter. En analys av varje myndighets och regions befogenheter i förhållande till gränsöverskridande effekter framstår varken som möjligt eller ändamålsmässigt. I stället behöver en övergripande tolkning göras. Tolkningen bör ha sin grund i direktivets syfte. Av skäl 48 följer att effekten av det tidigare NIS-direktivet inte var tillräckligt, eftersom cybersäkerhetskraven för verksamheter varierade mellan medlemsländerna inom unionen. Skillnaderna ledde till en fragmentering av den inre marknaden. Vissa medlemsländer kunde ha större sårbarhet för cyberhot med potentiella spridningsrisker i hela unionen. Syftet med NIS2-direktivet var därför enhetliga kriterier för vilka verksamheter som

omfattas i huvudsak efter storlekskravet. Undantag för offentliga verksamheter bör avse verksamheter vars övervägande del bedrivs på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning.

Utredningens slutsats är med hänsyn till det anförda är att direktivet inte syftar till att göra en skiljelinje mellan offentlig verksamhet utifrån i vilken utsträckning deras beslut har gränsöverskridande påverkan utan syftet är att ett så stort antal verksamhetsutövare som möjligt ska omfattas, men med beaktande av storlekskravet och nationell säkerhet med mera. Vidare beaktar utredningen vid denna tolkning också att direktivet enligt artikel 5 är ett minimidirektiv med innebörd att medlemsstaterna får anta bestämmelser som säkerställer en högre cybersäkerhetsnivå.

5.2.7 Andra kritiska sektorer

De andra kritiska sektorerna finns i bilaga 2 och är sju. Det handlar om post- och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, digitala leverantörer och forskning. Vidare finns det ett område som heter tillverkning. I det området ingår delsektorerna tillverkning av medicintekniska produkter, datorer, elektronikvaror och optik, elapparater, övriga maskiner, motorfordon, släpfordon och påhängsvagnar och andra transportmedel. I jämförelse med det tidigare NIS-direktivet och NIS-lagen är det i sin helhet nya områden.[12]

5.2.8 Storlekskravet

Som huvudregel omfattas alltså alla verksamhetsutövare som faller inom de högkritiska och kritiska områdena om verksamheterna är tillräckligt stora. Det saknar i det sammanhanget betydelse om det är offentliga eller privata verksamheter.

Storlekskravet finns i artikel 2.1. Det anges att en verksamhet är av tillräcklig storlek om den minst kan betecknas som ett medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation

[12] Undantag gäller för marknadsplatser online och sökmotorer som tidigare ingick i området var digitala tjänster.

2003/361/EG.[13] Ett vidare krav är att verksamheten tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen. Artikel 2 i bilagan till kommissionens rekommendation definierar mikroföretag samt små och medelstora företag (SMF-kategorin). Av artikeln följer att ett medelstort företag är ett företag som sysselsätter minst 50 personer eller vars omsättning eller balansomslutning överstiger 10 miljoner euro per år.

Av artikel 1 i samma rekommendation anges att med företag avses varje enhet, oberoende av juridisk form, som bedriver en ekonomisk verksamhet ska anses som ett företag. När det gäller till exempel statsstöd tolkas begreppet ekonomisk verksamhet mycket brett och omfattar varje organisation som med eller utan vinstsyfte köper eller säljer varor eller tjänster på en eller flera marknader. Det betyder att även offentliga aktörer – staten eller kommunala organ – kan bedriva ekonomisk verksamhet. Det gäller även områden som vård, skola och omsorg, vilka i sin kärna är icke-ekonomiska, men där det också förekommer områden med marknadselement som kan utgöra ekonomisk verksamhet. Detsamma gäller stiftelse, en ideell verksamhet eller en idrottsförening.[14] Däremot gäller särskilda skatterättsliga regler för stat och kommun som bedriver ekonomisk verksamhet.[15]

Stat och kommun omfattas dock inte av kommissionens rekommendation om företag, eftersom det i artikel 3.4 finns ett undantag. Det anges som huvudregel där att ett företag inte anses tillhöra SMF-kategorin, om 25 procent eller mer av dess kapital eller dess röstandel direkt eller indirekt kontrolleras av ett eller flera offentliga organ, individuellt eller gemensamt. I NIS2-direktivet är dock i artikel 2.1 den artikeln undantagen. En slutsats är därför att även statlig och kommunal verksamhet omfattas av artikel 2.1. som huvudregel av NIS2-direktivet. Kommuner är i Sverige enligt regeringsformens[16] 1 kap. 7 § uppdelade i regioner och kommuner. Som framgått har dock kommuner, men inte regioner undantagits från definitionen av offentlig förvaltning i bilaga 1 till direktivet.

Därutöver finns det dock också andra kvalificeringsgrunder angivna i artiklarna 2.2–2.5.

[13] Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.
[14] https://www.regeringen.se/regeringens-politik/naringspolitik/statsstod/, inhämtat 2023-04-06.
[15] https://www4.skatteverket.se/rattsligvagledning/321543.html, inhämtat 2023-04-06.
[16] Kungörelse (1974:152) om beslutad ny regeringsform.

I artikel 2.2–2.4 anges att verksamhetsutövare som är utpekade i bilaga 1 och 2, men som inte uppnår storlekskravet som redovisats ovan och därför inte omfattas av direktivet enligt huvudregeln ändå omfattas under tolv olika separata förutsättningar. För att omfattas enligt dessa krävs därför fortfarande att verksamhetsutövare utpekas i bilaga 1 eller 2, men det avser alltså mindre verksamheter som inte uppfyller storlekskravet, men som i stället uppfyller en annan grund.

Vidare finns det i artikel 2.5 en annan typ av särskild kvalificeringsgrund för kommuner och utbildningsinstitut. Det anges att medlemsstaterna får föreskriva att direktivet ska tillämpas på offentliga verksamhetsutövare på lokal nivå och utbildningsinstitut, särskilt om de utför kritisk forskningsverksamhet. Nedan kommer dessa särskilda kvalificeringsgrunder att analyseras.

5.2.9 Myndigheter och regioner

Utredningens bedömning: Samtliga statliga myndigheter i Sverige med undantag av regeringen, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och domstolarna samt samtliga regioner, med undantag av regionfullmäktige i varje region ska omfattas av cybersäkerhetslagen krav som utgångspunkt.

Av artikel 2.2 f följer att alla offentliga verksamhetsutövare på statlig nivå oavsett storlek ska omfattas om de är utpekade i bilaga 1 eller 2. Det här får långtgående konsekvenser för statliga myndigheter. Som framgått är offentlig verksamhet ett särskilt område som pekas ut i bilaga 1 och 2. Det är dock definierat som statlig eller regional verksamhet, dvs. kommuner faller utanför. Med statlig verksamhet avses som framgått myndigheter med undantag av regeringen, myndigheter som lyder under riksdagen och domstolarna. Huvudregeln är för alla verksamhetsutövare som utpekas i bilagorna att storlekskravet är avgörande, det behöver vara uppfyllt för att NIS2-direktivets krav ska vara uppfyllt. Genom artikel 2.2 f sätts dock storlekskravet ur spel för myndigheter. Innebörden av detta blir sammantaget att alla myndigheter utom regeringen, myndigheter under riksdagen och domstolarna omfattas av NIS2-direktivets krav som utgångspunkt.

I artikel 2.2 f anges också att offentliga förvaltningsverksamheter på regional nivå omfattas oavsett storlekskravet, men bara under särskilda förutsättningar. De som omfattas oavsett storlekskravet är regional verksamhet som enligt en riskbaserad bedömning tillhandahåller tjänster vars störning kan ha en betydande effekt på kritisk samhällelig eller ekonomisk verksamhet. Kriteriet förutsätter alltså en bedömning. Utredningen menar dock att en sådan bedömning är överflödig för Sverige, eftersom samtliga 21 regioner bör uppfylla storlekskravet. Som framgått är kravet minst 50 anställda eller en balansomslutning på 10 miljoner euro. Regionernas intäkter för 2021 uppgick till sammanlagt 458 miljarder kronor.[17] Som framgått ska dock regionfullmäktige i varje region undantas.

5.2.10 Kommuner

Utredningens bedömning: Majoriteten av alla kommuner, omfattas av NIS2-direktivets krav redan genom att en stor andel av samtliga kommuner bedriver hemsjukvård och att samtliga uppfyller storlekskravet. Det är kommunen som juridisk person som omfattas som vårdgivare. Det saknas därmed i huvudsak skäl att överväga om kommuner ska omfattas som offentliga förvaltningsverksamheter på lokal nivå enligt artikel 2.5 a. Utredningen föreslår dock i fullständighetens namn att alla kommuner omfattas, men att kommunfullmäktige undantas.

Som framgått ingår kommuner inte i offentlig förvaltning enligt direktivets definitioner. Det betyder att kommuner inte som helhet är utpekade i bilaga 1 som statliga myndigheter och regioner är. Däremot bedriver kommuner verksamhet inom områden som exempelvis fjärrvärme och avfallshantering, som utgör utpekade områden i bilaga 1 och 2, men denna verksamhet sker enligt SKR många gånger i bolagsform, vilken betyder att det inte skulle vara kommunen som är verksamhetsutövare. Som framgått definieras offentlig förvaltningsentitet i artikel 6, punkt 35, genom att fyra kriterier behöver vara uppfyllda. Det fjärde kriteriet är att verksamheten har befogenhet att rikta administrativa eller reglerade beslut till fysiska eller

[17] skr.se/skr/ekonomijuridik/ekonomi/sektornisiffror/diagramforregionerna.1883.html/, inhämtat 2023-04-18.

juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital. Kommunala bolag kan enligt kommunallagens 10 kap. 2 § vara helägda eller delägda. Med ett helägt kommunalt bolag avses ett aktiebolag där kommunen eller regionen direkt eller indirekt innehar samtliga aktier och med ett delägt kommunalt bolag avses ett aktiebolag eller handelsbolag där kommunen eller regionen bestämmer tillsammans med någon annan. Aktie- eller handelsbolag kan inte rikta administrativa eller andra beslut mot fysiska eller juridiska personer som påverkar deras gränsöverskridande rörlighet. Bedrivs verksamheten genom kommunala bolag är det inte kommunen som är verksamhetsutövare enligt utredningens bedömning.

Vidare gäller att en stor andel av samtliga kommuner enligt uppgift från SKR bedriver hemsjukvård. Det betyder att majoriteten av alla kommuner är vårdgivare enligt definitionen inom området hälso- och sjukvårdssektorn enligt bilaga 1. I bilagan hänvisas beträffande definitionen av vårdgivare till en definition i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU.[18] Här definieras vårdgivare som ”varje fysisk eller juridisk person eller varje annan entitet som lagligen bedriver hälso- och sjukvård på en medlemsstats territorium”.

Utredningen har tidigare dragit den slutsatsen att en verksamhetsutövare enligt NIS2-direktivet är en fysisk eller juridisk person som bedriver verksamhet. Samtidigt är det dock som angetts tidigare tillräckligt för offentliga förvaltningsverksamhetsutövare att den har ställning som juridisk person eller lagstadgad rätt att agera för en annan verksamhet.

Det har från SKR invänts att det inte är nödvändigt att det är kommunen som juridisk person som är verksamhetsutövare och att kommunen därmed utgör en enhet. SKR har pekat på att staten som juridisk person behöver vara uppdelad i många enheter. Det har tillagts att det då skulle vara möjligt att se en nämnd inom kommunen, som inte är en egen juridisk person, som en särskild enhet.

Utredningen delar inte denna uppfattning utan anser att det föreligger en skillnad mellan statliga myndigheter och nämnder som har betydelse för införlivandet av direktivet. Statliga myndigheter är i och för sig inte självständiga rättssubjekt utan är en del av rätts-

[18] Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård.

subjektet staten, vilket betyder att myndigheter inte kan föra talan mot varandra. Det saknar dock i sammanhanget betydelse. Däremot får myndigheter till skillnad från nämnder enligt 27 § myndighetsförordningen (2007:515) som huvudregel, företräda staten vid domstol inom sitt verksamhetsområde. Detta gäller även när talan förs exempelvis om olika sanktionsavgifter, vilket är relevant för cybersäkerhetslagen, eftersom den kommer att innehålla sanktioner.[19] Motsvarande gäller inte för nämnder. Enligt kommunallagen (2017:725) 6 kap. 15 § får styrelsen själv eller genom ombud företräda kommunen eller regionen i alla mål och ärenden, om inte någon annan ska göra det på grund av lag eller annan författning eller beslut av fullmäktige.

För kommuner gäller då huvudregeln om att storlekskravet måste vara uppfyllt. En förutsättning är därför att kommunen uppfyller storlekskravet på minst 50 anställda eller har en omsättning eller balansomslutning som överstiger 10 miljoner euro per år, dvs. det är tillräckligt att ett av kraven är uppfyllda. Enligt uppgift från SKR uppfyller alla kravet på antalet anställda[20] och möjligen även balansomslutningen. Slutsatsen blir därmed att de flesta kommuner omfattas i sin helhet av NIS2-direktivets krav redan genom att de bedriver hemsjukvård. På samma sätt som har utvecklats för regioner, bör fullmäktige, dvs. här kommunfullmäktige undantas och även här gäller att lagen ska omfatta svenska kommuner. Med denna slutsats saknas det i huvudsak skäl att ta ställning till artikel 2.5 a om att medlemsstaterna får föreskriva att direktivet även ska tillämpas på offentliga verksamhetsutövare på lokal nivå. Utredningen föreslår dock i fullständighetens namn att alla kommuner omfattas, dvs. även de som möjligtvis inte bedriver hemsjukvård.

5.2.11 Alternativt förslag

Till utredningen har från MSB föreslagits att hela den offentliga sektorn, dvs. samtliga statliga myndigheter, regioner och kommuner som utgångspunkt borde omfattas av cybersäkerhetslagen för att säkerställa ett allriskperspektiv. Det skulle betyda att även myndigheterna under riksdagen inklusive Sveriges Riksbank och därutöver

[19] https://www.jk.se/beslut-och-yttranden/2017/03/7951-16-80, inhämtat 2023-08-30.
[20] De två minsta kommunerna i Sverige är Dorotea och Bjurholm. År 2022 hade Dorotea 247 tillsvidareanställda och Bjurholm 219.

även domstolarna borde omfattas. Vidare saknas enligt Säkerhetspolisen skäl att undanta myndigheter som bedriver säkerhetskänslig verksamhet eller brottsbekämpning. I stället utgör NIS-direktivets krav en lämplig ”bottenplatta", som i förekommande fall kan kompletteras av säkerhetsskyddsregleringens bestämmelser. Eftersom direktivet är ett minimidirektiv menar myndigheterna att det finns möjligheter för Sverige att utöka tillämpningsområdet.

Utredningen har dock redan i avsnitt 2.1.2 slagit fast att utredningens tidsram omöjliggör att tillämpningsområdet utökas och att utredningen i stället bör fokusera på analyser och förslag med syfte att införliva direktivet. Utredningens uppdrag är också att införliva direktivet inte att utarbeta ett nytt system från grunden. Skälet är, att om avvägningen som kommissionen och EU:s lagstiftare,[21] förhandlat fram i åsidosätts, behöver konsekvenserna för tillkommande områden övervägas ingående, eftersom det arbetet inte utförts tidigare.

För exempelvis Sveriges Riksbank och domstolarna skulle särskilt konsekvenserna för dessa myndigheters särskilda ställning och oberoende behöva analyseras. Från Säkerhetspolisen har då anförts att en möjlig lösning är att hela den offentliga verksamheten omfattas som utgångspunkt, men att kraven differentieras för de olika myndigheterna samt regionerna och kommunerna beroende på behov. Arbetet med differentieringen skulle enligt Säkerhetspolisen regeringen kunna göra i efterhand med stöd av ett bemyndigande. Sektorsmyndigheterna skulle kunna ge regeringen ett underlag för en bedömning i vilken utsträckning enskilda respektive offentliga verksamhetsutövare skulle omfattas av cybersäkerhetslagen. På samma sätt skulle det då vara möjligt att även låta myndigheter som i hög omfattning bedriver säkerhetskänslig verksamhet omfattas som utgångspunkt, men kraven differentieras, vidare om säkerhetskänslig verksamhet i avsnitt 5.5.4.

Utredningen anser att förslaget i sig har fördelar och har därför övervägt det. Det framstår som ett enkelt och attraktivt synsätt att NIS2-direktivets krav utgör en bottenplatta som byggs på exempelvis av säkerhetsskyddslagens krav. Inledningsvis ska dock konstateras att enligt utredningens slutsats omfattas redan hela den offentliga sektorn som utgångspunkt med undantag av endast fyra statliga myndigheter under riksdagen, domstolarna samt region- och kommunfullmäktige. Samtliga dessa omfattas också som utgångspunkt

[21] Ministerrådet och Europaparlamentet.

av samtliga krav i direktivet. Den differentiering som är möjlig kan därför som utgångspunkt enbart avse de fyra statliga myndigheterna under Riksdagen och domstolarna, eftersom dessa inte ingår i direktivets tillämpningsområde. Därutöver skulle sedan tillkomma undantag för säkerhetskänslig verksamhet och brottsbekämpning, se vidare avsnitt 5.5.4.

Utredningen menar därför inledningsvis att det är tveksamt om en ramlag med differentierade krav i en förordning framstår som ändamålsmässig, eftersom endast ett fåtal myndigheter faller helt utanför tillämpningsområdet och att det därutöver enbart behöver skapas undantag för säkerhetskänslig verksamhet. Till stöd för sitt arbete har utredningen också experter från de olika sektorsmyndigheterna. Om utredningen endast föreslår en ramlag som för alla krav överlämnar åt regeringen att i ett senare skede bedöma i vilken utsträckning verksamhetsutövare ska omfattas blir det svårt för remissinstanserna att kunna ha synpunkter på förslagen, eftersom konsekvenserna inte går att bedöma. Det ingår också i utredningens uppdrag att även lämna författningsförslag för en förordning. Från Försvarsdepartementet har anförts att det med hänsyn till den snäva tid som finns för införlivning av direktivet att det är angeläget att utredningen i denna del fullgör sitt uppdrag.

Sammantaget anser utredningen därför att en mer långtgående utredning och utvidgning av direktivets krav skulle behöva ske i särskild ordning. Domstolarna och de fyra statliga myndigheterna under riksdagen ska inte ska omfattas av cybersäkerhetslagen. Utredningen kommer att behandla förslaget vidare i förhållande till säkerhetskänslig verksamhet och brottsbekämpning i avsnitt 5.5.4.

5.2.12 Enskilda verksamhetsutövare

Utredningens förslag: Enskilda verksamhetsutövare som bedriver verksamhet inom EES, innefattas i bilaga 1 eller 2 till direktivet samt uppfyller storlekskravet för medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG ska omfattas av lagen.

Regeringen eller den myndighet regeringen bestämmer får i föreskrifter besluta om undantag för partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet.

Utredningens bedömning: Regeringen bör ge respektive tillsynsmyndighet i uppdrag att med stöd av Myndigheten för samhällsskydd och beredskap skyndsamt utforma en vägledning för den enskilde verksamhetsutövaren om vem som omfattas av sektorsbeskrivningarna.

Ovan har redovisats för vad som gäller för offentliga verksamhetsutövare och i vilken utsträckning de omfattas av direktivet. Direktivet gäller dock också för alla andra verksamhetsutövare, dvs. alla fysiska och juridiska personer som inte är en myndighet, region eller en kommun. Utredningen kommer för dem att använda begreppet enskilda verksamhetsutövare. För alla dem är det tillräckligt att de bedriver verksamhet inom EES, omfattas av bilaga 1 eller 2 till direktivet och att de uppfyller storlekskravet för medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG. Som kommer att framgå av kapitel 6 kommer det finnas en skyldighet för den enskilde verksamhetsutövaren som omfattas att anmäla sig till tillsynsmyndigheten och att lämna uppgifter om bland annat verksamheten.

Syftet med NIS2-direktivet är att det ska vara enklare än tidigare för den enskilde verksamhetsutövaren att veta om verksamheten omfattas av lagens krav, det är tillräckligt att verksamhet bedrivs inom sektorn och att storlekskravet är uppfyllt. När det gäller storlekskravet är det förstås oftast enkelt, det som möjligen kan innebära svårigheter är bedömningen i särskilda fall för exempelvis partnerföretag, se avsnitt 5.2.2. När det vidare gäller om verksamhetsutövaren omfattas av sektorn föreslår utredningen på samma sätt som tidigare lag en direkt hänvisning till bilagorna I NIS2-direktivet. Skälet är att NIS2-direktivet i denna del innehåller en omfattande klassificering i såväl sektorer som undersektorer. Det innebär att avgörande för om verksamhetsutövaren omfattas eller inte är en tolkning av NIS2-diektivet i denna del. Utredningen bedömer att detta i de flesta fall inte innebär några svårigheter. Som dock framgår av kapitel 4 finns det dock några oklarheter, det kan exempelvis krävas en tolkning inte bara av NIS2-direktivet utan även av andra direktiv. Så är till exempelvis fallet för sektorn energi och undersektorn elektricitet i bilaga 1 till NIS2-direktivet. Med hänsyn till det föreslår utredningen att regeringen ger tillsynsmyndigheterna i uppdrag att med stöd av MSB utformar en vägledning om de oklarheter som kan

föreligga i sektorsbeskrivningarna till stöd för den enskilde verksamhetsutövaren. Detta arbete behöver med hänsyn till frågornas vikt slutföras skyndsamt.

Därutöver kommer det förstås att ankomma på tillsynsmyndigheten att vidta åtgärder mot verksamhetsutövare som omfattas av bilagorna, men inte uppfyller sin anmälningsskyldighet.

Sammantaget betyder det anförda enligt utredningens bedömning att det inledningsvis till dess vägledning är på plats från tillsynsmyndighet i enstaka fall kan framstå som oklart för verksamhetsutövaren om NIS2-direktivets skyldigheter gäller.

Med juridiska personer avses förstås till exempel aktiebolag, handelsbolag eller en förening. En enskild firma är inte en juridisk person utan en fysisk, den drivs i stället av den enskilde näringsidkaren. Som redovisats ovan i avsnitt 5.2.1 ger NIS2-direktiveten möjlighet att meddela undantag för de juridiska personer som inte i sig uppfyller storlekskravet, men gör det genom sin anknytning exempelvis till ett moderbolag. Enligt direktivet får så ske när det är proportionellt. Utredningen föreslår att det av förordningen följer att sådana undantag får meddelas efter ansökan till tillsynsmyndigheten när skäl finns. Skäl kan föreligga när den juridiska personen inte i sig uppfyller storlekskravet och därutöver vid en sammantagen bedömning med utgångspunkt från lagens syfte inte behöver omfattas.

5.2.13 Övriga särskilda kvalificeringsgrunder för enskilda verksamhetsutövare

Utredningens förslag: Verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner, DNS-tjänster eller domännamnsregistrering behöver inte uppfylla storlekskravet för medelstort företag. Detsamma gäller om verksamheten

1. är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner,
2. en störning kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet, folkhälsa eller medföra

betydande systemrisker särskilt om det får gränsöverskridande konsekvenser, eller

3. är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av denna verksamhet omfattas också av lagen.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter.

Artikel 2.2 a–e innehåller sammantaget åtta särskilda kvalificeringsgrunder för verksamhetsutövare som inte uppfyller storlekskravet. Det behöver vara enskilda verksamhetsutövare, eftersom storlekskravet inte gäller för myndigheter och samtliga regioner bedöms uppfylla det. För kommuner är bedömningen att alla eller i vart fall en stor majoritet av kommunerna bör uppfylla det och som framgått föreslår utredningen i fullständighetens namn att samtliga kommuner omfattas.

Det anges att verksamheter som pekas ut i bilaga 1 eller 2 och som inte uppfyller storlekskravet ändå omfattas om någon av de åtta kvalificeringsgrunderna är uppfylld. De två första återfinns i artikel 2.2 a och avser vissa elektroniska tjänster. De som avses är följande:

1. Tjänster tillhandahålls av tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, och

2. tjänster tillhandahålls av tillhandahållare av betrodda tjänster.

Elektronisk kommunikation regleras i lagen (2022:482) om elektronisk kommunikation (LEK). Allmänt elektroniskt kommunikationsnät är i lagens 1 kap. 7 § definierat som ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stöder informationsöverföring mellan nätanslutningspunkter. Tillhandahållare behöver som huvudregel enligt lagens 2 kap. 1 § anmäla tillhandahållandet av allmänna elektroniska kommunikationsnät som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster till PTS.

Med betrodd tjänst avses en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av

a) skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller

b) skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller

c) bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster.

Innebörden av det anförda är det av LEK framgår vad som avses med tillhandahållare av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. Enligt definitionerna i artikel 6 punkt 24 och 25 i NIS2-direktivet hänvisas beträffande betrodd tjänst och tillhandahållare av betrodd tjänst till förordning (EU) nr 910/2014.[22] Med tillhandahållare av betrodda tjänster avses enligt EU-förordningen nr 910/2014 en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerade eller icke kvalificerade tillhandahållare av betrodda tjänster.

Det ska noteras att i den nu gällande NIS-lagen är enligt 5 § leverantörer av elektroniska kommunikationsnät med hänsyn till regleringen i LEK undantagna från NIS-lagen. Detsamma gäller enligt 6 § för leverantörer av betrodda tjänster med hänvisning till ovan nämnda EU-förordning.

Undantaget med hänsyn till LEK trädde i kraft under 2022 samtidigt som LEK trädde i kraft. Det innebar dock ingen sakändring, utan en ändring med hänsyn till att LEK ersatte den tidigare lagen (2003:389) om elektronisk kommunikation[23]. Undantagen var i stället en följd av undantag i NIS-direktivet.[24]

I NIS2-direktivet saknas motsvarande undantag. Det finns alltså inget undantag varken för elektronisk kommunikation eller betrodda tjänster i stort som i artikel 1.3 i NIS-direktivet. I stället är det t.o.m.

[22] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.
[23] Prop. 2021/22:136 s. 100.
[24] SOU 2017:36, s. 284 och 285.

så att detta omfattas av NIS2-direktivet inte bara om storlekskravet är uppfyllt utan även för mindre sådana verksamhetsutövare.

I artikel 2.2 a anges också att även registreringsenheter för toppdomäner och leverantörer av domännamnssystemtjänster omfattas av NIS2-direktivet, även om storlekskravet inte är uppfyllt.

Registreringsenheter för toppdomäner är definierade i artikel 6 punkt 21. Utredningen kommer att i förslag till den nya lagen, cybersäkerhetslagen, definiera de olika begreppen i det inledande kapitlet.

Vidare följer av 2.2 b–e ytterligare fyra särskilda kvalificeringsgrunder, varav följer att vissa verksamheter ändå ska omfattas av direktivets krav trots att de inte uppfyller storlekskravet. Dessa är följande:

1. Om verksamheten är den enda leverantören av en tjänst i medlemsstaten som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,
2. om en störning av den tjänst som verksamheten tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa,
3. om en störning av den tjänst verksamheten tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser, och
4. verksamheten är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer i medlemsstaten som är beroende av denna verksamhet.

Som framgår krävs det en bedömning av dessa särskilda krav för att mindre verksamheter ändå ska omfattas Begreppen är inte definierade i artikel 6 i direktivet och saknar också direkt motsvarighet i NIS-lagen. Som en jämförelse kan nämnas att det av 4 § NIS-lagen följer att regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om vilka tjänster som är samhällsviktiga och innebörden av en betydande störning. I NIS-förordningen anges sedan i 3 § att MSB får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela föreskrifter om vilka tjänster som är samhällsviktiga tjänster samt att föreskrifterna ska uppdateras minst vartannat år. Av 4 § följer vilka sektoröverskridande faktorer som ska beaktas vid bedömningen av betydande störning samt att

MSB får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela ytterligare föreskrifter om vad som avses med en betydande störning.

Detta har MSB sedan gjort i Anmälan och identifiering av leverantörer av samhällstjänster, (MSBFS 2021:9).

Utredningen föreslår nu en liknande systematik med innebörd att det av lagen följer övergripande kriterier för vilka mindre verksamheter som ska omfattas trots att de inte uppfyller storlekskravet och att det i föreskrifter anges vilka verksamheter som uppfyller något kriterium. Det är självklart att föreskrifterna vid behov bör uppdateras.

Av artikel 2.3 följer att även verksamheter som av Sverige som bedöms som kritiska enligt artikel 6 i CER-direktivet ska omfattas av NIS2-direktivets krav. Utredningen kommer att i sitt slutbetänkande återkomma till denna fråga.

Slutligen följer av artikel 2.4 att även verksamhetsutövare som tillhandahåller dommännamnsregistrering ska omfattas av NIS2-direktivet även om storlekskravet inte är uppfyllt. Sådana verksamhetsutövare definieras i artikel 6 punkt 22.

5.2.14 Utbildningsinstitut

Utredningens bedömning: Lärosäten med examenstillstånd bör omfattas av cybersäkerhetslagen.

Som framgått ovan får medlemsstaterna, enligt artikel 2.5 b, föreskriva att direktivet ska tillämpas på utbildningsinstitut, särskilt om de utför kritisk forskningsverksamhet. NIS2-direktivet innehåller ingen definition av begreppet utbildningsinstitut. Enligt kommittédirektivet ska utredningen överväga om universitet och högskolor, eller ett urval av dessa, bör omfattas av den nya regleringen. Utredningen ska ta hänsyn till principer som säkerställer akademisk frihet, institutionell autonomi och forskningsintegritet samt excellens och öppenhet inom högre utbildning och forskning.

Högre utbildning och forskning i Sverige bedrivs till största delen vid statliga universitet och högskolor. Det finns också några enskilda, icke statliga utbildningsanordnare. Gemensamt kan dessa benämnas lärosäten och utredningen tolkar att det är dessa som avses med begreppet utbildningsinstitut i NIS2-direktivet. Universitets-

och högskolesektorns utgifter för forskning och utveckling (FoU) under 2021 uppgick till cirka 43 miljarder, vilket motsvarar 23 procent av Sveriges totala FoU-utgifter.[25] Jämfört med många andra länder bedrivs endast en liten del av forskningen i Sverige av forskningsinstitut.[26]

Det finns 49 lärosäten i Sverige som har examenstillstånd. Ett flertal av dessa är statliga lärosäten som är egna myndigheter. En stor del av lärosätena kommer därmed att omfattas av regleringen i egenskap av statlig myndighet, i sektorn offentlig förvaltning, under förutsättning att utredningen inte föreslår ett undantag för dem.

Forskning är en egen sektor i NIS2-direktivet som inte innefattar utbildningsinstitutioner. Att relativt liten andel av forskningen i Sverige bedrivs i forskningsinstitut talar enligt utredningen för att inkludera lärosäten i regleringen. Resultatet skulle annars bli att en större del av den forskning som bedrivs i Sverige inte skulle omfattas av NIS2-direktivet. Detta skulle gå emot direktivets syfte.

Riksrevisionen har granskat informationssäkerheten vid 24 lärosäten som bedriver naturvetenskaplig och teknisk forskning.[27] Riksrevisionens övergripande slutsats är att universitet och högskolor inte bedriver ett effektivt informationssäkerhetsarbete för att skydda forskningsdata. Detta trots att föreskriftskrav funnits sedan 2008 och bristerna varit kända sedan länge.

Utredningen anser med hänsyn till att omfattande forskning bedrivs vid lärosäten som har examenstillstånd och de brister som framkommit i Riksrevisionens rapport att dessa bör omfattas av cybersäkerhetslagens tillämpningsområde.

Nästa steg blir då att bedöma om det finns skäl som talar emot att inkludera lärosäten i regleringen.

Forskningens frihet är skyddad i 2 kap. 18 § regeringsformen och vidare reglerad i 1 kap. 6 § högskolelagen (1992:1434). Det innebär att forskningsproblem fritt får väljas, forskningsmetoder fritt får utvecklas och forskningsresultat fritt får publiceras. 2021 skrevs även akademisk frihet in i 1 kap. 6 § högskolelagen. Här framgår att som allmän princip i högskolornas verksamhet ska gälla att den akademiska friheten ska främjas och värnas. Att en allmän princip om akademisk frihet infördes i högskolelagen innebär dock inte att hög-

[25] SCB, Forskning och utveckling vid universitet och högskolor 2021.
[26] https://www.uka.se/sa-fungerar-hogskolan/forskning-vid-universitet-och-hogskolor.
[27] *Informationssäkerhet vid universitet och högskolor – hanteringen av skyddsvärda forskningsdata* (RiR 2023:20).

skolan eller de verksamma vid högskolan står fria från styrning eller reglering. Det fria kunskapssökandet och den fria kunskapsspridningen ska alltid utövas inom de rättsliga ramar som finns.[28] Utredningen bedömer inte att cybersäkerhetslagen innebär sådana inskränkningar i dessa principer vilket skulle motivera att inte inkludera lärosäten i regleringen.

Utredningen har övervägt att endast inkludera ett urval av universitet och högskolor i regleringen. Ett sådant urval skulle till exempel kunna göras utifrån storlek eller typ av forskning som bedrivs vid lärosätet. Som framgått ovan i avsnitt 5.2.8 innehåller NIS2-direktivet ett storlekskrav för enskilda verksamhetsutövare. En förutsättning är därför att icke-statliga lärosäten uppfyller storlekskravet på minst 50 anställda eller har en omsättning eller balansomslutning som överstiger 10 miljoner euro per år. Utredningen har inte funnit anledning att införa ett annat storlekskrav för lärosäten eller att begränsa tillämpningen till någon viss typ av forskning.

Utredningen föreslår därför att samtliga lärosäten med examenstillstånd som uppfyller storlekskravet ska omfattas av cybersäkerhetslagen.

5.3 Jurisdiktion

Ovan har tillämpningsområdet för NIS2-direktivet analyserats och utredningen har dragit slutsatser om vem som omfattas av direktivet. För att klarlägga vem som omfattas inte bara av direktivet utan av utredningens förslag till en ny lag behöver dock även Sveriges jurisdiktion analyseras. Den är reglerad i artikel 26. Bestämmelserna är olika för offentliga verksamhetsutövare jämfört med enskilda verksamhetsutövare och det finns därutöver särskilda jurisdiktionsbestämmelser för vissa enskilda verksamhetsutövare.

[28] Prop. 2020/21:60 s. 131.

5.3.1 Jurisdiktion för offentliga verksamhetsutövare

Utredningens förslag: Lagen ska som utgångspunkt omfatta svenska statliga myndigheter med undantag av regeringen, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och domstolarna samt svenska regioner och kommuner med undantag av kommunfullmäktige och regionfullmäktige.

Av artikel 26.1 följer att huvudregeln är att verksamhetsutövare som omfattas av direktivets tillämpningsområde ska anses omfattas av jurisdiktionen i den medlemsstat där de etablerade. För offentliga verksamhetsutövare gäller i stället att de ska omfattas av jurisdiktionen i den medlemsstat som inrättade dem. För Sveriges del betyder det svenska myndigheter samt svenska regioner och kommuner.

5.3.2 Jurisdiktion för enskilda verksamhetsutövare

Utredningens förslag: Enskilda fysiska eller juridiska personer som omfattas av direktivet ska som huvudregel omfattas av cybersäkerhetsregleringen om de är etablerade i Sverige.

För tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster gäller i stället att de omfattas av lagen om de erbjuder tjänster i Sverige.

Gränsöverskridande verksamhetsutövare är verksamhetsutövare som erbjuder DNS-tjänster, registreringsenheter för toppdomäner, domännamnsregistreringstjänster, molntjänster, datacentraltjänster, nätverk för leverans av innehåll, hanterade tjänster, hanterade säkerhetstjänster eller marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster.

Gränsöverskridande verksamhetsutövare som erbjuder tjänster inom EES, men saknar etablering där ska utse en företrädare med etablering i något av de länder där tjänster erbjuds.

För gränsöverskridande verksamhetsutövare krävs det i stället för etablering att Sverige är huvudsakligt etableringsställe eller att företrädaren är etablerad i Sverige för att verksamhetsutövaren ska omfattas av lagen. Därutöver gäller kapitel 5 för gränsöver-

skridande verksamhetsutövare som erbjuder tjänster i Sverige, men inte utser en företrädare.

Regeringen får meddela föreskrifter om vad som utgör huvudsakligt etableringsställe. Vid bedömningen ska i första hand plats för beslut om riskhanteringsåtgärder för cybersäkerhet vara avgörande, därefter platsen för cybersäkerhetsverksamhet och i sista hand plats där verksamhetsutövaren har flest anställda.

Huvudregeln för enskilda verksamhetsutövare är enligt artikel 26.1 att det medlemsland där verksamheten är etablerad har jurisdiktion. Den som bedriver en faktisk och reell verksamhet med hjälp av en stabil struktur anses vara etablerad. Den rättsliga formen för en sådan struktur, dvs. om det är fråga om exempelvis en filial eller ett dotterbolag, är inte en avgörande faktor.[29] Det betyder att de som omfattas av direktivet utifrån vad utredningen anfört ovan ska som huvudregel innefattas av lagen om de är etablerade i Sverige.

För tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster gäller i stället att de enligt artikel 26.1 a omfattas av jurisdiktionen i det land de tillhandahåller sina tjänster. Det betyder alltså att en sådan verksamhetsutövare ska omfattas av lagen om tjänster tillhandahålls i Sverige.

Huvudregeln för regeln om etablering respektive tillhandahållandet av tjänster är att om verksamhetsutövaren är etablerad i flera medlemsländer respektive tillhandahåller tjänster i flera medlemsländer har samtliga dessa länder jurisdiktion. Det följer av skäl 113. Där anges också att medlemsländerna i dessa fall bör samarbeta samt att efterlevnadskontrollåtgärder och sanktioner inte bör påföras mer än en gång för samma handling enligt principen om ne bis in idem, dvs. förbud mot dubbelprövning och dubbelbestraffning.

För gränsöverskridande verksamhetsutövare finns det dock en särregel. De som här kommer i fråga är enligt artikel 26.1 b verksamhetsutövare som tillhandahåller DNS-tjänster, registreringsenheter för toppdomäner, verksamhetsutövare som tillhandahåller domännamnsregistreringstjänster, molntjänster, datacentraltjänster, nätverk för leverans av innehåll, hanterade tjänster, hanterade säkerhetstjänster, marknadsplatser online, sökmotorer eller plattformar för sociala

[29] Skäl 21 i det tidigare NIS-direktivet och prop. 2017/18:205 s. 21.

nätverkstjänster. För dem gäller att ett medlemsland har jurisdiktion endast om det huvudsakliga etableringsstället ligger i landet. Det följer av skäl 114 att anledningen till denna särregel är att endast ett medlemsland bör ha jurisdiktion över dessa verksamheter.

Vid bedömningen om vad som utgör ett huvudsakligt etableringsställe är i första hand platsen för beslut om riskhanteringsåtgärder för cybersäkerhet vara styrande, i andra hand platsen för cybersäkerhetsoperationer och i sista hand ska det etableringsställe som har flest anställda vara styrande. Detta föreslås framgå av förordningen.

För dessa verksamhetsutövare gäller också enligt artikel 26.3 att om det saknas etablering inom unionen, men tjänster erbjuds där ska en företrädare utses. Företrädaren ska vara etablerad i ett av medlemsländerna där tjänster erbjuds och det medlemslandet har jurisdiktion. Om en företrädare inte utses får varje medlemsland där verksamhet bedrivs vidta rättsliga åtgärder mot verksamhetsutövaren.

För den svenska lagens del innebär det att det i lagen bör införas en bestämmelse om att gränsöverträdande verksamhetsutövare som erbjuder tjänster inom EES, men saknar etablering där ska utse en företrädare med etablering i något av de länder där tjänster erbjuds.

I artikel 26.4 anges det att det faktum att en gränsöverskridande verksamhetsutövare utsett en företrädare inte ska påverka eventuella rättsliga åtgärder mot verksamhetsutövaren. Det menar utredningen behöver inte anges specifikt, eftersom det är självklart så länge det inte särskilt anges att sanktioner ska riktas mot företrädaren om sådan utsetts. Av artikel 26.5 följer att de medlemsstater som mottagit en begäran om ömsesidigt bistånd avseende gränsöverskridande verksamhetsutövare får vidta lämpliga tillsyns- och efterlevnadskontrollåtgärder för verksamhetsutövaren som erbjuder tjänster eller som har ett nätverks-och informationssystem inom landets territorium. Enligt utredningens bedömning krävs det inte heller en särskild reglering om detta, eftersom avgörande för åtgärder är den nationella lagregleringen.

5.4 Undantag för sektorsspecifika unionsrättsakter och andra författningar

Utredningens förslag: Om annan författning innehåller bestämmelser om krav på riskhanteringsåtgärder eller incidentrapportering för en verksamhetsutövare med motsvarande verkan gäller inte kraven i cybersäkerhetslagen om riskhanteringsåtgärder incidentrapportering för verksamhetsutövaren. Vid jämförelsen av verkan mellan författningarna ska hänsyn tas till bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till bestämmelserna.

Regeringen får i föreskrifter ange vilka andra bestämmelser om riskhanteringsåtgärder och incidentrapportering som har motsvarande verkan.

Redan nu bör det av förordningen följa att finansiella verksamhetsutövare som omfattas av Dora-förordningen inte ska omfattas av riskhanterings- och rapporteringsskyldigheter enligt cybersäkerhetslagen. Som följd kommer då inte heller tillsyns- och efterlevnadskontroll i denna del enligt lagen gälla för dem.

Lagen ska inte tillämpas på verksamheter som undantagits enligt artikel 2.4 i Dora-förordningen.

I artikel 4 i direktivet finns ett särskilt undantag för riskhanteringsåtgärder och rapportering om betydande incidenter. Innebörden är att om det i sektorsspecifika unionsrättsakter redan finns krav om sådana åtgärder med minst samma verkan ska NIS2-direktivets krav inte gälla.

Om de sektorsspecifika unionsrättsakterna inte omfattar alla verksamhetsutövare inom sektorn ska NIS2-direktivets bestämmelse gälla för dem som inte omfattas.

Vid bedömningen av vad som är samma verkan ska för riskhanteringsåtgärder kraven i artikel 21.1 och 21.2 i NIS2-direktivet beaktas, se vidare kapitel 7.

Alternativt kan bestämmelserna i den sektorsspecifika unionsrättsakten enligt artikel 4.2.b anses ha samma verkan om det i den föreskrivs att tillgång på ett visst sätt till incidentunderrättelser från CSIRT-enheter, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt NIS2-direktivet. En ytterligare förutsätt-

ning är att kraven på underrättelse av betydande incidenter har minst samma verkan som kraven i artikel 23.1–23.6 i NIS2-direktivet. I dessa bestämmelser finns långtgående och detaljerade krav om rapporteringsskyldigheten, se vidare kapitel 7.

Slutligen anges i artikel 4 också att kommissionen senast i juli 2023 ska tillhandahålla riktlinjer för bedömningen minst samma verkan. Riktlinjerna ska regelbundet ses över. Sådana riktlinjer har presenterats.[30]

Dora-förordningen trädde i kraft i januari 2023 och ska börja tillämpas från och med den 17 januari 2025.[31] I direktivets skäl 28 anges särskilt att Dora-förordningen är en sådan sektorsspecifik unionsrättsakt och att medlemsstaterna inte bör tillämpa NIS2-direktivets bestämmelser om riskhanterings- och rapporteringsskyldigheter på finansiella verksamhetsutövare som omfattas av Dora-förordningen.

Av regeringens direktiv följer också att utredningen behöver beakta relevanta sektorsspecifika unionsrättsakter när det gäller vilka krav som ska ställas på verksamheterna, hur rollfördelningen mellan svenska myndigheter ska se ut och vilka befogenheter tillsynsmyndigheterna ska ha.

Enligt utredningens bedömning skulle en ingående analys av Dora-förordningens bestämmelser och andra unionsrättsakter som skulle kunna avses vara ett omfattande och tidskrävande arbete, som inte ryms inom utredningens tidsplan. Det ska också beaktas att det framöver kan tillkomma unionsrättsakter som utredningens förslag till lagstiftning också behöver ta höjd för. Detta talar enligt utredningens bedömning i stället för ett generellt utformat undantag.

I NIS-lagen finns också redan ett liknande sådant generellt undantag i 9 §, där det anges att om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder och incidentrapportering ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt denna lag, med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna. Paragrafen är inte preciserad i förordning eller föreskrifter.

[30] https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive, inhämtat 2024-01-19.
[31] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

Paragrafen innebär att lagen inte ska tillämpas om det i lag eller annan författning finns bestämmelser om krav på säkerhetsåtgärder och incidentrapportering vars verkan minst motsvarar verkan av skyldigheterna enligt lagen. Med lag eller annan författning avses även EU-förordningar och myndighetsföreskrifter.[32]

Bakgrunden till bestämmelsen var att det i artikel 1.7 i NIS-direktivet anges att bestämmelser i sektorsspecifika EU-rättsakter, som innehåller krav på leverantörer av samhällsviktiga eller digitala tjänster att säkerställa säkerheten i sina nätverk och informationssystem eller att rapportera incidenter, tillämpas i stället för bestämmelserna i direktivet förutsatt att verkan av kraven i fråga minst motsvarar verkan av skyldigheterna enligt direktivet.

Regeringen menade efter förslag från Utredningen om genomförande av NIS-direktivet att det i den nya lagen borde införas en motsvarande bestämmelse, som skulle gälla oavsett om bestämmelserna finns i EU:s rättsakter eller i nationella författningar. Vidare framhöll regeringen att vid bedömningen av om bestämmelser om säkerhetsåtgärder och incidentrapportering motsvarar verkan av skyldigheterna enligt den nya lagen, bör man bland annat beakta bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna. På Lagrådets inrådan föreslogs detta framgå av lagtexten. Regeringen angav också att exempel på bestämmelser om säkerhetsåtgärder och incidentrapportering som inte kunde anses ha motsvarande verkan är bestämmelserna i förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap samt dataskyddsförordningen. En följd skulle då bli att leverantörer behövde tillämpa dessa regelverk parallellt. Slutligen ansåg regeringen också att enstaka bestämmelser som innehåller krav på säkerhetsåtgärder eller incidentrapportering inte ska gälla i stället för motsvarande bestämmelser i den nya lagen, eftersom det inte vore ändamålsenligt. Det skulle också i mycket begränsad omfattning finnas nationella bestämmelser som innehåller krav som kan anses motsvara kraven enligt NIS-direktivet.[33]

Sammantaget drar utredningen den slutsatsen att det i lagen ska föras in ett generellt undantag som motsvarar artikel 4. Det kommer att ha likheter med nuvarande 9 §. Inledningsvis menar utredningen att det precis som i 9 § i lagen bör hänvisas till annan författning av

[32] Prop. 2017/18:205 s. 93.
[33] Prop. 2017/18:205 s. 29.

skäl som anfördes i propositionen till NIS-lagen. Det framstår också som ändamålsmässigt att hänvisning görs såväl till verkan av skyldigheterna enligt denna lag, med beaktande av bestämmelsernas omfattning som till tillsyn och sanktioner.

Till utredningen har dock framförts att tillämpningen av 9 § är svår. En skillnad föreligger också i att kommissionen ska meddela riktlinjer, som ska uppdateras enligt artikel 4. Från Svenska Bankföreningen har uppgetts att banker inte tillämpar paragrafen, eftersom osäkerhet föreligger om bedömningen.

Med hänsyn till det anförda och frågans komplexitet föreslår utredningen att regeringen i en bilaga till förordningen pekar ut de författningar som innehåller bestämmelser med krav om riskhanteringsåtgärder och rapportering om betydande incidenter som motsvarar verkan av skyldigheterna enligt denna lag. Bestämmelserna i bilagan bör beredas av den eller de myndigheter som regeringen finner lämpligt.

Redan nu bör det av förordningen följa att Dora-förordningen bör betraktas som en sådan sektorsspecifik unionsrättsakt som lever upp till kraven om att verkan sammantaget motsvarar skyldigheterna enligt utredningens förslag till lag. Det innebär att finansiella verksamhetsutövare som omfattas av Dora-förordningen inte ska omfattas av riskhanterings- och rapporteringsskyldigheter enligt lagen. Som följd kommer då inte heller tillsyns- och efterlevnadskontroll enligt lagen gälla för dem. Innebörden blir att dessa verksamhetsutövare endast kommer att omfattas av kraven i artikel 3 och artikel 27, som avser anmälan och registrering samt de ingripanden och sanktioner som kan gälla för dessa krav.

Grunden för detta är skäl 28 som uttryckligen anger att medlemsstaterna inte bör tillämpa detta direktivs bestämmelser om risk- och rapporteringsskyldigheter, tillsyn och efterlevnadskontroll beträffande cybersäkerhet på finansiella verksamhetsutövare som omfattas av denna förordning.

I artikel 2.2.10 anges att NIS2-direktivet inte ska tillämpas på verksamheter som medlemsstaterna har undantagit från Dora-förordningen enligt den förordningens artikel 2.4. För Sveriges del rör det sig om Svenska Skeppshypotekskassan. Medlemsstaten behöver underrätta kommissionen om sådana undantag. Sverige har ännu inte genomfört sådana undantag, men kan förstås komma att göra det i framtiden. Av lagen bör därför följa att den inte är tillämplig för sådana meddelade undantag.

5.5 Undantag för Sveriges säkerhet och brottsbekämpning

I detta avsnitt ska avgränsningen till säkerhetskänsligt och brottsförebyggande arbete analyseras.

5.5.1 Bestämmelserna i direktivet

Av artikel 2.6 följer att direktivet inte påverkar medlemsstaternas ansvar för att skydda nationell säkerhet och andra väsentliga statliga funktioner inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning.

I artikel 2.7 anges vad som gäller för offentliga verksamhetsutövare i den delen och av artikel 2.8 följer hur detta ska påverka andra verksamhetsutövare. Slutligen framgår av artikel 2.9 att undantagen i artikel 2.7 och 2.8 inte ska gälla för en verksamhetsutövare som agerar som en tillhandahållare av betrodda tjänster.

Tillhandahållare av betrodda tjänster definieras som framgått av avsnitt 5.2.13 enligt artikel 6 punkt 25 i artikel 3.19 i förordning (EU) nr 910/2014.[34] Definitionen där är en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av

a) skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller

b) skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller

c) bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster.

[34] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

5.5.2 Säkerhetsskyddslagen

Säkerhetsskyddslagen (2018:585) reglerar skyddsåtgärder för de mest skyddsvärda verksamheterna i samhället. Den gäller för alla som till någon del bedriver verksamhet av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet). Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.

Systematiken i lagen bygger på att det är verksamhetsutövaren själv som till någon del bedriver säkerhetskänslig verksamhet som ska utreda behovet av säkerhetsskydd (säkerhetsskyddsanalys). Säkerhetsskyddsanalysen ska identifiera vilka säkerhetsskyddsklassificerade uppgifter och vilken säkerhetskänslig verksamhet i övrigt som finns i verksamheten. Vidare ska verksamhetsutövaren i analysen specificera vilka delar av verksamheten som är säkerhetskänslig.[35]Analysen ska dokumenteras och med utgångspunkt i den ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.[36] Säkerhetsskyddsåtgärder avser informationssäkerhet, fysisk säkerhet och personalsäkerhet.[37] Med informationssäkerhet avses bland annat att förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs. Säkerhetsskyddsklassificerade uppgifter är uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.[38] Verksamhetsutövare ska också utan dröjsmål anmäla att den bedriver säkerhetskänslig verksamhet till tillsynsmyndigheten.[39]

[35] 2 kap. 2 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1).
[36] 2 kap. 1 §.
[37] 2 kap. 2–4 §§.
[38] 1 kap. 2§ andra stycket.
[39] 2 kap. 6 §.

5.5.3 Undantag för säkerhetsskyddsklassificerade uppgifter

Utredningens förslag: Skyldighet att lämna uppgifter enligt denna lag gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585).

Ovan redovisade artikel 2.6 ger möjlighet till undantag med hänsyn till nationell säkerhet och andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning. Av skäl 9 i andra delen framgår också att ingen medlemsstat bör vara skyldig att lämna information vars avslöjande skulle strida mot dess väsentliga intressen i fråga om nationell säkerhet, allmän säkerhet eller försvar. Unionsregler eller *nationella regler* till skydd för *säkerhetsskyddsklassificerade uppgifter*, sekretessavtal samt informella sekretessavtal såsom Traffic Light Protocol bör beaktas i detta sammanhang.

Direktivets skyldigheter för verksamhetsutövare handlar till stor del om rapportering och information. Av regeringens direktiv följer att för att säkerställa att säkerhetsskyddsklassificerade uppgifter inte lämnas ut är det inte tillräckligt att särskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet helt eller delvis kan undantas från direktivens krav på bland annat incidentrapportering. Det behöver enligt regeringen också säkerställas att uppgifter som rör säkerhetskänslig verksamhet inte registreras i den europeiska sårbarhetsdatabas som enligt NIS2-direktivet ska upprättas av Enisa (The European Union Agency for Cybersecurity). Det behöver därför införas regler som direkt undantar säkerhetsskyddsklassificerade uppgifter från såväl rapporteringskraven som från annan uppgiftslämning som regleras i direktiven.

Utredningen delar regeringens uppfattning och föreslår därför att det i lagen förs in ett undantag som anger att lagens skyldigheter att lämna uppgifter inte avser säkerhetsskyddsklassificerade uppgifter enligt säkerhetsskyddslagen.

5.5.4 Undantag för offentliga verksamhetsutövare

Utredningens förslag: Statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning omfattas inte av lagen.

Regeringen får i föreskrifter ange vilka statliga myndigheter som bedriver säkerhetskänslig verksamhet eller brottsbekämpning till övervägande del.

För andra statliga myndigheter, regioner och kommuner som bedriver säkerhetskänslig verksamhet eller brottsbekämpning gäller för den säkerhetskänsliga verksamheten och brottsbekämpningen inte kraven om att utse en företrädare, riskhanteringsåtgärder och incidentrapportering och inte heller bestämmelserna om tillsyn och sanktioner som avser detta. Innebörden är att för denna del av verksamheten kommer enbart anmälningsskyldigheten i artikel 3 som är genomförd i 2 kap. 2 § cybersäkerhetslagen att gälla. Som en följd kommer tillsyns- och sanktionsbestämmelser som hänför sig till dem att gälla. För den del av verksamheten som inte är säkerhetskänslig eller avser brottsbekämpning gäller cybersäkerhetslagen i dess helhet.

Av artikel 2.7 följer att direktivet inte är tillämpligt på offentliga verksamhetsutövare som bedriver verksamhet inom områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning. I brottsbekämpning ingår förebyggande, utredning, upptäckt och lagföring av brott. Utformningen i artikel 2.7 är alltså obligatorisk. Samtidigt är hela direktivet enligt artikel 5 ett minimidirektiv med innebörd att medlemsstaten får anta bestämmelser som säkerställer en högre cybersäkerhetsnivå. Det skulle för denna artikel kunna innebära att utredningen inte får undanta offentliga verksamhetsutövare i större utsträckning från cybersäkerhetslagen än vad som anges i artikel 2.7, däremot i mindre utsträckning.

Av skäl åtta följer vidare att undantaget i 2.7 bör omfatta offentliga verksamhetsutövare vars verksamhet *till övervägande del* bedrivs inom det angivna området, men att offentliga verksamhetsutövare vars verksamhet endast marginellt berör områdena inte bör vara undantagna. Vid tillämpningen anses verksamhetsutövare med tillsynsbefogenheter inte bedriva verksamhet på brottsbekämpningsområdet och är därför inte undantagna.

I skälet anges vidare att offentliga verksamheter som inrättats gemensamt med ett tredjeland i enlighet med ett internationellt avtal samt medlemsländernas diplomatiska och konsulära beskickningar i tredje länder eller nätverks- och informationssystem som drivs för användare i ett tredje land inte omfattas av direktivet.

Inom unionsrätten är nationell säkerhet ett vedertaget begrepp, men saknar en tydlig definition.[40] Med allmän säkerhet avses inom unionsrätten skydd av en medlemsstats institutioner, dess väsentliga offentliga tjänster och dess invånares överlevnad, och kan innefatta både en medlemsstats yttre och inre säkerhet.[41] I Sverige används begreppet Sveriges säkerhet, som innefattar såväl yttre som inre säkerhet. Med yttre säkerhet avses territoriell suveränitet och politisk självständighet. För den nationella försvarsförmågan av Sveriges territorium bär Försvarsmakten huvudansvaret. Inre säkerhet avser förmågan att upprätthålla och säkerställa Sveriges statsidé avseende funktion, handlingsfrihet och oberoende. Säkerhetsskyddet för Sveriges inre säkerhet handlar till stor del om att skydda särskilt kritiska anläggningar, funktioner och informationssystem för Sveriges demokratiska statsskick, rättsväsende eller brottsbekämpande förmåga. Ett annat begrepp är samhällsviktig verksamhet som exempelvis energiförsörjning, livsmedelsförsörjning, elektroniska kommunikationer, vattenförsörjning, transporter och finansiella tjänster. Samhällsviktig verksamhet kan, men behöver inte beröra Sveriges säkerhet. Avgörande är om en antagonistisk handling som exempelvis spioneri, sabotage eller terroristbrott skulle kunna medföra skadekonsekvenser på nationell nivå.[42]

En slutsats av det anförda är att enligt artikel 2.7 får Sverige undanta offentliga verksamhetsutövare som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning och får inte undanta utövare som bara marginellt utövar sådan verksamhet. Det finns ett stort spann mellan övervägande del och marginellt och här framstår det som om det finns en valmöjlighet för medlemsländerna. Offentliga verksamhetsutövare som till någon del bedriver säkerhetskänslig verksamhet omfattas alltså av säkerhetsskyddslagen (2018:585).

[40] Prop. 2017/18:89 s. 41.
[41] Prop. 2022/23:116 s. 22.
[42] Prop. 2017/18:89 s. 44.

Med offentliga verksamhetsutövare avses som redovisats under avsnitt 5.2.6 statliga myndigheter inklusive statliga affärsverk samt regioner med undantag av regionfullmäktige. Kommuner ingår inte som framgått tidigare i definitionen av offentliga verksamhetsutövare i bilaga 1 till direktivet. Att de omfattas av direktivet beror i stället på att i vart fall majoriteten av dem uppfyller storlekskravet och bedriver hemsjukvård, vilket betyder att de ingår i området hälso-och sjukvård. Samtidigt har dock utredningen i fullständighetens namn föreslagit att alla kommuner omfattas, dvs. även de som möjligtvis inte uppnår storlekskravet i dessa delar, se avsnitt 5.2.10. Det betyder att även kommunerna behöver inkluderas som utgångspunkt.

Ett stort antal myndigheter bedriver delvis säkerhetskänslig verksamhet. I 8 kap. 1 § säkerhetsskyddsförordningen (2021:955) listas ett stort antal myndigheter som Försvarsmakten eller Säkerhetspolisen är tillsynsmyndigheter för enligt säkerhetsskyddslagen. I bilagan till säkerhetsskyddsförordningen listas vilka statliga myndigheter som beslutar om placeringen i säkerhetsklass. Innebörden av listningen bör dock förstås på det sättet att dessa myndigheter kan bedriva säkerhetskänslig verksamhet. Regeringskansliet ingår inte i uppräkningen, men bedriver självklart också säkerhetskänslig verksamhet. Enligt 1 kap. 3 § säkerhetsskyddslagen gäller att regeringen får i fråga om Regeringskansliet, utlandsmyndigheterna och kommittéväsendet meddela föreskrifter om vissa undantag.

Det har tidigare inte varit självklart att en kommun eller en region som verksamhetsutövare bedriver säkerhetskänslig verksamhet. Regeringen anförde i propositionen till säkerhetsskyddslagen att uttrycket Sveriges säkerhet inte ska tolkas kategoriskt och att skyddsvärda verksamheter kan trots kravet på nationell betydelse finnas på regional eller till och med på lokal nivå. Exempelvis skulle en lokal eller regional störning av dricksvattenförsörjningen påverka ett stort antal människor i en region, vilket i förlängningen kan få nationella följdverkningar. Detta har dock förändrats främst på grund av den återupptagna totalförsvarsplaneringen. Enligt länsstyrelserna bedriver i stort sett alla kommuner och regioner säkerhetskänslig verksamhet i någon del, ofta torde det röra sig om deltagande i totalförsvarsverksamhet.

Det anförda betyder enligt utredningens uppfattning att om utredningen undantar all offentlig verksamhet som till någon del bedriver säkerhetskänslig verksamhet eller brottsbekämpning utom de

som endast gör det marginellt kommer en stor del av den offentliga verksamheten att undantas från cybersäkerhetslagen. Detta är i strid med direktivets syfte. Det kan även förutses att totalförsvarsverksamheten utvecklas och att cybersäkerhetslagen därmed skulle tappa betydelse för den offentliga verksamheten.

I regeringens direktiv anges dock att inriktningen för förslagen ska vara att säkerhetskänslig verksamhet undantas från den nya regleringen i den utsträckning som är möjlig.[43] Här ska dock noteras att undantaget i artikel 2.7 beroende på NIS2-direktivets konstruktion slår mot myndigheters, regioners och kommuners verksamhet som helhet, inte den del som kan täckas av säkerhetsskyddslagen. Grundproblemet är att säkerhetsskyddslagen endast berör den del av verksamheten som är säkerhetskänslig, medan cybersäkerhetslagen som framgått tidigare kommer att omfatta hela verksamheten. För verksamheter som bedriver brottsbekämpning skulle det kunna vara än sämre. De skulle varken omfattas av cybersäkerhetslagen eller säkerhetsskyddslagen, även om de brottsbekämpande myndigheterna oftast bör till någon del bedriva säkerhetskänslig verksamhet. Regeringens utgångspunkt är dock att offentliga verksamhetsutövare som bedriver verksamhet inom områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning är i sin helhet undantagna från direktivets tillämpningsområde.[44]

Ytterst när det gäller artikel 2.7 gäller alltså att det kan finnas ett behov av att undanta endast en del av verksamheten från cybersäkerhetslagen, den säkerhetskänsliga och den del som avser brottsbekämpning. En avgörande fråga är då om detta ändå är möjligt. Det finns som redovisats ovan i avsnitt 5.5.3 ett allmänt undantag i artikel 2.6 för skydd av bland annat nationell säkerhet. Det kan övervägas om det kan användas för att undanta all säkerhetskänslig verksamhet och brottsbekämpning från cybersäkerhetslagen. Skälen ger dock inte stöd för en sådan tolkning, eftersom det i skäl 9 särskilt hänvisas exempelvis till säkerhetsskyddsklassificerade uppgifter. Artikel 2.7 och artikel 2.8 tycks också konkretisera innebörden av artikel 2.6 när de gäller att undanta verksamhetsutövare, verksamhet eller del av verksamhet. Eftersom det i 2.7 finns en särskild artikel om hur offentliga verksamhetsutövare ska undantas bör det vara det som gäller i den delen. Det skulle i sin tur betyda att det finns långtgående möj-

[43] s. 18.
[44] s. 16–17.

lighet att undanta samtliga offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet och brottsbekämpning utom de som endast gör det marginellt i sin helhet från direktivet, men inte endast i den delen. Som utredningen anfört tidigare framstår det inte som en bra lösning att till stora delar undanta den offentliga verksamheten, eftersom det urholkar NIS2-direktivets syfte.

När det gäller att delvis undanta verksamheter avseende cybersäkerhet behöver också övervägas om det medför tekniska och praktiska svårigheter. NIS2-direktivet pekar alltså ut verksamhetsutövarens hela verksamhet. Ett skäl för det är förstås att det när det gäller cybersäkerhet är svårt att dela upp verksamheten, eftersom exempelvis incidenter inom del av verksamheten kan få effekter för hela verksamheten. Detta gäller dock enligt utredningens bedömning i mindre utsträckning för säkerhetskänslig verksamhet, eftersom det oftast förutsätter en högre nivå på tekniska och organisatoriska lösningar. Det ska också noteras att artikel 2.8, se nästa avsnitt, förutsätter att en del av verksamheten undantas. Även när det gäller brottsbekämpning menar utredningen att det är möjligt att undanta den delen, även om det kan medföra merarbete för myndigheten.

En lösning är att utredningen föreslår att endast en begränsad andel av offentliga verksamheter undantas i dess helhet från NIS2-direktivets krav. De som undantas helt bör endast vara de som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning. Vidare bör enligt utredningens bedömning även Regeringskansliet och kommittéväsendet undantas. Det skulle betyda att Sverige endast begränsat utnyttjar möjligheten att undanta hela verksamheter, eftersom det finns en möjlighet att undanta alla verksamheter som inte endast marginellt bedriver säkerhetskänslig verksamhet eller brottsbekämpning. I gengäld föreslår utredningen att endast den säkerhetskänsliga verksamheten och den del av verksamheten som avser brottsbekämpning hos andra statliga myndigheter, regioner och kommuner undantas i huvudsak från krav i NIS2-direktivet, men att den del av verksamheten som inte är säkerhetskänslig eller avser brottsbekämpning fullt ut omfattas av direktivets krav. Det som skulle kunna utgöra grunden för ett sådant förslag är trots den uttryckliga bestämmelsen i artikel 2.7 att direktivet är ett minimidirektiv. I stället för att tvingas undanta nästan hela offentliga verksamheten undantar utredningen endast en del. Det ger en högre cybersäkerhetsnivå, vilket därför är förenligt med artikel 5.

Sammantaget bedömer utredningen att det behövs två olika lösningar beroende på i vilken utsträckning säkerhetskänslig verksamhet eller brottsbekämpning bedrivs. Offentliga verksamheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning bör i sin helhet undantas från cybersäkerhetslagen.

Enligt utredningens bedömning bör detta undantag endast avse myndigheter, eftersom den säkerhetskänsliga verksamhet eller brottsbekämpning som kommuner eller regioner bedriver inte kan vara en övervägande del av deras verksamhet i stort. Enligt skäl 8 ska alltså den del av verksamheten som är säkerhetskänslig eller avser brottsbekämpning ställas i relation till verksamheten som helhet. Utredningen anser också att endast ett begränsat antal myndigheter bedriver säkerhetskänslig eller brottsbekämpande verksamhet till övervägande del.

De myndigheter som skulle vara berörda bör klart framgå av förordningen. Enligt utredningens bedömning bör de myndigheter som bedriver säkerhetskänslig verksamhet till övervägande del vara Försvarsmakten, Säkerhetspolisen, Fortifikationsverket, Försvarets materielverk, Försvarets radioanstalt, Försvarsunderrättelsedomstolen, Statens inspektion för försvarsunderrättelseverksamheten, Totalförsvarets forskningsinstitut och Totalförsvarets plikt- och prövningsverk. Dessa är även undantagna från delar av förordning (2022:524) om statliga myndigheters beredskap. Även Försvarshögskolan är undantagen från delar av den förordningen, men enligt utredningens uppfattning bedriver Försvarshögskolan inte säkerhetskänslig verksamhet till övervägande del.

Till utredningen har framförts att det kan finnas skäl att undanta även Inspektionen för strategiska produkter, ISP, och Säkerhets- och integritetsskyddsnämnden. Enligt utredningens uppfattning har dock båda dessa myndigheter bredare uppdrag, exempelvis är Säkerhets- och integritetsskyddsnämndens uppdrag bland annat att utöva tillsyn över de brottsbekämpande myndigheterna med uppgift att stärka rättssäkerheten och skyddet för den personliga integriteten inom den brottsbekämpande verksamheten.[45] Utredningen finner därför skäl att med undantag av Försvarshögskolan följa samma avgränsning som nämnda förordning.

När det gäller myndigheter vars verksamhet till övervägande del avser brottsbekämpning menar utredningen att enligt svensk rätt bör de myndigheter som betecknas som rättsvårdande myndigheter

[45] https://www.sakint.se, inhämtat 2023-08-30.

vara utgångspunkt. Polismyndigheten, Säkerhetspolisen, Åklagarmyndigheten, Ekobrottsmyndigheten, Sveriges Domstolar, Kriminalvården, Brottsförebyggande rådet, Rättsmedicinalverket, Genteknikmämnden och Brottsoffermyndigheten är rättsvårdande myndigheter.[46] Sveriges Domstolar omfattas inte av NIS2-direktivet.

När det gäller Rättsmedicinalverket och Genteknikmämnden kan man möjligen ifrågasätta om dessa bedriver brottsbekämpning. Här ska beaktas att enligt direktivet avses alltså med brottsbekämpning förebyggande, utredning, upptäckt och lagföring av brott. Rättsmedicinalverket utgör den medicinska länken i rättskedjan, som bidrar till ett rättssäkert samhälle.[47] Verket utfärdar exempelvis rättsintyg om skador och drogtester som kan utgöra bevisning i ett brottmål. Samtidigt utför verket även analyser som får enbart civilrättslig betydelse, exempelvis genom faderskapsutredning. Utredningen föreslår med hänsyn till ett helhetsperspektiv att Rättsmedicinalverket ska omfattas av undantaget. När det dock vidare gäller Genteknikmämnden menar utredningen att denna nämnd inte kan anses bedriva brottsbekämpning och därför inte bör omfattas. Nämnden har till uppgift att via rådgivande verksamhet främja en etiskt försvarbar och säker användning av gentekniken så att människors och djurs hälsa och miljön skyddas. Det sker främst via yttranden till regeringen och myndigheter.[48]

Sammantaget föreslår utredningen att de rättsvårdande myndigheterna med undantag av Genteknikmämnden inte ska omfattas av cybersäkerhetslagen.

Till utredningen har vidare anförts att även Tullverket och Kustbevakningen borde undantas. Även när det gäller dessa myndigheter menar utredningen att de har bredare uppdrag och att det därför finns skäl att följa avgränsningen för rättsvårdande myndigheter. Tullverkets uppdrag är exempelvis att övervaka och kontrollera varuflödet in och ut ur Sverige. Verket ser till att korrekta tullavgifter, skatter och andra avgifter betalas in samt att regler för in- och utförselrestriktioner följs.[49] Utredningen menar att eftersom det handlar om att undanta myndigheter från krav finns det skäl att vara

[46] https://www.regeringen.se/regeringens-politik/rattsvasendet/rattsvasendet-i-statens-budget/, inhämtat 2023-07-05.
[47] https://www.rmv.se, inhämtat 2023-07-07.
[48] https://www.genteknik.se/om-genteknikmamnden/, inhämtat 2023-07-07.
[49] www.tullverket.se/omoss/dethargortullverket/verksamhetochorganisation.4.153f8c8c16ffad23c2215f1.html, inhämtat 2023-08-28.

restriktiv. Undantagen bör därför avse myndigheter med verksamhet där brottsbekämpning utgör en övervägande andel.

När det gäller samtliga dessa myndigheter har Säkerhetspolisen föreslagit att även dessa myndigheter skulle omfattas av cybersäkerhetslagen, men att kraven skulle begränsas till riskhanteringsåtgärder. Däremot skulle de inte omfattas av krav om incidentrapportering och inte heller av tillsyn och sanktioner. Det utgår alltså från en grundsyn om att NIS2-kraven bör utgöra en ”bottenplatta” som kan kompletteras av krav i säkerhetsskyddslagen, jämför avsnitt 5.2.11.

Från Försvarsmakten har också upplysts att det pågår en policydiskussion om att myndigheten frivilligt åtager sig att följa NIS2-direktivets krav så långt som möjligt.

Utredningen menar dock att det framstår som en bättre lösning att helt undanta dessa enstaka myndigheter som bedriver säkerhetskänslig verksamhet och rättsvårdande myndigheter. I förhållande till det totala antalet statliga myndigheter som alltså är 346 utgör dessa knappt tjugo myndigheter en liten andel. Det skulle också kunna framstå som ologiskt om exempelvis Riksbanken inte omfattades men Försvarsmakten gjorde det. På samma sätt skulle det vara skevt om Polismyndigheten och Åklagarmyndigheten inkluderades, men inte domstolarna. Därutöver skulle det stå i strid med regeringens direktiv som har utgångspunkten att säkerhetskänslig verksamhet ska undantas så långt som möjligt och att direktivet möjliggör att all offentlig säkerhetskänslig verksamhet kan undantas. Utredningen menar också att det inte är effektivt att införa skyldigheter som det inte är lämpligt att bedriva tillsyn över och som inte heller skulle vara sanktionerade. En bättre lösning är då att även andra myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning på samma sätt som Försvarsmakten frivilligt åtager sig att följa lagen så långt som möjligt.

Vidare bör alltså enligt utredningens bedömning även Regeringskansliet inklusive kommittéväsendet undantas i sin helhet. Dessa kan inte anses bedriva säkerhetskänslig verksamhet eller brottsbekämpning till övervägande del, men bör likväl undantas på grund av sin särställning. Det framstår exempelvis komplicerat att en myndighet ska bedriva tillsyn över Regeringskansliet, med hänsyn till att myndigheter är underställda regeringen.

Därutöver bör det alltså gälla en särregel för övriga offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpning, men där den säkerhetskänsliga verksamheten eller brottsbekämpningen inte är en övervägande del. Detta bör avse alla andra myndigheter än de som pekas ut i förordningen enligt ovan samt regioner och kommuner. För dessa verksamheter bör den säkerhetskänsliga delen av verksamheten och verksamhet som avser brottsbekämpning undantas från kravet på incidentrapportering, riskhanteringsåtgärder och kravet om att utse företrädare samt tillsyn och sanktioner som hänför sig till dessa krav. Innebörden blir att den säkerhetskänsliga delen av verksamheten och den del som avser brottsbekämpning endast kommer att omfattas av informationskrav enligt artikel 3 och 27 samt tillsyn och sanktioner som kan avse den delen. När det gäller säkerhetskänslig verksamhet kommer det därutöver att finnas ett undantag från skyldigheter att lämna uppgifter som är säkerhetsskyddsklassificerade enligt förslaget ovan i avsnitt 5.5.3. Eftersom det inte föreslås någon begränsning av förslaget i den delen gäller även det om en tillsynsmyndighet efterlyser uppgifter.

För dessa myndigheters, regioners och kommuners övriga verksamhet som inte är säkerhetskänslig eller avser brottsbekämpning bör NIS2-direktivets krav gälla fullt ut.

Som framgått inledningsvis i detta avsnitt ska undantaget inte gälla för en verksamhetsutövare som agerar som en tillhandahållare av betrodda tjänster. I definitionen ligger att sådana elektroniska tjänster vanligen tillhandahålls mot ekonomisk ersättning. Utredningens bedömning är att ingen myndighet som undantas i dess helhet är tillhandahållare av betrodda tjänster, varför detta saknar relevans för svensk rätt. Det betyder att det saknas skäl till särskild lagreglering för tillhandahållare av betrodda tjänster.

Som framgått följer av skäl 8 att offentliga verksamheter som inrättats gemensamt med ett tredjeland i enlighet med ett internationellt avtal samt medlemsländernas diplomatiska och konsulära beskickningar i tredje länder eller nätverks- och informationssystem som drivs för användare i ett tredje land inte omfattas av direktivet. Sammantaget avses utlandsmyndigheterna, det vill säga ambassader, karriärkonsulat, representationer och delegationer vid internationella organisationer som EU, FN och OECD är det egna myndigheter

som lyder under regeringen.[50]Av lagen bör framgå att även dessa undantas från direktivet.

5.5.5 Undantag för enskilda verksamhetsutövare

Utredningens förslag: Lagen gäller inte för enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet eller brottsbekämpning. Detsamma ska gälla för enskilda verksamhetsutövare som enbart erbjuder tjänster till myndigheter som är helt undantagna från lagen.

För enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpning tillsammans med annan verksamhet gäller för den säkerhetskänsliga delen av verksamheten och verksamheten som avser brottsbekämpning enbart kravet om anmälan och uppgiftsskyldighet till tillsynsmyndigheten i 2 kap. 2 § cybersäkerhetslagen. Detsamma ska gälla för de tjänster som erbjuds till myndigheter som är helt undantagna från lagen.

Vad som anförs ovan i andra stycket gäller inte om verksamhetsutövaren är en tillhandahållare av betrodda tjänster.

För den del av verksamheten som inte är säkerhetskänslig, avser brottsbekämpning eller tjänster till myndigheter som är helt undantagna gäller cybersäkerhetslagen i dess helhet.

Ovan har utredningen redovisat hur undantaget bör tillämpas för offentliga verksamhetsutövare. I detta avsnitt ska analyseras vad som ska gälla för särskilda verksamhetsutövare enligt artikel 2.8. En första fråga är vad som avses med särskilda verksamhetsutövare. Utredningen tolkar det med hänsyn till placeringen av artikeln efter 2.7 till andra verksamhetsutövare än offentliga som bedriver sådan verksamhet som följer av artikel 2.8. Det betyder som utgångspunkt alla verksamhetsutövare som omfattas av direktivet utom statliga myndigheter, regioner eller kommuner. Utredningen använder begreppet enskilda verksamhetsutövare.

Som analyserats i avsnitt 5.2.12 och 5.2.13 omfattas som utgångspunkt andra fysiska eller juridiska personer än offentliga som bedriver verksamhet inom EES, innefattas i bilaga 1 eller 2 till direktivet

[50] https://www.regeringen.se/regeringskansliet/organisation/, inhämtat 2023-06-12.

samt uppfyller storlekskravet, vilket i korthet betyder att verksamheten sysselsätter minst 50 personer eller har en omsättning eller balansomslutning som överstiger 10 miljoner euro per år av direktivet.

Därtill kommer att vissa särskilda verksamhetsutövare omfattas även om de inte uppfyller storlekskravet. Det handlar till exempel om verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller utövare med särskilt kritiska verksamheter.

Artikel 2.8 anger alltså vad som gäller för enskilda verksamhetsutövare. Medlemsstaterna *får* undanta sådana verksamhetsutövare som bedriver verksamhet inom områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inte från direktivet, utan från skyldigheterna i artikel 21 och i artikel 23, som reglerar riskhanteringsåtgärder respektive incidentrapportering. Undantaget får bara avse den del av verksamheten som avser nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning. Det ska alltså noteras att detta undantag ger medlemsstaterna en möjlighet att undanta enskilda, (företag eller enskilda fysiska personer) verksamhetsutövares verksamhet till den del den är säkerhetskänslig eller om verksamheten avser brottsbekämpning. Här föreligger alltså som tidigare också konstaterats en skillnad mot undantaget avseende offentliga verksamhetsutövare, eftersom det undantaget är obligatoriskt utformat, medan detta är en möjlighet. Även enskilda verksamhetsutövare omfattas av säkerhetsskyddslagen om de bedriver säkerhetskänslig verksamhet.

Om medlemsstaten undantar sådan verksamhetsutövare från kravet på riskhanteringsåtgärder och incidentrapportering ska inte heller hela tillsyns- och efterlevnadskontrollkapitlet 7 i direktivet tillämpas på den specifika verksamheten eller dessa specifika tjänster.

Detsamma skulle gälla för de enskilda verksamhetsutövare som uteslutande erbjuder tjänster till offentliga verksamhetsutövare som undantagits från direktivet enligt artikel 2.7. I det fallet får alltså den delen av verksamheten undantas från riskhanteringsåtgärder och incidentrapportering samt tillsyn och sanktioner i den delen. Utgångspunkten är att utredningen som framgått i tidigare avsnitt endast föreslår att ett begränsat antal myndigheter ska undantas från lagen i dess helhet och då de myndigheter som bedriver säkerhetskänslig verksamhet eller brottsbekämpning till övervägande del. Utredningen föreslår med hänsyn härtill att enbart de som erbjuder tjänster till dessa myndigheter också undantas från krav om riskhanteringsåtgär-

der, incidentrapportering samt tillsyn- och sanktionsbestämmelser som hänför sig till dessa krav. Innebörden blir för de som erbjuder tjänster att de undantas från krav i den delen de erbjuder tjänster exempelvis till Försvarsmakten eller Polismyndigheten och därutöver i den delen som de själva bedriver säkerhetskänslig verksamhet eller verksamhet som avser brottsbekämpning. Däremot undantas de inte om de erbjuder tjänster till en myndighet, region eller kommun som bedriver säkerhetskänslig verksamhet eller brottsbekämpning i mindre utsträckning och inte heller själv bedriver säkerhetskänslig verksamhet eller brottsbekämpning.

Slutligen finns det en särregel. I sista meningen i artikel 2.8 anges att om verksamhetsutövaren enbart bedriver verksamhet eller erbjuder tjänster uteslutande av den typ som avses i den här punkten får medlemsstaterna besluta att befria dessa verksamhetsutövare också från skyldigheterna i artiklarna 3 och 27.

I artikel 3 finns en informationsskyldighet för samtliga verksamhetsutövare som omfattas av direktivet. Skyldigheten innebär krav att verksamhetsutövaren ska lämna information om verksamhetsutövarens namn, kontaktuppgifter samt i tillämpliga fall uppgift om den relevanta sektorn. Vidare ska i tillämpliga fall en förteckning lämnas över de medlemsstater som tjänster erbjuds som omfattas av direktivet.

Artikel 27 innehåller också informationskrav för verksamhetsutövare, men då för särskilda utövare som bedriver gränsöverskridande verksamhet som till exempel verksamhetsutövare som erbjuder DNS-tjänster. För dessa gäller som anförts under 5.3.2 att endast det medlemsland där verksamhetsutövaren har sitt huvudsakliga etableringsställe får utöva jurisdiktion. Artikeln innehåller därför även krav om kontaktuppgifter dit och till möjlig företrädare.

Innebörden av sista meningen i artikel 2.8 blir då att en enskild verksamhetsutövare som omfattas av direktivet och som enbart bedriver verksamhet som är säkerhetskänslig eller avser brottsbekämpning helt får undantas från lagen. Detsamma skulle gälla de som enbart erbjuder tjänster till myndigheter som är helt undantagna från lagen och inte samtidigt bedriver annan verksamhet. Skälet är att lagen saknar andra krav för verksamhetsutövare än riskhanteringsåtgärder, incidentrapportering och information.

Utredningen föreslår sammanfattningsvis att enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet, brottsbekämpning eller erbjuder tjänster till myndigheter som undantas helt från lagen inte ska omfattas. Förslaget i denna del speglar enligt vår bedömning väl förslaget för den offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet och brottsbekämpning till övervägande del och därför också är helt undantagna från cybersäkerhetlagen. En skillnad är dock att det inte kommer att framgå vilka dessa verksamhetsutövare är, eftersom de inte som myndigheterna kommer att vara utpekade. Den som inte omfattas av en lag har inga skyldigheter att exempelvis anmäla sig. Enligt utredningens uppfattning är detta ändamålsmässigt för dessa verksamhetsutövare. Det bör enligt utredningens uppfattning handla om ett fåtal, i huvudsak extern arbetskraft för myndigheter som exempelvis Försvarsmakten.

För övriga verksamhetsutövare gäller för den säkerhetskänsliga delen av verksamheten och verksamheten som avser brottsbekämpningen inte kraven om riskhanteringsåtgärder och incidentrapportering och inte heller bestämmelserna om tillsyn och sanktioner som avser riskhanteringsåtgärder eller incidentrapportering. Detsamma skulle gälla för den delen av verksamhet som erbjuder tjänster till myndigheter som exempelvis Försvarsmakten. Innebörden blir att för den delen av verksamheten gäller enbart krav om anmälan och uppgiftsskyldighet i artikel 3 och 27 och möjliga tillsyns- och sanktionsbestämmelser som avser denna information.

Utredningen menar att även detta förslag rimmar väl med förslaget för offentliga verksamhetsutövare. Det betyder att företag inte kommer att belastas av krav i olika regelverk, eftersom den delen av verksamheten som omfattas av säkerhetsskyddslagen i huvudsak inte även omfattas av krav enligt cybersäkerhetslagen. Undantag skulle enbart för en del avse informationskravet i cybersäkerhetslagen. Som framgått kommer vissa inte heller att omfattas av dem. Slutligen rimmar förslaget även med regeringens uppfattning i direktiven om att inriktning på förslagen ska vara att säkerhetskänslig verksamhet ska undantas från cybersäkerhetslagen i den utsträckning som är möjlig.

För den del av verksamheten som inte är säkerhetskänslig, avser brottsbekämpning eller tillhandahållandet av tjänster till myndigheter som är helt undantagna gäller cybersäkerhetslagen i dess helhet.

6 Klassificering och registrering

Utredningen har i kapitel 5 analyserat vilka verksamhetsutövare som ska omfattas av förslaget till cybersäkerhetslag. Som framgått handlar det såväl om offentliga som enskilda verksamhetsutövare. Av artikel 3 följer att samtliga verksamhetsutövare som omfattas ska klassificeras som väsentliga eller viktiga och att behöriga myndigheter ska upprätta ett register. Det kräver att verksamhetsutövarna lämnar uppgifter som ska ligga till grund för registret. Av artikel 3 följer också att behöriga myndigheter ska vidarebefordra uppgifterna om verksamhetsutövarna till kommissionen och samarbetsgruppen.[1] Vidare följer av artikel 27 att Enisa ska föra ett register över gränsöverskridande verksamhetsutövare, vilket förutsätter att de lämnar uppgifter till behörig myndighet och att den i sin tur vidarebefordrar uppgiften till Enisa. Gränsöverskridande verksamhetsutövare är definierade i 1 kap. 6 § cybersäkerhetslagen. Slutligen analyseras även skyldigheten att registrera domännamn.

6.1 Väsentlig eller viktig

Utredningens förslag: Följande verksamhetsutövare är väsentliga:

1. Statliga myndigheter,
2. verksamhetsutövare som bedriver verksamhet enligt bilaga 1 till NIS2-direktivet, är en kommun eller ett lärosäte med examenstillstånd och vars verksamhet överstiger trösklarna för medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,[2]

[1] Samarbetsgruppen beskrivs i kapitel 10.
[2] Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.

3. verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och vars verksamhet är medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,[3]
4. kvalificerade tillhandahållare av betrodda tjänster,
5. registreringsenheter för toppdomäner,
6. verksamhetsutövare som erbjuder DNS-tjänster, och
7. verksamhetsutövare som anges i 1 kap. 8 § och identifierats som väsentliga enligt 33 § förordning om cybersäkerhet.

Verksamhetsutövare som inte är väsentliga är viktiga verksamhetsutövare.

Förutsättningarna för om en verksamhetsutövare är väsentlig eller viktig följer av artikel 3.1 och 3.2. I artikel 3.1 a–g listas olika kriterier. En verksamhetsutövare som omfattas av lagen och uppfyller någon av punkterna är en väsentlig verksamhetsutövare. Samtliga verksamhetsutövare som inte uppfyller någon av punkterna är viktiga verksamhetsutövare enligt artikel 3.2.

Offentliga verksamhetsutövare som avses i NIS2-direktivets artikel 2.2 f i ska enligt artikel 3 d vara väsentliga. De som omfattas av den artikeln är de statliga myndigheter som omfattas av NIS2-direktivet. Innebörden blir att samtliga statliga myndigheter som inte är undantagna från utredningens förslag till cybersäkerhetslag är väsentliga. Det betyder samtliga myndigheter utom de som är undantagna enligt författningsförslagets 1 kap. 3 § 1[4] eller 1 kap. 11 §.[5]

Punkten a innehåller två olika kriterier. Ett första är att verksamheten ska bedrivas i en sektor som är listad i bilaga 1 till direktivet. De sektorer som avses är energi, transporter, bankverksamhet, finansmarknads-infrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, förvaltning av IKT-tjänster mellan

[3] Se fotnot 2.
[4] De myndigheter som är undantagna enligt författningsförslaget 1 kap. 3 § 1 är regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och Sveriges domstolar.
[5] I 1 kap. 10 § är statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) eller brottsbekämpning undantagna. Vilka dessa myndigheter är specificeras i förslag till förordningen.

företag, offentlig förvaltning och rymden. Därutöver ska verksamheten överstiga trösklarna för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361 EG.[6] Innebörden är att verksamheten ska sysselsätta minst 250 personer eller ha en årsomsättning på minst 50 miljoner euro eller en balansomslutning på minst 43 miljoner euro per år.

Utredningen menar att det när det gäller kommissionens rekommendation krävs det inte bara en hänvisning till artikel 2 utan även till artikel 3.1–3. Skälet är att det där finns bestämmelser som har betydelse för beräkning av storlekskraven. Här definieras nämligen vad som anges med begreppen partnerföretag och anknutna företag. Även om det i artikeln 3.1 a 1 i NIS2-direktivet inte finns en hänvisning till artikel 3.1–3.3 i rekommendationen framgår det av skäl 16 till direktivet att vid beräkningen ska hänsyn tas till partnerföretag och anknutna företag, även om skäl 16 i sin tur anger ett undantag, se vidare avsnitt 5.2.2. Utredningen finner därför skäl att även hänvisa till artikel 3.1–3.3 i kommissionens rekommendation.

Som analyserats närmare i avsnitt 5.2.8 omfattar kommissionens rekommendation som utgångspunkt även offentliga verksamhetsutövare som statliga myndigheter, kommuner och regioner. Som dock framgår i 5.2.8 finns det i artikel 3.4 ett särskilt undantag för offentlig verksamhet i kommissionens rekommendation, men det undantaget sätts i sin tur ur spel av artikel 2.1 andra stycket NIS2-direktivet. Offentlig förvaltning är en egen sektor enligt bilaga 1 i NIS2-direktivet. Eftersom undantaget i kommissionens rekommendation för offentlig verksamhet inte gäller i det här sammanhanget betyder det att större statliga myndigheter och regioner som sysselsätter minst 250 personer eller har en balansomslutning på minst 43 miljoner euro om året ska kategoriseras som väsentliga verksamhetsutövare. Som dock framgått inledningsvis gäller redan uttryckligen att statliga myndigheter är väsentliga. Denna bestämmelse får därför enbart betydelse för regioner. Vidare kommer även större verksamhetsutövare som inte är offentliga att vara väsentliga om verksamhet bedrivs inom områden som anges i bilaga 1 och storlekskravet är uppfyllt.

[6] Bilagan till kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.

Det ska dock noteras att kommuner inte omfattas av sektorn offentlig i bilaga 1 till NIS2-direktivet. Som utredningen belyst i avsnitt 5.2.11 bedriver dock majoriteten av kommunerna hemsjukvård och omfattas därför av sektorn hälso- och sjukvård som anges i bilaga 1 till direktivet. Det betyder att de kommuner som uppfyller storlekskravet och bedriver hemsjukvård är väsentliga. Enligt utredningens uppfattning är det svårt att föreställa sig att en större kommun som uppfyller detta kvalificerade storlekskrav inte bedriver hemsjukvård, men menar att det inte kan uteslutas. Utredningen har också i avsnitt 5.2.11 i fullständighetens namn att alla kommuner omfattas av lagen, dvs. även de som möjligtvis inte bedriver hemsjukvård. I konsekvens med detta menar utredningen också att samtliga kommuner som uppfyller det kvalificerade storlekskravet bör vara väsentliga. Det behöver därför ske en uttrycklig hänvisning i lagen till att kommuner är väsentliga.

Utredningen föreslår i avsnitt 5.2.14 att lärosäten med examenstillstånd ska omfattas av cybersäkerhetslagen. Ett flertal av dessa är statliga myndigheter och därmed väsentliga. När det gäller icke-statliga lärosäten så framgår inte av NIS2-direktivet om de är väsentliga eller viktiga eftersom det är frivilligt för medlemsstaten att inkludera dem och de därmed inte finns med i bilaga 1 eller 2. Utredningen menar att de icke-statliga lärosäten bör vara väsentliga om de uppfyller storlekskravet trots att de inte finns med i uppräkningen i bilaga 1. Det blir annars en omotiverad skillnad på lärosäten som bedrivs med staten som huvudman respektive de som inte gör det. Det behöver därför anges i lagen att även lärosäten som uppfyller storlekskravet är väsentliga.

Punkten b anger tre olika kategorier av verksamhetsutövare nämligen kvalificerade tillhandahållare av betrodda tjänster, registreringsenheter för toppdomäner samt leverantörer av DNS-tjänster (domännamnssystemtjänster) oavsett storlek. Som även framgår av avsnitt 5.2.13 avses med betrodd tjänst en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av

a) skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller

b) skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller

c) bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster.

En tillhandahållare av en betrodd tjänst erbjuder alltså sådana tjänster. Skillnaden mellan en tillhandahållare av en betrodd tjänst och en kvalificerad tillhandahållare av en betrodd tjänst är att den kvalificerade tillhandahållaren ska ha beviljats status som kvalificerad av tillsynsorganet.[7] Detta följer av artikel 3 punkt 20 i Europaparlamentets och rådets förordning (EU) nr 910/2014.[8] PTS är tillsynsmyndighet. Registreringsenhet för toppdomäner och DNS-tjänster är definierade i utredningens författningsförslag i 1 kap. 2 §.

I punkten c anges att tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som betraktas som medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag ska anses vara väsentliga. Begreppen allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster har samma innebörd som i lagen (2022:482) om elektronisk kommunikation (LEK), se utredningens definitioner i 1 kap. 2 § författningsförslaget. När det gäller storleken betyder definitionen att verksamheten ska sysselsätta minst 50 personer eller ha en omsättning eller balansomslutning som överstiger 10 miljoner euro per år, se avsnitt 5.2.8. Av samma skäl som anges för punkten 1 innefattas även offentliga verksamhetsutövare och det krävs även här en hänvisning till artikel 3.1–3.3 i rekommendationen. Samtidigt får det alltså bara betydelse för kommuner och regioner.

Av artikel 3.1 e och 3.2 andra meningen bör sammantaget följa att medlemsländerna får bestämma om de verksamhetsutövare som avses i artikel 2.2 b–e är väsentliga eller viktiga. Det betyder de verksamhetsutövare som följer av utredningens författningsförslag i 1 kap. 8 § ska identifieras som väsentliga eller viktiga. Vilka dessa verksamhetsutövare är ska anges av MSB enligt utredningens förslag till för-

[7] Därutöver är ett krav att en kvalificerad tillhandahållare tillhandahåller en eller flera kvalificerade betrodda tjänster.
[8] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

ordning om cyberssäkerhet 33 §, se även avsnitt 5.2.13. Utredningen föreslår att MSB även ska bestämma om verksamhetsutövaren är väsentlig. Bemyndigandet i 1 kap. 8 § för regeringen eller den myndighet regeringen bestämmer täcker även detta.

I artikel 3.1 f anges att verksamhetsutövare som identifierats som kritiska enligt CER-direktivet är väsentliga. Det betyder att det bör anges att verksamhetsutövare som identifierats som kritiska enligt den lag som föreslås införliva CER-direktivet är väsentliga. Denna fråga kommer utredningen att behandla senare och redovisa i sitt slutbetänkande. Slutligen anges i artikel 3.1 g att medlemsstater får föreskriva att verksamhetsutövare som före den 16 januari 2023 har identifierats som leverantörer av samhällsviktiga tjänster i enlighet med NIS1-direktivet[9] eller nationell rätt är väsentliga. Det som därmed avses är att det är möjligt att föreskriva att samtliga de leverantörer som tillhandahåller en samhällsviktig tjänst och som fram till den 15 januari 2023 omfattades av NIS-lagen är väsentliga. För att bedöma om det föreligger ett sådant behov krävs det en jämförelse mellan den lagen och utredningens författningsförslag.

Vem som omfattas av NIS-lagen följer av den lagens 3 § 1. Där anges det att leverantörer som anges i bilaga 2 till NIS-direktivet och som tillhandahåller en samhällsviktig tjänst omfattas under förutsättning att leverantören är etablerad i Sverige, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Vid bedömningen om vad som utgör en betydande störning ska enligt 4 § förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster bland annat beaktas antalet användare som är beroende av den samhällsviktiga tjänsten, leverantörens marknadsandel, storleken av det geografiska område som skulle kunna påverkas av en incident och hur beroende andra sektorer är av den samhällsviktiga tjänst som leverantören tillhandahåller. MSB får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela ytterligare föreskrifter om vad som avses med en betydande störning. Detta har myndigheten gjort i (MSBFS 2021:9). I föreskriften har MSB för varje sektor angett olika detaljerade tröskelvärden. Tröskelvärdena har enligt uppgift från MSB tagits fram i nära samverkan med berörd tillsynsmyndighet.

[9] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

Som analyserats tidigare i bakgrunden är skillnaden mellan NIS-direktivets krav och NIS2-direktivets att det senare omfattar fler områden och skärper kraven. Det betyder att samtliga sju sektorer som NIS-lagen omfattar även kommer att innefattas i utredningens författningsförslag. Som vidare framgår av NIS-lagens 3 § är en central förutsättning för att identifieras som leverantör av samhällsviktig tjänst att en incident skulle medföra en betydande störning. I utredningens författningsförslag i 1 kap. 8 § finns också redan en möjlighet att klassificera verksamhetsutövare som väsentliga om en störning i verksamheten kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet, folkhälsa eller medföra betydande systemrisker särskilt om det får gränsöverskridande konsekvenser. Därmed menar utredningen att det är överflödigt att särskilt även ange att verksamhetsutövare som tidigare bedömts vara leverantörer av samhällsviktiga tjänster som väsentliga verksamhetsutövare i utredningens författningsförslag. Redan på grund av detta saknas det anledning att införa en sådan bestämmelse. Därutöver skulle det innebära stora lagtekniska svårigheter att låta tidigare lagstiftning ligga till grund för bedömningar enligt ny lagstiftning, eftersom den tidigare lagen kommer att upphävas med följd att även tidigare gällande föreskrifter behöver omarbetas. Detta kan medföra oklarheter och tillämpningssvårigheter särskilt med hänsyn till att såväl tidigare NIS-lag som den framtida cybersäkerhetslagen bygger på att verksamhetsutövaren har en skyldighet att identifiera sin verksamhet och anmäla sig, se vidare avsnitt 6.2.

6.2 Register över väsentliga och viktiga verksamhetsutövare

Utredningens förslag:

1. Varje tillsynsmyndighet ska inom sitt tillsynsområde upprätta ett register över väsentliga och viktiga verksamhetsutövare. Ett första register ska vara upprättat och ingivet till den gemensamma kontaktpunkten senast den 1 mars 2025 och därefter ska det ske en uppdatering och ny rapportering i vart fall vartannat år.
2. Den gemensamma kontaktpunkten ska senast den 17 april 2025 och därefter vartannat år underrätta kommissionen och sam-

arbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare som förtecknats för varje sektor och delsektor. Vidare ska den gemensamma kontaktpunkten informera om antalet väsentliga och viktiga verksamhetsutövare samt deras verksamhet som identifierats enligt 1 kap. 8 §.

3. Verksamhetsutövare ska i en anmälan till tillsynsmyndigheten lämna uppgift om identitet, kontaktuppgift, IP-adressintervall, verksamhet och uppgift om i vilka länder verksamhet bedrivs till tillsynsmyndigheten. Uppgifter bör vara lämnade den 17 januari 2025 och ändringar ska anmälas inom 14 dagar.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om uppgifterna.

Av artikel 3.3 följer att medlemsstater senast den 17 april 2025 ska upprätta ett register över väsentliga och viktiga verksamhetsutövare samt verksamhetsutövare som erbjuder domännamnsregistreringstjänster. Registret ska enligt artikeln uppdateras regelbundet och minst vartannat år.

Utredningen föreslår i kapitel 8 ett delat tillsynsansvar. Det innebär att varje tillsynsmyndighet behöver upprätta ett sådant register för sitt ansvarsområde.

Dessa register ska sedan rapporteras till den gemensamma kontaktpunkten. Den myndigheten behöver sedan senast den 17 april 2025 och därefter vartannat år i enlighet med artikel 3.5 underrätta kommissionen och samarbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare för varje sektor och delsektor som omfattas av cybersäkerhetslagen. Vidare ska den myndigheten också lämna relevant information till kommissionen om antalet väsentliga och viktiga verksamhetsutövare som identifierats i enlighet med artikel 2.2 b–e. Det betyder information om verksamheter som anges i 1 kap. 8 §, dvs., verksamheter som enligt bedömning från MSB är särskilt kritisk (33 § cybersäkerhetsförordningen).

En fråga är varför artikel 3.3 särskilt även anger att medlemsstater ska upprätta ett register över verksamhetsutövare som erbjuder domännamnsregistreringstjänster. Som framgår finns det i denna del ingen rapporteringsskyldighet till kommissionen eller samarbetsgruppen. Däremot följer det av artikel 27 att Enisa ska upprätta ett register

över gränsöverskridande verksamhetsutövare. Verksamhetsutövare som erbjuder domännamnsregistreringstjänster är en sådan gränsöverskridande verksamhet. Med hänsyn härtill saknas skäl för att särskilt peka ut ett register för domännamnsregistreringstjänster.

Till grund för förteckningen ska varje verksamhetsutövare enligt artikel 3.4 lämna uppgift till sin tillsynsmyndighet om identitet, kontaktuppgifter, IP-adresser (utredningen kommer framöver att använda begreppet IP-adressintervall, se nästa avsnitt) samt uppgift om verksamheten och i vilka länder den utövas. Innebörden är att även cybersäkerhetslagen precis som NIS-lagen bygger på att verksamhetsutövaren själv bär ansvaret för att identifiera att verksamheten omfattas av lagen och har en skyldighet att anmäla sig till myndigheten och lämna uppgifter om verksamheten. Som utredningen anför i avsnitt 5.2.12 bör det dock ankomma på varje tillsynsmyndighet att med stöd av MSB att utforma en vägledning om de oklarheter som kan föreligga i sektorsbeskrivningarna till stöd för den enskilde verksamhetsutövaren.

Det får ankomma på den gemensamma kontaktpunkten, dvs. MSB att närmare föreskriva om hur uppgifterna ska lämnas och uppgifternas närmare innehåll samt när uppgifterna behöver vidarebefordras till den gemensamma kontaktpunkten. Skälet är att det blir den gemensamma kontaktpunkten som nationellt blir slutmottagare av uppgifterna. Det följer av artikel 3.4 att medlemsstaterna får inrätta nationella mekanismer som gör det möjligt för verksamhetsutövarna att registrera sig själva. Av regeringens direktiv följer också att utgångspunkt bör vara att även det framtida regelverket bör utformas utifrån att verksamhetsutövaren är ansvarig för att avgöra om denne omfattas av regelverket och i så fall anmäla sig till tillsynsmyndigheten.[10] Utredningen anser att uppgifterna av samordningsskäl bör inges senast den 17 januari 2025, jämför vidare avsnitt 6.2.1 nedan. Datum bör dock enligt utredningens uppfattning följa av myndighetens föreskrifter. Det ska också beaktas att även tillkommande verksamhetsutövare behöver lämna uppgifter. Vidare framgår att kommissionen med bistånd från Europeiska unionens cybersäkerhetsbyrå, Enisa, ska tillhandahålla riktlinjer och mallar för dessa uppgiftsskyldigheter. Detta har kommissionen gjort i september 2023.[11]

[10] Dir. 2023:30 s. 5.
[11] https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-34-directive-eu-20222555-nis-2-directive.

Därutöver har förstås tillsynsmyndigheterna ett ansvar för att skyldigheten att anmälan och uppgiftsskyldigheten följs och kan vidta åtgärder om det inte sker, se vidare kapitel 9 om ingripanden och sanktioner.

Slutligen följer av artikel 3.6 att medlemsländerna *får* på begäran av kommissionen lämna uppgift om namn på de väsentliga och viktiga verksamhetsutövarna som anges i 1 kap. 8 § och som ska identifieras av MSB enligt 33 § cybersäkerhetsförordningen fram till den 17 april 2025. Här handlar det alltså inte om en skyldighet utan om en möjlighet för myndigheten och det avser tiden innan register är upprättade. Enligt utredningens bedömning behöver detta inte lagregleras.

6.2.1 Särskilt register över gränsöverskridande verksamhetsutövare

Utredningens förslag: Den gemensamma kontaktpunkten ska upprätta ett särskilt register över gränsöverskridande verksamhetsutövare och ge in det skyndsamt till Enisa. Vidare ska den gemensamma kontaktpunkten löpande underrätta Enisa om uppgifter avseende gränsöverskridande verksamhetsutövare. Registret ska vila på uppgifter som lämnats av verksamhetsutövarna till tillsynsmyndigheterna och som myndigheterna lämnat vidare till den gemensamma kontaktpunkten enligt förslag i 6.2 punkt 3 ovan. För gränsöverskridande verksamhetsutövare gäller dock att de utöver tidigare uppgifter även ska lämna uppgift om verksamhetsutövarens huvudsakliga etableringsställe och i förekommande fall kontaktuppgift till företrädaren.

Av artikel 27.1 följer att Enisa ska föra ett register över gränsöverskridande verksamhetsutövare. Enisa ska också ge behöriga myndigheter i medlemsstaterna tillgång till registret. De som omfattas är verksamhetsutövare som erbjuder följande

1. DNS-tjänster,
2. registreringsenheter för toppdomäner,
3. domännamnsregistreringstjänster,

4. molntjänster,
5. datacentraltjänster,
6. nätverk för leverans av innehåll,
7. hanterade tjänster,
8. hanterade säkerhetstjänster, eller
9. marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster.

Samtliga begrepp i uppräkningen ovan är definierade i utredningens förslag till cybersäkerhetslag.

För att Enisa ska kunna upprätta ett register ska verksamhetsutövarna lämna anmälan med uppgifter till sin tillsynsmyndighet. Dessa uppgifter är i hög grad samma som samtliga verksamhetsutövare som omfattas av lagen behöver lämna enligt artikel 3 och som beskrivits ovan. Uppgifterna får också enligt artikel 27.5 lämnas genom att verksamhetsutövarna registrerar dem själva genom de nationella mekanismer som kan ha inrättats enligt artikel 3.4 och som även det har beskrivits ovan.

Skillnaden i uppgiftsskyldigheten är att samtliga verksamhetsutövare enligt artikel 3 ska lämna uppgift om IP-adress, men att de gränsöverskridande verksamhetsutövarna ska lämna uppgift om IP-adressintervall. Det framstår dock som om detta inte är en skillnad i sak, eftersom kommissionen i riktlinjerna från september 2023 för såväl artikel 3.4 som 27.2 använder begreppet IP-adressintervall.[12] Vidare ska enligt artikel 27.2, men inte 3.4 även lämnas uppgift om verksamhetsutövarens huvudsakliga etableringsställe och i förekommande fall adress till företrädare. Skillnaden beror förstås på att det för dessa gränsöverskridande verksamhetsutövare gäller ett förhöjt krav för att de ska omfattas av svensk lag. De omfattas endast om det huvudsakliga etableringsstället ligger i Sverige och i vissa fall behöver en företrädare utses (jämför artikel 26.1 b och avsnitt 5.3.2). Innebörden är att det kommer att finnas gränsöverskridande verksamhetsutövare som är verksamma i Sverige, men vars huvudsakliga etableringsställe finns i en annan medlemsstat. Dessa omfattas så-

[12] https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-34-directive-eu-20222555-nis-2-directive, jämför s. 1 och 2.

ledes inte av cybersäkerhetslagen. Samordningen kommer att underlättas av att behöriga myndigheter har tillgång till Enisas register.

Därutöver är kravet för ändringar för gränsöverskridande verksamhetsutövare att de ska inges inom 90 dagar och inte 14 som gäller för samtliga verksamhetsutövare. Slutligen är också en skillnad mellan uppgifterna enligt artikel 3 och artikel 27 att uppgifterna enligt artikel 27, dvs. uppgifter från de gränsöverskridande verksamhetsutövarna ska lämnas till tillsynsmyndigheten senast den 17 januari 2025, medan det av artikel 3.3 endast följer att medlemsstaternas förteckning ska vara upprättad senast 17 april 2025.

Utredningen föreslår att de olika uppgiftsskyldigheterna samordnas av effektivitetsskäl. Det ligger i linje med kommissionens uppfattning, som i sina riktlinjer från september 2023 anvisar samma mall för uppgifter enligt såväl artikel 3.3 som 27.2. Kommissionen anger administrativ effektivitet som skäl för det.[13]

Det betyder att samtliga verksamhetsutövare ska lämna sina uppgifter vid den tidigaste tidpunkten, dvs. den 17 januari 2025, att ändringar ska inges inom 14 dagar och att tillsynsmyndigheterna sammanställer dem i register och vidarebefordrar dem till den gemensamma kontaktpunkten senast den 1 mars 2025 och att den i sin tur rapporterar inte bara till kommissionen och samarbetsgruppen utan även till Enisa. Därutöver behöver särskilt anges att gränsöverskridande verksamhetsutövare även behöver ange huvudsakligt etableringsställe och i förekommande fall kontaktuppgift till företrädare.

6.3 Domännamnsregistreringsuppgifter

Utredningens förslag: Lagen (2006:24) om nationella toppdomäner för Sverige på internet ändras på följande sätt för att anpassas till NIS2-direktivets krav:

1. Rubriken till lagen ska vara lag om toppdomäner på internet.
2. Lagen ska omfatta toppdomäner med huvudsakligt etableringsställe i Sverige på internet, inte nationella toppdomäner för Sverige på internet,

[13] Se länk ovan s. 2.

3. Registerskyldigheten för bland annat domännamn ska även innehålla registreringsdatum, alltså när domännamnet registrerades.
4. Det ska uttryckligen av toppdomänlagen följa att det är möjligt för myndigheter och andra med offentligrättsliga uppgifter inom EES att begära ut uppgifter på annat sätt av registreringsenheten för toppdomäner än genom internet. Uppgifterna ska lämnas skyndsamt. De närmare bestämmelserna om denna uppgiftsskyldighet bör följa av föreskrifter. Det finns redan ett bemyndigande för PTS i regleringen.

Av artikel 28.1 och 28.2 följer att medlemsstaterna ska ålägga registreringsenheter för toppdomäner och verksamhetsutövare som erbjuder domännamnsregistreringstjänster att samla in och upprätta registreringsuppgifter över domännamn. Registret ska utöver domännamnet även innehålla identitet och kontaktuppgift för innehavaren av domännamnet eller kontaktuppgifter till en kontaktpunkt. Det ska enligt artikel 28.3 finnas en strategi och förfaranden inbegripet kontrollförfaranden för att uppgifterna i registret är korrekta som offentliggörs. Från PTS har anförts att en fråga är hur medlemsstaterna ska se till att uppgifterna är korrekta. Det kan exempelvis krävas identifiering genom bank-id eller liknande. Frågan diskuteras inom EU:s arbetsgrupper. Enligt utredningens uppfattning behöver detta lösas genom föreskrifter.

Vidare ska verksamhetsutövarna för domännamnsregistreringstjänster och registreringsenheter för toppdomäner enligt artikel 28.4 utan dröjsmål efter registreringen offentliggöra uppgifterna, med undantag för personuppgifter och även enligt artikel 28.5 på begäran ge legitima åtkomstsökanden tillgång till uppgifterna. Det betyder att legitima åtkomstsökanden behöver definieras. Enligt utredningens uppfattning avses i första hand myndigheter inom EES, se vidare nedan. Svar på en sådan begäran ska lämnas skyndsamt och i vart fall inom 72 timmar. Medlemsstaterna ska se till att det även finns en strategi för utlämnandet av uppgifterna och att strategin offentliggörs. Slutligen föreskriver artikel 28.6 att bestämmelserna i artikeln inte får leda till en dubbel insamling av registreringsuppgifter för domännamn, varför registreringsenheter för toppdomäner och verk-

samhetsutövare som tillhandahåller domännamnsregistreringstjänster ska samarbeta med varandra.

I Sverige gäller lagen (2006:24) om nationella toppdomäner för Sverige på internet (toppdomänlagen). Den reglerar teknisk drift av nationella toppdomäner för Sverige på internet samt tilldelning och *registrering av domännamn* under dessa toppdomäner (1 §). I lagens 6 § anges att domänadministratören, dvs. den som ansvarar för administration av en nationell toppdomän för Sverige ska föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna. Registret ska innehålla

1. domännamnet,
2. namnet på domännamnsinnehavaren och dennes postadress, telefonnummer och adress för elektronisk post,
3. namnet på den som tekniskt administrerar domännamnet och dennes postadress, telefonnummer och adress för elektronisk post,
4. uppgifter om de namnservrar som är knutna till domännamnet, samt
5. övrig teknisk information som behövs för att administrera domännamnet.

Vidare ska uppgifterna i registret kunna hämtas utan avgift via internet. Personuppgifter får endast göras tillgängliga på detta sätt om den registrerade har samtyckt till det. Domänadministratören är personuppgiftsansvarig för behandling av personuppgifter i registret.

Bestämmelsen är enligt propositionen till toppdomänlagen betydelsefull av flera anledningar. Tjänsten gör det möjligt att komma i kontakt med ansvariga för datorer som sprider datavirus. Det har även betydelse ur ett konsument- och näringslivsperspektiv när det används för att kontrollera vem som innehar ett domännamn vid elektronisk handel eller när ett immaterialrättsligt intrång begåtts. Slutligen kan registret användas av rättsvårdande myndigheter för att identifiera ansvariga för domännamn till vilka webbplatser med olagligt innehåll finns kopplade. Traditionen i internetsammanhang skulle också vara att s.k. ”whois”-data finns offentligt tillgängliga på internet i en sökbar databas.[14]

[14] Prop. 2004/05:175 s. 248.

Enligt 9 § samma lag gäller enligt punkt 2 att regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om register och säkerhetskopior enligt 6 §. Av förordningen (2006:25) om nationella toppdomäner för Sverige på internet följer av 3 § att PTS får meddela föreskrifter om register och säkerhetskopior enligt 6 § lagen om nationella toppdomäner för Sverige på internet. Myndigheten har inte meddelat sådana föreskrifter.

Enligt uppgift innebär i praktiken denna bestämmelse att om en person begär ut uppgifter erhåller de endast begränsade uppgifter, i huvudsak uppgift om domännamnet, eftersom övriga uppgifter är ”maskade”. Det beror på den särskilda bestämmelsen i 6 § om att personuppgifter endast får göras tillgängliga på internet om den registrerade har samtyckt till det. Denna reglering har varit oförändrad sedan lagens tillkomst 2006. Vid den tidpunkten gällde personuppgiftslagen (1998:204). Den lagen upphävdes 2018 i samband med att EU:s dataskyddsförordningens bestämmelser[15] och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning började gälla. Vid den tidpunkten gjordes även en ändring av 3 § toppdomänlagen med innebörd att det anges att bestämmelserna i 6 § är kompletteringar till dataskyddsbestämmelserna och att bestämmelserna i toppdomänlagen har företräde framför dem. Sammantaget gäller alltså att det krävs samtycke för att personuppgifterna enligt toppdomänlagen ska kunna publiceras.

Utredningen drar av den anförda slutsatsen att kraven i artikel 28 delvis redan är uppfyllda genom toppdomänlagen. Som framgår ovan ska registret enligt den lagen innehålla domännamn, innehavarens identitet och kontaktuppgifter. I artikel 28 krävs som alternativ till innehavarens kontaktuppgifter motsvarande till kontaktpunkten. Enligt 6 § finns som alternativ namn och kontaktuppgifter till den som tekniskt administrerar domännamnet, vilket får anses vara jämförbart. Att skyldigheten är lagreglerad betyder också att det finns en strategi från Sverige som är offentlig, vilket uppfyller kravet i artikel 28.3. För såväl skyldigheten i toppdomänlagen som artikel 28 gäller också begränsningar genom dataskyddsregleringen.

[15] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Det finns dock några skillnader. En viktig skillnad är att toppdomänlagen endast omfattar nationella toppdomäner för Sverige. Det betyder i praktiken Internetstiftelsens drift av den svenska toppdomänen .se. Samtidigt sköter Internetstiftelsen även i dag drift och administration av toppdomänen .nu, som inte omfattas av lagen. Av propositionen till toppdomänlagen framgår att syftet med lagen var att på ett effektivt sätt kontrollera administrationen av toppdomäner som särskilt avser Sverige, även om Konkurrensverket föreslagit att regleringen av konkurrensneutrala skäl borde avse all administration av toppdomäner som utövas från ett fast driftställe i Sverige.[16]

NIS2-direktivet har dock enligt utredningens uppfattning en bredare ansats, eftersom artikel 28 pekar ut registreringsenheter för toppdomäner. Utredningen har i författningsförslaget definierat begreppet som en verksamhet som ansvarar för att administrera, förvalta, sköta teknisk drift samt registrering av domännamn under en specifik toppdomän, dock inte om toppdomänen endast avses för eget bruk. Det är i sin tur en förenklad version av den definition som direktivet anger i artikel 6.21.

Från PTS har dock invänts att i artikel 6.21 i NIS2-direktivet definieras registreringsenhet som en enhet som har delegerats en specifik toppdomän **och** som ansvarar för administrationen av toppdomänen. Båda kraven är uppfyllda för Internetstiftelsen när det gäller .se-domänen men inte för .nu-domänen där Internetstiftelsen endast sköter administrationen. Delegering ligger hos IUSN Foundation. Samtidigt menar PTS att kraven i artikel 28.1 om att samla in registreringsuppgifter även avser .nu. Myndigheten menar att implementeringen av artikel 28 för .nu bör ske i den nya cybersäkerhetslagen och att endast toppdomäner som uppfyller såväl kravet på delegering som administration bör regleras i toppdomänlagen. I framtiden skulle man enligt PTS kunna tänka sig även andra toppdomäner som till exempel .sverige. Dessa skulle då också omfattas av toppdomänlagen. Sammantaget menar alltså PTS att Internetstiftelsens verksamhet avseende .nu inte omfattas av definitionen i artikel 6.21, men att om IUSN Foundation skulle etablera ett huvudsakligt etableringsställe i Sverige skulle den likväl omfattas av kraven för registreringsenheter i artikel 28.

[16] Prop. 2004/05:175 s. 242.

Utredningen delar inte denna uppfattning. I artikel 6.21 definieras begreppet registreringsenhet och kraven för registreringsenhet följer av artikel 28. Om .nu inte omfattas av definitionen i 6.21 omfattas den inte heller av kraven i artikel 28. Enligt utredningens bedömning vore det dock olyckligt, eftersom det är angeläget med en registrering för att bidra till domännamnssystemens säkerhet. När det gäller definitionen är det inte heller klart vad som avses. Den engelska lydelsen är "top-level domain name registry' or TLD name registry means an entity which has been delegated a specific TLD and is responsible for administering the TLD." Sammantaget bedömer utredningen att en alltför strikt tolkning av definition av registreringsenhet får oönskade konsekvenser. I vart fall har utredningen också möjlighet att föreslå mer långtgående bestämmelser, eftersom NIS2 är ett minimidirektiv. Utredningen föreslår därför den mer ändamålsenliga definitionen av registreringsenheter i cybersäkerhetslagen dvs. en verksamhet som ansvarar för att administrera, förvalta, sköta teknisk drift samt registrering av domännamn under en specifik toppdomän, dock inte om toppdomänen endast avses för eget bruk. Det betyder i sin tur att även .nu omfattas av kraven i artikel 28. Slutligen bedömer utredningen också att det är rimligt med en sammanhållen lagstiftning, varför införlivningen av artikel 28 i dess helhet bör ske i toppdomänlagen.

Vidare omfattas gränsöverskridande verksamhetsutövare som exempelvis registreringsenheter för toppdomäner om Sverige är det huvudsakliga etableringsstället (se utredningens författningsförslag 1 kap. 6 §). En annan mindre skillnad är att NIS2-direktivet ställer krav om registreringsdatum, vilket inte finns i toppdomänlagens paragraf sex.

En fråga är vidare i vilken utsträckning det föreligger en skillnad mellan att uppgifterna enligt toppdomänlagen erbjuds på internet, men att det av artikel 28.5 följer att det finnas en skyldighet att lämna ut specifika uppgifter till "lagliga och motiverade begäran från legitima sökanden" och att svar ska ges inom 72 timmar. Skillnaden blir enligt utredningens uppfattning att det finns ett förstärkt skydd för personuppgifter genom att publiceringen sker på internet. Utredningen föreslår därför att det uttryckligen av toppdomänlagen även bör framgå att myndigheter inom EES ska kunna begära uppgifter genom direkt kontakt med registreringsenheten för toppdomäner. Hänsyn ska i den delen enbart tas till dataskyddsregleringen.

Utredningen föreslår utifrån det anförda att 1 § i toppdomänlagen ändras så att den omfattar teknisk drift av toppdomäner på internet med huvudsakligt etableringsställe i Sverige samt tilldelning och registrering av domännamn under dessa toppdomäner och att kravet om registreringsdatum läggs till i toppdomänlagens 6 §. Vidare föreslår utredningen också att det uttryckligen av 6 § bör följa att myndigheter kan begära ut uppgifter på andra sätt av registreringsenheten och att uppgifterna ska lämnas skyndsamt. Från PTS har anförts att även andra kan innefattas i begreppet legitima åtkomstsökanden, exempelvis i ärenden gällande cybersäkerhetsrelaterad brottslighet. Utredningen föreslår att myndigheter och andra med offentligrättsliga uppgifter inom EES ska kunna begära ut utgifter på detta sätt. Däremot bör rättigheten inte utsträckas till privatpersoner, eftersom det inte, som för myndigheter och offentligrättsliga subjekt, kan presumeras att privatpersoner har legitima skäl. Den närmare definitionen av personer med offentligrättsliga uppgifter bör följa av föreskrifter. Det finns redan en möjligen för PTS att meddela föreskrifter, vilket alltså inte använts. Utredningen menar att det av föreskrifter även bör följa närmare hur och inom vilka tidsgränser uppgiftsskyldigheten ska fullgöras.

Slutligen är också en skillnad att skyldigheten enligt artikel 28 i NIS2-direktivet gäller för såväl registreringsenheter för toppdomäner som de verksamhetsutövare som erbjuder domännamnsregistreringstjänster. Enligt den svenska lagen åvilar ansvaret endast registreringsenheter för toppdomäner och inte dem som erbjuder domännamnsregistreringstjänster. Samtidigt anges i artikel 28.6 att bestämmelserna inte får leda till dubblerad insamling av registreringsuppgifter. Med hänsyn till det bedömer utredningen att det är tillräckligt att det finns nationella bestämmer som ser till att registeruppgifter finns tillgängligt som registreringsenheter för toppdomäner bär ansvaret för.

7 Riskhantering och incidentrapportering

I detta kapitel analyseras riskhanteringsåtgärder enligt artikel 20, 21 och 25 i avsnitt 7.1 och 7.2. Incidentrapportering enligt artikel 23 och 30 behandlas i avsnitt 7.3 och certifiering enligt artikel 24 i 7.4.

7.1 Övergripande lagreglering om riskhanteringsåtgärder

Utredningens bedömning:

1. Kraven om riskhanteringsåtgärder ska regleras övergripande i cybersäkerhetslagen.
2. Lagen bör fyllas ut av föreskrifter som meddelas av tillsynsmyndigheten. Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig över föreskrifterna. Detta ska följa av cybersäkerhetsförordningen.
3. Regeringen bör ge Myndigheten för samhällsskydd och beredskap i uppdrag att skyndsamt utarbeta en vägledning om riskhanteringsåtgärder till stöd för tillsynsmyndighetens föreskriftsarbete.

I artikel 21 anges kraven för riskhanteringsåtgärder för cybersäkerhet. Som följer av artikeln är det dels övergripande bestämmelser, dels en uppräkning av olika krav i punkter.

I kapitel 8 föreslår utredningen ett delat tillsynsansvar med innebörd att det kommer att finnas olika tillsynsmyndigheter för de olika sektorerna. De olika tillsynsmyndigheterna kommer att behöva bedriva tillsyn över att ovanstående krav uppfylls. Om så inte sker ska

tillsynsmyndigheten meddela sanktioner, se kap. 9. Vidare får det ankomma på varje[1] tillsynsmyndighet att meddela närmare föreskrifter om riskhanteringsåtgärder, se vidare kapitel 8.

Kommissionen ska också enligt artikel 21.5 senast den 17 oktober 2024 anta genomförandeakter för de åtgärder som krävs för vissa verksamhetsutövare, i huvudsak gränsöverskridande verksamhetsutövare, vilket behöver beaktas i genomförandearbetet, se vidare om detta kapitel 8.

Från särskilt MSB har anförts att det förhållande att olika myndigheter får meddela föreskrifter innebär en risk för att kraven tillämpas olika. Enligt utredningens uppfattning är det dock som också framgår av kapitel 8 angeläget att föreskrifterna kan sektorsanpassas och att den myndighet som har tillsyn också har föreskriftsrätten.

Från MSB, Säkerhetspolisen, Transportstyrelsen och IMY har då föreslagits att det borde ankomma på MSB att meddela föreskrifter med grundläggande krav på säkerhet och att de olika tillsynsmyndigheterna, vid behov, kompletterar dessa föreskrifter genom att meddela föreskrifter med särskilda krav på utökad säkerhet för sin sektor. Som anges i kapitel 8 menar utredningen att det skulle kunna leda till motstridiga krav i de olika föreskrifterna, vilket inte skulle uppfylla kraven på förutsebarhet och klarhet vid normgivning. Utredningen har därför bedömt att en sådan lösning inte är en framkomlig väg.

Samtidigt finns det skäl att närmare klarlägga de olika kraven i artikel 21, särskilt med hänsyn att utformningen av artikel 21 delvis är oklar. Här handlar det bland annat om tekniska detaljer, som det saknas förutsättningar för utredningen att klargöra.

Utredningen föreslår med hänsyn till att flera tillsynsmyndigheter kommer att meddela föreskrifter för olika områden att de grundläggande kraven av rättssäkerhetsskäl följer av förslaget till cybersäkerhetslagen. Samtidigt bör dock kraven inte anges alltför detaljerat, eftersom det kommer att ankomma på tillsynsmyndigheterna att meddela föreskrifter som anpassar kraven till respektive sektor. Som framgår av artikel 21.1 ska åtgärderna vara proportionella i förhållande till risken. Vidare föreslår utredningen att regeringen ger MSB i uppdrag att skyndsamt utarbeta en vägledning om riskhanteringsåtgärder till stöd för tillsynsmyndigheternas föreskriftsarbete. Även om denna vägledning – som MSB påpekat – inte kommer att vara juri-

[1] Undantag kommer dock att gälla för sektorn offentlig förvaltning. För denna sektor kommer länsstyrelser att bedriva tillsyn, men MSB ha föreskriftsrätt avseende riskhanteringsåtgärder.

diskt bindande bör den likväl utgöra en viktig grund för likvärdiga föreskrifter.

7.1.1 Övergripande om begrepp

Utredningens bedömning: Det är inte möjligt att anpassa begreppen i cybersäkerhetslagen till begreppen i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Som framgått skiljer sig kraven i NIS2-direktivet i hög grad från kraven i NIS-direktivet. Utredningen har därför som följer av avsnitt 5.1 föreslagit att den tidigare regleringen som införlivade NIS-direktivet upphävs och ersätts av ett nytt regelverk som införlivar NIS2-direktivet. Eftersom kraven i direktiven i hög grad skiljer sig åt innebär det i sin tur att de båda direktiven också använder olika begrepp. Ett exempel är att artikel 21 använder begreppet riskhanteringsåtgärder. Från MSB har anförts att säkerhetsåtgärder är det etablerade begreppet. Myndigheten menar att det är angeläget att cybersäkerhetsregelverket så långt som möjligt ansluter sig till tidigare begrepp, eftersom verksamhetsutövarna redan är förtrogna med dem och myndighetens föreskrifter använder dem. Utredningen noterar att begreppet säkerhetsåtgärder används i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, se 11–14 §§. Det beror i sin tur på att NIS-direktivet använder begreppet säkerhetsåtgärder i artikel 16. Kraven på åtgärder i den artikeln skiljer sig i hög grad från kraven i artikel 21 i NIS2-direktivet.

Utredningen delar inte myndighetens bedömning. Inledningsvis menar utredningen att det kan finnas skäl för att använda direktivets begrepp. Därutöver menar utredningen också att det skulle bli förvirrande att använda samma begrepp när kraven i hög grad är nya. Eftersom lagen från 2018 föreslås upphävas innebär det också att myndighetens föreskrifter behöver omarbetas.

7.1.2 Riskhanteringsåtgärder

Utredningens förslag: Verksamhetsutövaren ska vidta tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken. De ska utvärderas och särskilt innefatta följande:

1. Incidenthantering,
2. kontinuitetshantering
3. säkerhet i leveranskedjan,
4. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation,
5. strategier och förfaranden för användning av kryptografi och kryptering,
6. personalsäkerhet,
7. strategier för åtkomstkontroll och tillgångsförvaltning,
8. säkrade lösningar för kommunikation, och
9. lösningar för autentisering.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om riskhanteringsåtgärder. Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig.

Artikel 21.1 och 21.2 anger att medlemsstaterna ska säkerställa att väsentliga och viktiga verksamhetsutövare vidtar lämpliga och proportionella åtgärder för att hantera risker som hotar säkerheten i nätverk- och informationssystem och systemens fysiska miljö. I artikeln används såväl begreppet lämpliga som begreppet proportionella, som har snarlik betydelse, även om det också finns en skillnad. När det gäller lämpliga anges också att åtgärderna ska vara lämpliga i förhållande till risken. För begreppet proportionella anges det att hänsyn ska tas till verksamhetens grad av riskexponering, storlek, sannolikhet för att incidenter inträffar och deras allvarlighetsgrad, inbegripet

deras samhälleliga och ekonomiska konsekvenser. De angivna omständigheterna ovan som grad av riskexponering, storlek sannolikhet för att incidenter inträffar och deras allvarlighetsgrad, inbegripet samhälleliga och ekonomiska konsekvenser är alla omständigheter som handlar om risken. Sammantaget menar utredningen att åtgärderna ska vara proportionella i förhållande till risken. Det bör följa av lagtexten. Att åtgärderna även ska vara lämpliga i förhållande till risken blir då överflödigt, eftersom det inte tillför något. Den närmare anvisningen för proportionalitetsbedömningen bör följa av lagkommentaren.

Samtliga verksamhetsutövare som omfattas av förslaget till cybersäkerhetslagen är antingen väsentliga eller viktiga. Det innebär att kraven gäller för alla verksamhetsutövare. Det handlar om tekniska, driftsrelaterade och organisatoriska åtgärder. Åtgärderna ska ske hos verksamhetsutövaren och syftet är att förhindra eller minimera incidenters påverkan på mottagaren av tjänsterna eller andra tjänster.

Enligt artikel 21.1 andra stycket ska relevanta europeiska och internationella standarder beaktas i tillämpliga fall. Även av artikel 25.1 följer att medlemsstaterna, utan att föreskriva eller gynna användningen av viss teknik, ska uppmuntra användningen av europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem. Innebörden bör vara att medlemsstaterna inte kan uppställa krav om standarder. Med hänsyn härtill menar utredningen att det inte är möjligt att i lag föreskriva att standarder ska beaktas utan detta får uppmuntras på andra och frivilliga sätt.

I artikel 21.2 anges tio olika punkter som är obligatoriska. MSB har övergripande om de olika punkterna anfört att vissa punkter borde lyftas fram och stå i början, att vissa delar i en del punkter borde samordnas med delar i andra punkter samt att vissa punkter borde delas upp, eftersom de är särskilt viktiga.

Utredningen menar att när det gäller övergripande lagreglering är det tillräckligt att punkterna som speglar kraven återfinns i paragrafen, eftersom det ger en skyldighet, men att det saknar betydelse var i paragrafen kravet anges. Ett problem med att flytta delar av punkterna och samordna med andra punkter eller att lyfta upp en del ur en punkt till en egen punkt innebär också att sammanhanget går förlorat och ges en annan innebörd. För att kunna göra så måste det

stå klart att skrivningarna i artikeln är bristfälliga. Utredningen saknar underlag för en sådan slutsats.

Från PTS har anförts att det är angeläget att cybersäkerhetslagen använder så nära formuleringar från NIS2-direktivet som möjligt. Utredningens utgångspunkt är som följer av avsnitt 5.2.1 att direktiven inte ska införlivas direktivnära utan att förslagen ska utformas utifrån den systematik och terminologi som används i svensk rätt. Ett normalt språkbruk ska eftersträvas. Det följer även uttryckligen av regeringens direktiv att den terminologi som används i direktiven ska anpassas till vedertagna begrepp i nationell reglering. Med hänsyn till att regleringen omfattar ett stort antal olika sektorer menar utredningen att ett sådant förhållningssätt är nödvändigt. Motsvarande slutsats drogs även i arbetet med att införliva NIS-direktivet.

Åtgärderna ska baseras på en allriskansats och en riskanalys och de ska utvärderas.

Åtgärderna ska minst enligt artikel 21.2 omfatta strategier för riskanalys och informationssystemens säkerhet. När det gäller denna punkt menar utredningen att det inte behöver anges särskilt, eftersom det följer av utredningens förslag till övergripande reglering, se ovan. Detsamma gäller punkten f om strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet. Den inledande delen i punkten g om grundläggande praxis för cyberhygien är enligt utredningens bedömning onödig, eftersom cyberhygien är ett samlingsbegrepp för det som följer av artikeln i dess helhet. Andra delen av punkten g avser utbildning i cybersäkerhet. Utbildning behandlas specifikt och i ett större sammanhang i avsnitt 7.2.

I punkten b anges incidenthantering och driftskontinuitet i punkten c. Med driftskontinuitet avses enligt artikeln exempelvis hantering av säkerhetskopiering, katastrofhantering och krishantering. Från MSB har anförts att begreppet driftskontinuitet borde ersättas med det mer etablerade begreppet kontinuitetshantering. Utredningen ansluter sig till detta. Från MSB har vidare anförts att det behöver tydliggöras, precis som i artikeln, att säkerhetskopiering och krishantering ingår. Katastrofhantering ska ses som en del av krishantering. Här menar dock utredningen att eftersom detta är exempel på kontinuitetshantering är det mer lämpligt att det följer av författningskommentaren.

Av artikel 21.2 d följer vidare att säkerhet i leveranskedjan är ett minimikrav.

En särskild fråga är då vad som avses med säkerhet i leveranskedjan, hur många led i kedjan som verksamhetsutövaren ansvarar för. Av artikeln följer att i säkerhet i leveranskedja inbegrips säkerhetsaspekter som rör förbindelserna mellan varje verksamhetsutövare och dess *direkta* leverantörer eller tjänsteleverantörer. Det betyder enligt utredningens uppfattning att varje verksamhetsutövare endast behöver vidta riskhanteringsåtgärder i förhållande till sin leverantör. Innebörden skulle vara att varje verksamhetsutövare ansvarar för ett led i kedjan. De närmare bestämmelserna om detta bör följa av föreskrifter.

I punkten e anges säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem. Här ska inbegripas hantering av sårbarheter och sårbarhetsinformation. Från MSB har föreslagits att förvärv ersätts med anskaffning för att signalera att kraven gäller även när något inte köpts, exempelvis vid utkontraktering. En begränsning till endast inköp är olycklig.

Utredningen delar inte den bedömningen, eftersom förvärv betyder att ta över något med äganderätt. Det myndigheten föreslår är därmed en utvidgning av kraven i direktivet. Utredningen har förstås möjlighet att utvidga kraven, eftersom direktivet är ett minimidirektiv. Som framgått tidigare föreslår också utredningen en utvidgning i andra fall. För att kunna göra det krävs det dock underlag om att det är angeläget och en slutsats om att utvidgningen inte får oönskade konsekvenser. När det gäller utkontraktering omhändertas detta också till viss del i punkten om säkerhet i leveranskedjan.

I punkten h anges strategier och förfaranden för användning av kryptografi och när så är lämpligt kryptering. Därutöver finns det krav på personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning, säkrade lösningar för kommunikation, och lösningar för autentisering.

7.1.3 Systematiskt informationssäkerhetsarbete

Utredningens förslag: Verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om systematiskt och riskbaserat informations-

säkerhetsarbete. Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig.

Från MSB har anförts att det är viktigt att föreskriva att informationssäkerhetsarbetet ska ske systematiskt och riskbaserat på samma sätt som följer av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Utredningen noterar att detta krav inte följer av direktivet, men att det som myndigheten anför finns i gällande lag. I den lagens 11 § anges att leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.

Innebörden av informationssäkerhetsarbete är att skydda uppgifter som lagras, behandlas, hämtas eller överförs. De ska enligt artikel 6.2 skyddas utifrån aspekterna tillgänglighet, autenticitet, riktighet och konfidentialitet. Det betyder allt arbete som syftar till att säkerställa systemen, tjänsterna och informationen som lagras/behandlas/överförs genom dem. Därmed täcks exempelvis enligt skäl 79 även fysisk hantering av sådant som kan påverka systemen som tillträde till lokaler skyddas, trots att det inte är i digital form.

Ett systematiskt och riskbaserat informationssäkerhetsarbete enligt gällande lag innebär bland annat att arbetet bedrivs långsiktigt, kontinuerligt och metodiskt samt att det finns en tydlig rollfördelning med särskilt utpekat ansvar. Därigenom kan verksamhetens ledning på ett systematiskt sätt styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering. Detta kan bland annat innefatta olika typer av analyser som verksamhetsanalys, riskanalys och GAP-analys (analys som jämför nuvarande säkerhetsnivå med den önskade).[2]

[2] Prop. 2017/18:205 s. 39.

7.2 Ansvar och utbildning – riskhanteringsåtgärder

Utredningens bedömning:

1. Kravet i artikel 21.4 om att verksamhetsutövare som inte uppfyller kraven om riskhanteringsåtgärder utan dröjsmål förmås vidta korrigeringar uppfylls genom utredningens förslag om tillsyn samt ingripanden och sanktioner.
2. Ledningsorgan i enskilda verksamheter ska ha ett personligt ansvar för överträdelser av kraven om riskhanteringsåtgärder. Innebörden av detta ansvar är att det ska vara möjligt att vidta åtgärder eller rikta sanktioner mot denna personkrets. Av kapitel 9 följer att det ska vara möjligt att meddela ett förbud för en person att utöva en ledningsfunktion.

Utredningens förslag: Av cybersäkerhetslagen ska följa att ledningen i enskilda och offentliga verksamheter ska genomgå utbildning om riskhanteringsåtgärder och att anställda ska erbjudas sådan utbildning.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om utbildning. Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig.

Av artikel 21.4 följer att medlemsstaterna ska säkerställa att verksamhetsutövare som inte uppfyller kraven vidtar åtgärder utan dröjsmål. Det uppfylls genom utredningens förslag om tillsyn samt ingripanden och sanktioner, se kapitel 8 och 9.

Av artikel 20.1 följer att medlemsstaterna ska säkerställa att verksamhetsutövarens ledningsorgan godkänner och övervakar genomförandet av riskhanteringsåtgärderna. Syftet är att ledningsorganen kan ställas till svars för överträdelserna. Med ledningsorgan avses primärt styrelsen i ett aktiebolag (se vidare kapitel 9).

Enligt utredningens uppfattning behöver detta inte regleras civilrättsligt. Det följer redan av aktiebolagslagens (2005:551) 8 kap. 4 § att styrelsen svarar för bolagets organisation och förvaltningen av bolagets angelägenheter. I handelsbolag är det bolagsmännen själva som är ansvariga. För offentliga verksamhetsutövare följer särskilt av artikel 20.2 att artikel 20 inte påverkar ansvarsreglerna i nationell rätt för offentliga verksamheter.

Däremot framgår det av artikel 20.1 att ledningsorgan ska kunna ställas till svars för överträdelser avseende riskhanteringsåtgärder. Av kapitel 9 följer att det ska vara möjligt att meddela ett förbud för en person att utöva en ledningsfunktion.

Slutligen följer av artikel 20.2 att medlemsstaterna ska säkerställa att verksamhetsutövarnas ledningsorgan är skyldiga att genomgå utbildning om riskhanteringsåtgärder. Anställda ska erbjudas liknande utbildning. Som framgått ovan under avsnitt 7.1 är utbildning i cybersäkerhet en punkt som särskilt ska beaktas enligt artikel 21.2. Utredningen anser därför att kravet i artikel 20.2 om utbildning ska ses som en precisering av punkten om kravet om utbildning enligt avsnitt 7.1 ovan och ska därför utgå där för att i stället särskilt lagfästas enligt vad som anges här i detta avsnitt. Utredningen föreslår att detta krav övergripande ska framgå av lag, men att den närmare utformningen av krav på utbildning ska följa av föreskrifter. Det beror på att utbildningen behöver sektorsanpassas och även anpassas till olika målgrupper.

Detta krav bör gälla för såväl enskilda som offentliga verksamhetsutövare. För enskilda betyder det alltså styrelsen, men för offentliga bör det rimligen avse exempelvis generaldirektör med stab i myndighet och kommun- respektive regionstyrelsen i en kommun eller region. Anställda ska erbjudas utbildning. Den närmare omfattningen bör följa av föreskrifter som ska meddelas av tillsynsmyndigheten. MSB ska ges tillfälle att yttra sig.

7.3 Incidentrapportering

Utredningens förslag:

1. Med betydande incident avses

a. En incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller

b. en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande incident.

2. Verksamhetsutövaren ska som en *varning* underrätta CSIRT-enheten om betydande incidenter inom 24 timmar efter det att verksamhetsutövaren fått kännedom om den. Det ska anges om det finns misstanke om att incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter.

3. Verksamhetsutövaren ska också inom 72 timmar från tidpunkten för kännedom göra en incidentanmälan till CSIRT-enheten om betydande incidenter. Den ska innehålla en inledande bedömning av hur allvarlig den betydande incidenten är, konsekvenserna av den och förekomsten av angreppsindikatorer. Vidare ska varningen i punkt 2 uppdateras.

För verksamhetsutövare som erbjuder betrodda tjänster ska en incidentanmälan ska göras inom 24 timmar.

CSIRT-enheten får begära ytterligare information av verksamhetsutövaren.

Verksamhetsutövaren ska samtidigt även informera kunder som kan antas påverkas av den betydande incidenten. Kunderna ska vid behov informeras om avhjälpande åtgärder. Detsamma gäller betydande cyberhot.

4. Verksamhetsutövaren ska inom en månad från incidentanmälan i punkt 3 lämna en *slutrapport* till CSIRT-enheten. Om incidenten fortfarande är pågående ska i stället en *lägesrapport* lämnas som ska kompletteras med en slutrapport en månad efter det att incidenten har hanterats. Slutrapporten eller lägesrapporten ska innehålla en beskrivning av

a. Incidenten och dess konsekvenser,
b. hur allvarlig incidenten bedöms vara,
c. vad som sannolikt utlöst incidenten,
d. åtgärderna för att begränsa incidenten, och
e. incidentens möjliga gränsöverskridande effekter.

5. Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om incidentrapporteringen.

I artikel 23 finns bestämmelser om incidentrapportering.

Av artikel 23.1 följer att medlemsstaterna ska säkerställa att verksamhetsutövare som omfattas av cybersäkerhetslagen utan dröjsmål

underrättar sin CSIRT-enhet eller sin behöriga myndighet om betydande incidenter. MSB är CSIRT-enhet i Sverige. Om rapportering sker till behörig myndighet ska den vidarebefordra uppgiften till CSIRT-enheten. Utredningen föreslår att underrättelsen av effektivitetsskäl sker direkt till CSIRT-enheten, som utan dröjsmål ska tillgängliggöra informationen i incidentrapporter för tillsynsmyndigheterna, se avsnitt 10.2.3.

Med betydande incident avses enligt artikel 23.3 en incident som orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomisk skada för den berörda verksamhetsutövaren eller/och har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada. Av artikeln framgår alltså inte om det är tillräckligt med angivna konsekvenser för antingen verksamhetsutövaren eller annan eller om det krävs konsekvenser för såväl verksamhetsutövaren som annan person. Av skäl 101 följer dock att det är tillräckligt med angivna konsekvenser för antingen verksamhetsutövaren eller annan person för att det ska vara en betydande incident. Det får ankomma på MSB att i föreskrifter mer detaljerat precisera innebörden av betydande incident. En slutsats är att definitionen av betydande incident är väldigt vid. Här ska dock beaktas att ett grundläggande krav är att det är en incident. Med incident avses enligt artikel 6 punkt 6 i NIS2-direktivet en händelse som undergräver tillgängligheten, autenciteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom nätverks- och informationssystem.

Ett tillbud, definieras i samma artikel punkt 5 på likartat sätt, men med skillnaden att händelsen kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos uppgifterna eller tjänsterna, men som hindrades från att utvecklas eller som inte uppstod. Cyberhot definieras enligt punkt 10 i artikel 6 i artikel 2.8 i förordning (EU) 2019/881.[3] Definitionen av cyberhot är där en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare dessa system och andra personer. Dessa definitioner ska följa av utredningens författningsförslag.

[3] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

I artikel 23.4 anges rapporteringskraven. Som framgår av skäl 101 är rapporteringssystemet uppbyggt med en strategi om flera steg. Syftet är att uppnå en balans mellan å ena sidan snabb rapportering för att begränsa spridning och å andra sidan en ingående rapportering med syfte att dra lärdomar.

Det följer av 23.4 a att verksamhetsutövare som omfattas ska utan dröjsmål och under alla omständigheter inom 24 timmar efter kännedom lämna en första varning till CSIRT-enheten, det vill säga MSB om en betydande incident inträffat. Verksamhetsutövaren ska vid den tidpunkten också ange om det finns misstanke om att incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter. Utredningen tolkar artikeln på det sättet att kravet är att en varning ska lämnas inom 24 timmar.

Inom 72 timmar från kännedom ska verksamhetsutövaren lämna ytterligare information. Det ska då ges en inledande bedömning av hur allvarlig den betydande incidenten är, konsekvenserna av den och förekomsten av angreppsindikatorer. Vidare ska varningen ovan uppdateras.

CSIRT-enheten får begära ytterligare information.

Verksamhetsutövaren ska inom en månad från incidentanmälan i punkt 2 lämna en slutrapport till CSIRT-enheten. Om incidenten fortfarande är pågående ska i stället en lägesrapport lämnas som ska kompletteras med en slutrapport en månad efter det att incidenten har hanterats. Slutrapporten eller lägesrapporten ska innehålla en beskrivning av

a) Incidenten och dess konsekvenser,

b) hur allvarlig incidenten bedöms vara,

c) vad som sannolikt utlöst incidenten,

d) åtgärderna för att begränsa incidenten, och

e) incidentens möjliga gränsöverskridande effekter.

I sista stycket i artikel 23.4 anges att en tillhandahållare av betrodda tjänster som ett undantag från punkt b i artikel 23.4 ska underrätta CSIRT-enheten. Innebörden är att tillhandahållare av betrodda tjänster ska lämna sin incidentanmälan efter 24 timmar i stället för 72 timmar.

Slutligen anges också i artikel 23.1 att när så är lämpligt ska verksamhetsutövaren utan dröjsmål även underrätta mottagarna av deras tjänster om betydande incidenter som sannolikt inverkar negativt på tillhandahållandet av tjänsterna. Innebörden bör enligt utredningens uppfattning vara att verksamhetsutövaren även ska underrätta sina kunder som kan antas påverkas av den betydande incidenten. I denna del anges inga tidskrav och inte heller om det ska ske i samband med varning, incidentanmälan eller slutrapport till myndigheten.

Utredningen föreslår att det ska ske efter senast 72 timmar i samband med incidentanmälan.

I artikel 23.2 anges också att verksamhetsutövare utan dröjsmål underrättar de mottagare av deras tjänster som kan påverkas av ett betydande cyberhot och samtidigt informera om avhjälpande åtgärder.

Av artikel 23.5–10 följer skyldigheter för CSIRT-enheten. Dessa är analyserade i kapitel 10.

Enligt artikel 30.1 följer att medlemsstaterna ska säkerställa att det utöver den underrättelseskyldighet som följer av ovanstående ska vara möjligt att på frivillig väg lämna uppgifter. Det avser enligt 30.1 a såväl verksamhetsutövare som omfattas av cybersäkerhetslagen som andra verksamhetsutövare avseende incidenter, cyberhot och tillbud. Det ska noteras att här hänvisas till incidenter, inte betydande incidenter och till cyberhot, men inte betydande sådana enligt artikel 23. Vidare nämns också tillbud.

Detta skulle enligt utredningens uppfattning inte behöva regleras särskilt. Enligt 19 § förvaltningslagen gäller att en enskild kan formlöst inleda ett ärende hos en myndighet genom en ansökan, anmälan eller annan framställning.

I artikel 30.2 följer sedan att myndigheterna ska behandla dessa underrättelser i enlighet med de förfaranden som följer av artikel 23. Inte heller det skulle behöva regleras särskilt, eftersom myndigheter redan enligt förvaltningslagen är skyldig att handlägga ärenden som en enskild inlett. Att CSIRT-enheten i vissa fall behöver informera den gemensamma kontaktpunkten följer av de förfaranden som utredningen föreslår i kapitel 10.

Vidare följer det dock av artikeln att informationen ska förbli konfidentiell och skyddas på lämpligt sätt. Det är inte helt förenligt med den svenska grundlagen, eftersom inkomna handlingar till myndigheter som huvudregel är offentliga, även om det finns möjligheter att sekretessbelägga dem.

Slutligen följer det av sista meningen i artikel 30 att den verksamhetsutövare som lämnat underrättelser inte ska åläggas ytterligare skyldigheter på grund av underrättelserna. Detta gäller dock inte ”förebyggande, utredning, avslöjande och lagföring av brott.” Vilka dessa ”ytterligare” skyldigheter skulle kunna vara är svårt att förutse. Det anförda betyder att den sista stycket i artikeln inte fullt ut rimmar med svensk rätt. Samtidigt menar utredningen att de förfaranden som redan finns tillgängliga i svensk rätt tillsammans med dem som föreslås i kapitel 8 är tillräckliga för att syftet med artikel 30 ska vara uppfyllt. Därutöver finns det möjligheter för MSB att på samma sätt som sker i dag att genom föreskrifter införa förenklade möjligheter till frivillig rapportering. Myndigheten har ett bemyndigande att kunna göra så. Utredningen kommer också att i sitt slutbetänkande återkomma med överväganden om ändring i offentlighets- och sekretesslagen (2009:400).

Slutligen anges i artikel 23.11 att kommissionen får anta genomförandeakter som närmare anger bland annat förfarandet för underrättelser enligt ovan.

7.4 Certifiering

Utredningens bedömning: Certifieringskrav bör införas först genom kommissionens delegerade akter.

I artikel 24.1 anges att medlemsstaterna *får* ålägga verksamhetsutövare att använda certifierade IKT-produkter, IKT-tjänster och IKT-processer enligt europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 49 i förordning (EU) 2019/881.[4] Dessutom ska medlemsstaterna uppmuntra verksamhetsutövare att använda kvalificerade betrodda tjänster.

Det anges dock vidare i 24.2 att kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 38. Av den artikeln följer villkor för kommissionen att anta delegerade akter, bland annat följer av 38.2 att befogenheten att anta delegerade akter enligt 24.2 och 24.3

[4] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

gäller i fem år från den 16 januari 2023 och att delegeringen när som helst får återkallas av Europaparlamentet eller rådet.

Syftet med att kommissionen enligt 24.2 ges befogenhet att anta delegerade akter är att de ska komplettera NIS2-direktivet genom att ange vilka verksamhetsutövare som ska vara skyldiga att använda certifierade IKT-produkter, IKT-tjänster och IKT-processer. De delegerade akterna ska antas om det har fastställts att säkerhetsnivån är otillräcklig och ska omfatta en genomförandeperiod. Innan kommissionen antar sådana delegerade akter ska den göra en konsekvensbeskrivning och genomföra samråd i enlighet med artikel 56 i förordning (EU) 2019/881.

Av det anförda följer att kommissionen kan anta genomförandeakter som komplement till direktivet, men att medlemsstaterna redan dessförinnan får införa certifieringskrav. Utredningen menar att det är rimligt att avvakta kommissionens beslut i denna fråga, eftersom kraven ska införas först om cybersäkerhetsnivån är otillräcklig och dessutom föregås av bland annat en konsekvensanalys.

8 Tillsyn

8.1 Inledning

Varje medlemsstat ska utse en eller flera behöriga myndigheter med ansvar för cybersäkerhet och för de tillsynsuppgifter som följer av NIS2-direktivet. De behöriga myndigheterna ska övervaka genomförandet av direktivet på nationell nivå.

I kommittédirektivet anges att systemet för tillsyn bör utgå från den struktur som finns enligt dagens regelverk. Enligt den nu gällande NIS-lagen finns det för varje sektor och för de digitala tjänster som omfattas av lagen en utpekad tillsynsmyndighet som utövar tillsyn över att regelverket följs. Utredningen ska göra en utvärdering av den tillsyn som har bedrivits enligt den nuvarande NIS-regleringen samt föreslå vilka myndigheter som ska utöva tillsyn över de tillkommande sektorerna i NIS2-direktivet. Utredningen ska också analysera vilka ändringar av den befintliga tillsynsstrukturen som i övrigt behövs samt analysera vilka befogenheter i fråga om tillsyn och sanktioner som tillsynsmyndigheterna bör ha.

Mot bakgrund av detta är det utredningens utgångspunkt att de tillsynsmyndigheter som i dag ansvarar för tillsyn enligt NIS-regleringen även fortsättningsvis har kvar ansvaret för dessa sektorer. För de nya sektorer där det i dag saknas tillsyn behöver utredningen föreslå vilken myndighet som bör få den uppgiften. Inriktningen bör enligt kommittédirektivet vara att om det redan finns en myndighet med tillsynsuppgifter inom informationssäkerhet i den nya sektorn är det naturligt att den myndigheten även utses till tillsynsmyndighet enligt NIS2-direktivet.

8.2 Generella utgångspunkter för reglering om tillsyn

I regeringens skrivelse till riksdagen, *En tydlig, rättssäker och effektiv tillsyn*,[1] redovisas generella bedömningar av hur en tillsynsreglering bör vara utformad. Skrivelsen är avsedd att vara ett stöd och en vägledning vid bland annat översyn av materiella regelverk av olika slag. I skrivelsen framhålls betydelsen av enhetlighet i fråga om offentlig tillsyn. Det lämnas dock utrymme för att göra avsteg från de bedömningar som görs i skrivelsen. En utgångspunkt i skrivelsen är att begreppet tillsyn främst bör användas för verksamhet som avser självständig granskning för att kontrollera om tillsynsobjektet uppfyller krav som följer av lagar och andra bindande föreskrifter. Ett grundläggande moment i tillsynen är därför enligt skrivelsen att tillsynsorganet har författningsreglerade möjligheter att ingripa. Tillsynsorganen bör också ha rätt att av den objektsansvarige få del av de upplysningar eller handlingar som behövs för tillsynen. Likaså bör organet ha tillträdesrätt till utrymmen som används i den tillsynspliktiga verksamheten. Tillsynsorganen bör även ha möjlighet att begära biträde från Polismyndigheten och Kronofogdemyndigheten.

Vidare bör tillsynsorganen enligt skrivelsen ha möjlighet att ålägga den som är objektsansvarig att utöva egen kontroll av sin verksamhet. Samtliga ingripanden bör kunna överklagas. Ett viktigt skäl för att precisera tillsynsbegreppet anges vara att en tydlig definition gör det enklare att skilja granskande från främjande verksamhet. Ett strikt avgränsat tillsynsbegrepp anges dock inte hindra att tillsynsmyndigheter även i fortsättningen kan ha till uppgift att arbeta främjande och förebyggande för att effektivt uppnå lagstiftningens mål. Det framhålls att det i allmänhet inte är lämpligt att tillsynsmyndigheten ger råd om hur tillsynsobjekten ska agera i specifika ärenden. Ett skäl till det anges vara att det kan uppstå svårigheter, om tillsynsmyndigheten tidigare lämnat mycket precisa råd i ärenden som sedan blir föremål för tillsyn. Samtidigt framhålls att inom vissa tillsynsområden kan skäl tala för att, utöver upplysningar om gällande rätt, även rekommendationer och vägledning ska vara en del av tillsynen.

[1] Skr. 2009/10:79, bet. 2009/10:FiU12.

8.3 Tillsyn enligt NIS-direktivet

Varje medlemsstat ska enligt artikel 8.1 och 8.2 i NIS-direktivet utse en eller flera myndigheter som ska övervaka direktivet på nationell nivå. Enligt 21 § NIS-lagen ska den myndighet som regeringen bestämmer vara tillsynsmyndighet. I 17 § NIS-förordningen regleras vilka myndigheter som ansvarar för tillsyn över vilka sektorer, se avsnitt 3.1.2.

8.3.1 Utredningens enkät om tillsyn

För att få en överblick över den tillsyn som genomförts sedan NIS-lagens ikraftträdande den 1 augusti 2018 har utredningen ställt ett antal frågor till tillsynsmyndigheterna om deras arbete med tillsyn enligt NIS-regleringen.

Svaren visar en stor spridning på antal tillsynsobjekt inom de olika sektorerna.

Tabell 8.1 Antal tillsynsobjekt per tillsynsmyndighet

Tillsynsmyndighet	Antal tillsynsobjekt
Statens energimyndighet	249
Finansinspektionen	12
IVO	240
Livsmedelsverket	94
PTS	9
Transportstyrelsen	130

PTS har även tillsyn över cirka 40–50 leverantörer av digitala tjänster. För digitala tjänster gäller att tillsynsåtgärder endast får vidtas när tillsynsmyndigheten har befogad anledning att anta att en leverantör inte uppfyller kraven enligt NIS-regleringen. PTS har inte inlett något tillsynsärende rörande digitala tjänster. Dessa leverantörer har heller ingen skyldighet att anmäla sig till tillsynsmyndigheten så antalet leverantörer är PTS uppskattning.

Svaren visar också en stor skillnad i antalet tillsynsärenden som myndigheterna inlett sedan NIS-lagens ikraftträdande den 1 augusti 2018. En förklaring till detta är att det skiljer sig avsevärt hur många leverantörer som tillsynsmyndigheterna bedriver tillsyn över. Trots

detta så visar svaren att relativt få tillsynsärenden inletts i förhållande till antalet leverantörer i några sektorer.

Tabell 8.2 Antal tillsynsärenden

Tillsynsmyndighet	Antal tillsynsärenden
Statens energimyndighet	140
Finansinspektionen	0
IVO	159
Livsmedelsverket	118
PTS	39
Transportstyrelsen	11

Även när det gäller beslut om sanktionsavgifter så finns en relation mellan dessa och antalet tillsynsobjekt i sektorn.

Tabell 8.3 Antal beslut om sanktionsavgifter

Tillsynsmyndighet	Antal sanktionsbeslut
Statens energimyndighet	21
Finansinspektionen	0
IVO	28
Livsmedelsverket	12
PTS	0
Transportstyrelsen	5

Finansinspektionen har gjort bedömningen att kraven i Finansinspektionens föreskrifter[2] överensstämmer med MSB:s föreskriftskrav avseende det systematiska och riskbaserade informationssäkerhetsarbetet. Mot bakgrund av det har Finansinspektionen inte sett behov av ytterligare föreskrifter på området. De tillsynsinsatser som utförts har utgått från Finansinspektionens föreskrifter och har bland annat skett genom att uppföljning av risker kopplat till it- och informationssäkerhet lyfts i riktade tillsynsaktiviteter mot enskilda institut.

[2] Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem (FFFS 2014:5), Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker (FFFS 2014:4) och Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1).

8.3.2 Samarbetsforum

Av 21 § NIS-förordningen framgår att MSB ska leda ett samarbetsforum där tillsynsmyndigheterna och Socialstyrelsen ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

MSB har låtit göra en utvärdering av resultatet av Sveriges implementering av NIS-direktivet.[3] Rapporten innehåller intervjuer med MSB, tillsynsmyndigheter och leverantörer som omfattas av NIS-regelverket. Av rapporten framgår att tillsynsmyndigheterna anser att samarbetsforumet bidragit till värdefullt erfarenhetsutbyte mellan myndigheterna. Det har också bidragit till viss harmonisering av tillsynen. Bland annat har gruppen tagit fram kriterier för hur myndigheterna ska göra urvalet av vilka verksamhetsutövare som ska kontrolleras via tillsyn. Samarbetsforumet har också bidragit till att nya tillsynsmyndigheter kunnat dra nytta av metodstöd för att utforma sin tillsynsprocess. När det gäller myndigheternas föreskriftsarbete så har det funnits brister i samordningen. Detta har resulterat i att föreskrifterna i de olika sektorerna innehåller olika begrepp och krav trots att de utgår från samma grund. Av rapporten framgår också att flera tillsynsmyndigheter efterfrågar en tydligare styrning från MSB och att myndigheten i större utsträckning får mandat att vägleda tillsynsmyndigheterna.

Livsmedelsverket, Transportstyrelsen och SKR har framfört till utredningen att behovet av samordning kommer att öka med den nya regleringen när det blir fler tillsynsmyndigheter och verksamhetsutövare.

8.3.3 Utredningens slutsatser gällande nuvarande system för tillsyn

Vid implementeringen av NIS-direktivet anförde regeringen att direktivet omfattar verksamheter av vitt skilda slag och att detta talade för att ha olika tillsynsmyndigheter för respektive sektor.[4] Det som främst talade för att utse en tillsynsmyndighet för samtliga sektorer var enligt regeringen, och flera remissinstanser, att tillsyn när det gäller

[3] *Utvärdering av resultatet av Sveriges implementering av NIS-direktivet*, Myndigheten för samhällsskydd och beredskap, slutrapport 2022-12-20.
[4] Prop. 2017/18:205 s. 57.

säkerhet i nätverks- och informationssystem kräver särskild kompetens. Regeringen ansåg dock att det inom de berörda sektorerna var viktigt att höja kompetensen när det gäller informationssäkerhet och att tillsynsmyndigheterna behövde skaffa den kompetens som krävs.

De myndigheter som utsågs till tillsynsmyndigheter hade olika grad av erfarenhet av att bedriva tillsyn och att arbeta med säkerhet i nätverks- och informationssystem. Vissa myndigheter var tvungna att ta fram nya processer och rekrytera nödvändig kompetens medan andra kunde dra nytta av befintliga processer och redan hade tillgång till nödvändig kompetens. Detta har inneburit att det tagit olika lång tid för tillsynsmyndigheterna att utfärda föreskrifter och att börja bedriva tillsyn.

Riksrevisionen har granskat Transportstyrelsens tillsynsverksamhet och resultatet av granskningen redovisas i granskningsrapporten *Transportstyrelsens tillsyn – styrning och prioritering* (RiR 2022:24). Av rapporten framgår att Transportstyrelsen bedrivit mycket lite faktisk tillsyn enligt NIS-regleringen. Den tillsyn som har bedrivits har i huvudsak syftat till att öka anmälningsgraden. En orsak som Transportstyrelsen angett för att tillsynen knappt kommit i gång är svårigheter att rekrytera kompetent personal. Riksrevisionen gör bedömningen att Transportstyrelsens problem är en följd av att myndigheten inte tagit tillräcklig höjd för de krav som ställs vid inrättandet av nya tillsynsområden.

De föreskrifter som utfärdats sedan NIS-lagens ikraftträdande den 1 augusti 2018 är följande:

- Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster; MSBFS 2021:9. Föreskrifterna trädde i kraft den 1 mars 2022 när MSBFS 2018:7 upphörde att gälla. MSBFS 2018:7 trädde i kraft den 1 november 2018.
- Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster; MSBFS 2018:8. Föreskrifterna trädde i kraft den 1 november 2018.

- Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster; MSBFS 2018:9. Föreskrifterna trädde i kraft den 1 mars 2019.
- Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av digitala tjänster; MSBFS 2018:10. Föreskrifterna trädde i kraft den 1 mars 2019.
- Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet; MSBFS 2018:11. Föreskrifterna trädde i kraft den 1 mars 2019.
- Statens energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn; STEMFS 2021:3. Föreskrifterna trädde i kraft den 1 mars 2021.
- Post- och telestyrelsens föreskrifter och allmänna råd om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur; PTSFS 2021:3. Föreskrifterna trädde i kraft den 1 juni 2021.
- Transportstyrelsens föreskrifter och allmänna råd om säkerhetsåtgärder för leverantörer inom transportsektorn; TFFS 2022:14. Föreskrifterna trädde i kraft den 1 juli 2022.
- Livsmedelsverkets föreskrifter om informationssäkerhetsåtgärder för samhällsviktiga tjänster inom sektorn leverans och distribution av dricksvatten; LIVFS 2022:2. Föreskrifterna trädde i kraft den 1 september 2022.
- Livsmedelverkets föreskrifter om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar; LIVFS 2008:13. Ändringen i 6 § avseende leverantörer som omfattas av LIVFS 2022:2 trädde i kraft den första september 2022.

MSB:s föreskrifter trädde i kraft i anslutning till NIS-lagens ikraftträdande medan tillsynsmyndigheternas föreskrifter trädde i kraft mellan den 1 mars 2021 och den 1 september 2022. I sektorn hälso- och sjukvård har Socialstyrelsen ännu inte beslutat om några föreskrifter.

Utredningen har med hänsyn till den korta tid som utredningen har till sitt förfogande inte kunnat genomföra någon djupare analys av den tillsyn som bedrivits enligt den nuvarande NIS-regleringen, men tillsynsmyndigheternas svar visar att samtliga myndigheter bedrivit tillsyn enligt NIS-regleringen. Det är dock inte möjligt att dra några djupare slutsatser om tillsynsarbetets effektivitet endast utifrån antalet tillsynsärenden eftersom dessa kan avse så vitt skilda saker såsom skyldigheten att anmäla sig som leverantör av en samhällsviktig tjänst eller leverantörens säkerhetsarbete. Utredningen kan dock konstatera att flera tillsynsmyndigheter under perioden från den 1 augusti 2018 till den 24 mars 2023 i huvudsak bedrivit tillsyn rörande leverantörernas anmälningsplikt. Detta innebär att tillsyn rörande leverantörernas säkerhetsarbete varit begränsad under denna period. En bidragande orsak till detta är att det tagit lång tid för tillsynsmyndigheterna att besluta om föreskrifter om säkerhetsåtgärder som anger vilka krav som leverantören behöver uppfylla.

Mot bakgrund av att det tagit lång tid att utfärda föreskrifter och komma i gång med tillsyn bedömer utredningen att det troligen går att dra liknande slutsatser om flera tillsynsmyndigheter som Riksrevisionen gjort avseende Transportstyrelsen. Utredningen bedömer ändå att nuvarande system för tillsyn är ändamålsenligt, men att föreslagna tillsynsmyndigheter måste ta höjd för den nya cybersäkerhetslagen. Det kan också finnas skäl för regeringen att följa upp arbetet med föreskrifter och tillsyn. I sektorn hälso- och sjukvård där det ännu inte beslutats om några föreskrifter kan det också finnas anledning att se över om bemyndigandet att besluta om föreskrifter bör flyttas från Socialstyrelsen till IVO som är tillsynsmyndighet. Utredningen återkommer till frågan om föreskrifter i avsnitt 8.4.5.

8.4 Utredningens överväganden och förslag

8.4.1 System för tillsyn

Utredningens bedömning: Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Det ska finnas en eller flera tillsynsmyndigheter för varje sektor som utövar tillsyn.

Nuvarande system för tillsyn innebär att sex tillsynsmyndigheter ansvarar för tillsynen över sju sektorer av samhällsviktiga tjänster samt sektorn digitala tjänster. Vid implementeringen av NIS-direktivet övervägde utredningen om det skulle utses en tillsynsmyndighet per sektor eller om en tillsynsmyndighet skulle ha ansvaret för samtliga sektorer. Efter att ha övervägt för och nackdelar med båda alternativen föreslog utredningen att det skulle utses en tillsynsmyndighet för varje sektor.[5]

Mot bakgrund av skillnaderna i nationella förvaltningsstrukturer, bör medlemsstaterna även enligt NIS2-direktivet kunna utse eller inrätta en eller flera behöriga myndigheter med ansvar för cybersäkerhet och för tillsynsuppgifterna enligt direktivet (artikel 8 och skäl 38).

NIS2-direktivet innebär att antalet sektorer utökas till 18 och att det även tillkommer delsektorer och nya typer av verksamhetsutövare. Detta innebär att antalet verksamhetsutövare som kommer att omfattas av den nya regleringen kraftigt kommer att öka. Även om det kan finnas fördelar med att samla tillsynsansvaret i en central tillsynsmyndighet så skulle det bli en mycket omfattande uppgift för en myndighet att utöva tillsyn över samtliga verksamhetsutövare. Nuvarande tillsynsmyndigheter har också byggt upp kunskap och erfarenhet i arbetet med den nuvarande NIS-regleringen. Enligt kommittédirektivet ska utredningen utgå ifrån den struktur som finns enligt dagens regelverk. Att samla all tillsyn till en central myndighet ligger därmed utanför utredningens uppdrag och skulle behöva utredas i särskild ordning. Det är därför utredningens bedömning att det ska utses en tillsynsmyndighet för varje sektor även vid implementeringen av NIS2-direktivet.

Nästa fråga blir då om det bör utses nya tillsynsmyndigheter för tillkommande sektorer eller om tillsynsansvaret ska läggas på en myndighet som redan bedriver NIS-tillsyn. För vissa tillkommande sektorer som till exempel vätgas finns en tydlig koppling till en myndighet, nämligen Statens energimyndighet som i dag bedriver tillsyn i sektorn energi. För andra sektorer är det mindre tydligt vilken myndighet som bör bedriva tillsyn, till exempel för sektorn tillverkning.

Tillsyn när det gäller cybersäkerhet kräver expertkunskap som det råder en stor konkurrens om på arbetsmarknaden. Det är därför utredningens mening att det inte vore ett effektivt utnyttjande av

[5] SOU 2017:36 s. 163 ff.

statens resurser att alltför många myndigheter ska rekrytera sådan kompetens och bygga upp en organisation för att bedriva tillsyn över endast en tillkommande sektor eller typ av verksamhetsutövare. Utredningen anser därför i stället att det är en mer effektiv lösning att så långt möjligt nyttja den kompetens som finns hos befintliga tillsynsmyndigheter när tillsynsansvaret för nya sektorer ska fördelas. Utredningens utgångspunkt är därför att en befintlig tillsynsmyndighet i första hand bör få tillsynsansvar över en tillkommande sektor i NIS2-direktivet.

I de fall detta inte är lämpligt eller det saknas en sådan tillsynsmyndighet är utredningens utgångspunkt att tillsynsansvaret om möjligt bör läggas på en myndighet som redan bedriver tillsyn rörande cybersäkerhet.

Utredningen behöver också beakta att det bör vara samma tillsynsmyndighet för NIS2- och CER-direktivet för de sektorer som omfattas av båda direktiven.

8.4.2 Tillsynsmyndigheter i Sverige

Utredningens bedömning: Statens energimyndighet ska vara tillsynsmyndighet för sektorn energi, Transportstyrelsen för sektorerna transporter och del av sektorn tillverkning, Finansinspektionen för sektorerna bankverksamhet och finansmarknadsinfrastruktur, Inspektionen för vård och omsorg för del av hälso- och sjukvårdssektorn, Läkemedelsverket för del av hälso- och sjukvårdssektorn och del av sektorn tillverkning, Livsmedelsverket för sektorerna dricksvatten, avloppsvatten och produktion, bearbetning och distribution av livsmedel, Post- och telestyrelsen för sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster, post- och budtjänster och sektorn rymden, länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län för sektorerna offentlig förvaltning, avfallshantering, forskning, del av sektorn tillverkning och tillverkning, produktion och distribution av kemikalier samt lärosäten med examenstillstånd. Detta ska följa av förslag till cybersäkerhetsförordning.

I de sektorer som är oförändrade i förhållande till det första NIS-direktivet är utredningens förslag att befintliga tillsynsmyndigheter fortsätter att ansvara för dessa. Det innebär att Transportstyrelsen ska vara tillsynsmyndighet för sektorn transporter, Finansinspektionen för sektorerna bankverksamhet och finansmarknadsinfrastruktur och Livsmedelsverket för sektorn dricksvatten. Som framgått av kapitel 4 innebär dock NIS2-direktivet också att ett flertal nya sektorer, undersektorer och typer av verksamhetsutövare kommer att omfattas av reglering. Utredningen föreslår nedan vilka myndigheter som ska utöva tillsyn över dessa förändrade sektorer.

Energi

I sektorn energi tillkommer verksamhetsutövare inom delsektorerna elektricitet, fjärrvärme eller fjärrkyla, olja och vätgas. Statens energimyndighet är i dag tillsynsmyndighet för sektorn energi och myndigheten bör därför även fortsättningsvis vara tillsynsmyndighet för sektorn och även ansvara för tillsyn över de nya verksamhetsutövare som kommer att omfattas i sektorn.

Hälso- och sjukvård

I sektorn hälso- och sjukvård tillkommer EU-referenslaboratorier, forskning och utveckling avseende läkemedel, tillverkning av farmaceutiska basprodukter och läkemedel samt tillverkning av medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan. IVO är utpekad tillsynsmyndighet för sektorn som i dag dock endast omfattar vårdgivare. Läkemedelsverket är förvaltningsmyndighet för verksamhet som rör läkemedel och medicintekniska produkter. Läkemedelsverket ansvarar också för kontroll och tillsyn av läkemedel. Myndigheten ansvarar vidare för tillsyn, inklusive marknadskontroll, av medicintekniska produkter, samt för att utse och övervaka anmälda organ för medicintekniska produkter. De nya verksamhetsutövarna i sektorn har en tydlig koppling till Läkemedelsverkets nuvarande tillsynsuppdrag. Med hänsyn till detta föreslår utredningen att Läkemedelsverket ska vara tillsynsmyndighet för de tillkommande verksamhetsutövarna i sektorn även om myndigheten

inte i dag bedriver tillsyn rörande cybersäkerhet. Utredningen föreslår att IVO fortsätter att ansvara för vårdgivare.

Avloppsvatten

Avloppsvatten är en ny sektor i NIS2-direktivet. Länsstyrelsen är tillsynsmyndighet för de stora avloppsreningsverken och kommunerna är tillsynsmyndighet för de mindre. Vid införandet av NIS-direktivet bedömde utredningen att Livsmedelsverket skulle vara tillsynsmyndighet för sektorn leverans och distribution av dricksvatten.[6] Myndigheten hade då inget tillsynsansvar inom sektorn. Kommunerna utövar offentlig kontroll över dricksvattenanläggningar och länsstyrelserna samordnar kommunernas verksamhet i länet. Eftersom Livsmedelsverket är tillsynsmyndighet för leverans och distribution av dricksvatten enligt NIS-direktivet och därmed har en upparbetad organisation för tillsyn av dessa anläggningar föreslår utredningen att myndigheten även bör vara tillsynsmyndighet för sektorn avloppsvatten.

Digital infrastruktur

I sektorn digital infrastruktur tillkommer leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, tillhandahållare av betrodda tjänster, tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster. PTS är i dag utpekat tillsynsmyndighet för sektorn. PTS bedriver också tillsyn över tillhandahållare av betrodda tjänster och tillhandahållare av allmänna kommunikationsnät samt allmänt tillgängliga elektroniska kommunikationstjänster. Utredningen föreslår därför att PTS även fortsatt ska vara tillsynsmyndighet för sektorn inklusive de nya verksamhetsutövarna som kommer att omfattas.

[6] SOU 2017:36 s. 170 ff.

Förvaltning av IKT-tjänster

Förvaltning av IKT-tjänster mellan företag är en ny sektor i NIS2-direktivet som innefattar två typer av verksamhetsutövare. Dessa är leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster. Utredningen har inte identifierat någon myndighet som ansvarar för tillsyn över denna kategori av verksamhetsutövare. IKT-tjänst avser en tjänst som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via nätverks- och informationssystem. Utredningen anser att det ligger närmast till hands att den myndighet som ansvar för sektorn digital infrastruktur även ansvarar för förvaltning av IKT-tjänster. Utredningen föreslår därför att PTS ska vara tillsynsmyndighet för sektorn.

Offentlig förvaltning

Offentlig förvaltning är en ny sektor i NIS2-direktivet. Sektorn innefattar statliga myndigheter,[7] regioner och kommuner.

Tillsynsansvaret enligt säkerhetsskyddsregleringen när det gäller informationssäkerhet i offentlig förvaltning är fördelat mellan Försvarsmakten och Säkerhetspolisen som ansvarar för vissa utpekade myndigheter och fyra länsstyrelser som ansvarar för kommuner, regioner och statliga myndigheter som inte hör till någon annan myndighets ansvarsområde.

MSB är inte tillsynsmyndighet rörande cybersäkerhet men ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och regioner samt företag och organisationer.[8]

Enligt 13 § i förordningen (2022:524) om statliga myndigheters beredskap ansvarar statliga myndigheter för att de egna informationshanteringssystemen uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. MSB får meddela ytterligare föreskrifter om sådana säkerhetskrav för informationshanteringssystem som avses i

[7] Några myndigheter är dock undantagna från cybersäkerhetslagens tillämpningsområde, se vidare kapitel 5.
[8] 11 a § i förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

13 § utom i fråga om Regeringskansliet, kommittéväsendet och Försvarsmakten. MSB har med stöd av förordningen beslutat om föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter och föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter.

Enligt 14 § i förordningen ska en myndighet skyndsamt rapportera it-incidenter till MSB som inträffat i den rapporterande myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller som inträffat i tjänster som myndigheten tillhandahåller åt en annan organisation. MSB får enligt förordningen meddela närmare föreskrifter om it-incidentrapportering vilket myndigheten gjort i föreskrifter (MSBFS 2020:8) om rapportering av it-incidenter för statliga myndigheter. MSB har dock ingen befogenhet att bedriva tillsyn över att regelverket följs.

I betänkandet *En ny säkerhetsskyddslag*, SOU 2015:25, lämnades förslag med innebörden att MSB skulle få ansvar för tillsyn över kommuner och regioner samt för enskilda verksamhetsutövare som verkar utanför övriga tillsynsmyndigheters ansvarsområden när det gäller säkerhetsskyddsregleringen.[9] Flera remissinstanser framförde att den stödjande roll som MSB har på informationssäkerhetsområdet riskerar att försvagas om förslaget genomförs. Någon ändring i tillsynsstrukturen gjordes därför inte i den nya säkerhetsskyddslagen jämfört med 1996 års säkerhetsskyddslag. Regeringen beslutade i stället att ge en särskild utredare i uppdrag att se över hur en ändamålsenlig tillsyn ska vara utformad.[10] Den nya utredningen delade remissinstansernas uppfattning att MSB inte bör utöva tillsyn enligt säkerhetsskyddslagen.[11]

Utredningen har övervägt att tillsynsansvaret för offentlig förvaltning antingen ska ligga hos MSB eller länsstyrelsen. MSB har i dag ett flertal uppgifter enligt gällande NIS-reglering. MSB är nationell kontaktpunkt och CSIRT-enhet. Myndigheten leder också ett nationellt samarbetsforum och tar emot incidentrapporter. Myndigheten har även föreskriftsrätt på flera områden och föreslås få fler uppgifter. Det kan vidare antas att behovet av råd, stöd, utbildning och samordning kommer att öka när den nya NIS-regleringen träder

[9] SOU 2015:25 s. 492 ff.
[10] *Utkontraktering av säkerhetskänslig verksamhet, sanktioner och tillsyn – tre frågor om säkerhetsskydd*, dir. 2017:32.
[11] SOU 2018:82 s. 385.

i kraft. CSIRT-enheten får också fler uppgifter i NIS2-direktivet. CSIRT-enheten ska bland annat tillhandhålla stöd till verksamhetsutövare vid en cybersäkerhetsincident. Den ska också kunna bistå verksamhetsutövaren med att upptäcka sårbarheter i nätverks- och informationssystem. I skäl 41 framhålls vikten av att stärka förtroendeförhållandet mellan verksamhetsutövarna och CSIRT-enheterna och att det därför bör övervägas en funktionell åtskillnad mellan de operativa uppgifter som utförs av CSIRT-enheterna, särskilt när det gäller informationsutbyte och bistånd till verksamhetsutövarna, och de behöriga myndigheternas tillsynsverksamhet när en CSIRT-enhet är en del av en behörig myndighetet. Om MSB skulle bedriva tillsyn över offentlig sektor enligt direktivet skulle tillsynsverksamheten sannolikt behöva funktionellt avskiljas från övrig stödjande verksamhet och den operativa CSIRT-verksamheten. Även med en sådan funktionell åtskillnad finns det risk för att den stödjande verksamheten försvagas om myndigheten bedriver tillsyn över samma verksamhetsutövare som är i behov av råd och stöd. Utredningen anser därför att MSB:s roll även i fortsättningen bör vara stödjande och samordnande.

Prövningen av vilka uppgifter och uppdrag som länsstyrelserna ska ansvara för bör enligt regeringen ske med vägledning av de kriterier som redovisas i budgetpropositionen för 2021.[12] Ett kriterium som anges är att uppgiften omfattas av länsstyrelsens roll som statens företrädare i länen. Länsstyrelserna har enligt regeringen en viktig roll i att upprätthålla en väl fungerande offentlig förvaltning samt bidra till att skapa goda förutsättningar för att nationella mål ska få genomslag i länen. Länsstyrelserna bedriver också tillsyn inom ett flertal områden och kan därför antas ha en hög tillsynskompetens i allmänhet. Fyra länsstyrelser bedriver också tillsyn över bland annat informationssäkerhet enligt säkerhetsskyddsregleringen. Länsstyrelsen är också högsta civila totalförsvarsmyndighet inom länet och har centrala roller i det civila försvaret. De har även en etablerad relation med kommunerna när det gäller risk- och sårbarhetsanalyser. I budgetpropositionen för 2022 anger regeringen även kriterier för att koncentrera vissa verksamheter till ett färre antal länsstyrelser.[13] Detta kan bland annat ske om det finns ett behov av förstärkt likformighet i utförande och om verksamheten har hög komplexitet.

[12] Prop. 2020/21:1 utg.omr 1 avsnitt 10.5.
[13] Prop. 2021/22:1 utg.omr 1 avsnitt 9.5.

Dessa kriterier är enligt utredningen uppfyllda avseende NIS2-tillsyn. Det vore inte heller effektivt utnyttjande av resurser att samtliga länsstyrelser skulle bygga upp kompetens på området. Det är enligt utredningen i stället bättre att nyttja den kompetens och erfarenhet som finns hos de fyra länsstyrelser som bedriver tillsyn enligt säkerhetsskyddsregleringen.

Mot bakgrund av det som anförs ovan så är utredningens bedömning att tillsyn över offentlig förvaltning bör följa det system som finns enligt säkerhetsskyddsregleringen och att de länsstyrelser som bedriver tillsyn enligt den regleringen även ska vara tillsynsmyndigheter för sektorn. Dessa är länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län. I säkerhetsskyddsregleringen är Säkerhetspolisen och Försvarsmakten tillsynsmyndigheter för ett antal statliga myndigheter. Utredningen föreslår inte att de ska ha motsvarande tillsynsuppgifter enligt cybersäkerhetslagen. Flera av de myndigheter som finns inom Säkerhetspolisens och Försvarsmaktens tillsynsområde enligt säkerhetsskyddsregleringen kommer att vara undantagna från cybersäkerhetslagens tillämpningsområde. Arbetet med säkerhetsskydd hos Säkerhetspolisen och Försvarsmakten är nära kopplat till annan verksamhet som myndigheterna bedriver medan cybersäkerhetslagen har ett vidare syfte där denna koppling inte är lika tydlig. Utredningen föreslår därför att Länsstyrelsen i Stockholms län ska vara tillsynsmyndighet för kommuner och regioner som hör till Stockholms, Uppsala, Södermanlands, Västmanlands, Värmlands, Gotlands, Örebro, Dalarnas eller Gävleborgs län och statliga myndigheter som har sitt säte i något av dessa län. Länsstyrelsen i Skåne län ska vara tillsynsmyndighet för kommuner och regioner som hör till Kronobergs, Blekinge, Kalmar eller Skåne län och statliga myndigheter som har sitt säte i något av dessa län. Länsstyrelsen i Västra Götalands län ska vara tillsynsmyndighet för kommuner och regioner som hör till Hallands, Jönköpings, Västra Götalands eller Östergötlands län och statliga myndigheter som har sitt säte i något av dessa län. Länsstyrelsen i Norrbottens län ska vara tillsynsmyndighet för kommuner och regioner som hör till Västernorrlands, Jämtlands, Västerbottens eller Norrbottens län och statliga myndigheter som har sitt säte i något av dessa län.

Länsstyrelserna som utredningen föreslår kommer själva att ingå i sektorn offentlig förvaltning. Eftersom det bör undvikas att en tillsynsmyndighet utövar tillsyn över den egna organisationen så före-

slår utredningen att Länsstyrelsen i Stockholms län och Länsstyrelsen i Norrbottens län ska vara tillsynsmyndigheter för varandra och att Länsstyrelsen i Västra Götaland och Länsstyrelsen i Skåne län ska vara tillsynsmyndigheter för varandra.

Rymden

Rymden är en ny sektor i NIS2-direktivet och avser operatörer av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter och som stöder tillhandahållandet av rymdbaserade tjänster, undantagen tillhandahållare av allmänna elektroniska kommunikationsnät. Rymdbaserade tjänster har ofta dubbla användningsområden eftersom de kan användas både ur ett civilt och militärt perspektiv och kan därför ha betydelse för totalförsvaret.

Rymdbaserade tjänster avser bland annat satellitkommunikation, positionerings- och tidstjänster samt jordobservation. Sektorn anknyter därmed närmast till den befintliga sektorn digital infrastruktur där PTS är tillsynsmyndighet.

Rymdstyrelsen har bland annat till uppgift att bereda ärenden om tillstånd till rymdverksamhet samt utöva kontroll av sådan verksamhet. Myndigheten bedriver dock ingen tillsyn över säkerhet i nätverks- och informationssystem.

Även MSB bedriver arbete i sektorn, myndigheten har en funktion för rymdsäkerhet och är bland annat behörig myndighet för PRS (public regulated service) som är en tjänst för att producera positions- och tidsdata för EU:s medlemsländer.

Utredningen har övervägt att tillsynsansvaret för rymdsektorn antingen ska ligga hos MSB eller PTS. Utredningen föreslår, på grund av sektorns anknytning till digital infrastruktur och allmänna elektroniska kommunikationsnät samt det faktum att PTS är en befintlig tillsynsmyndighet i den nuvarande NIS-regleringen, att PTS ska vara tillsynsmyndighet för sektorn.

Post- och budtjänster

Post- och budtjänster är en ny sektor i NIS2-direktivet. PTS är förvaltningsmyndighet med ett samlat ansvar inom postområdet. Myndigheten är även i dag en tillsynsmyndighet enligt NIS-regleringen.

Utredningen föreslår därför att PTS ska vara tillsynsmyndighet för sektorn.

Avfallshantering

Avfallshantering är en ny sektor i NIS2-direktivet. Naturvårdsverket är förvaltningsmyndighet i frågor om avfall. Myndigheten har flera uppgifter på området vilket bland annat innefattar att utfärda föreskrifter, utföra tillsyn och ta fram tillsynsvägledning. Myndigheten bedriver ingen tillsyn av cybersäkerhet. Länsstyrelsen beslutar om tillstånd enligt miljöprövningsförordningen (2013:251) och ansvarar för tillsyn över tillståndspliktiga verksamheter om de inte överlåtit tillsynen till kommunen. Avfallshantering är en sektor som endast omfattas av reaktiv tillsyn. Eftersom tillsyn av cybersäkerhet kräver speciell kompetens vore det inte effektivt utnyttjande av resurser att Naturvårdsverket skulle bygga upp kompetens på detta område för att endast bedriva tillsyn över sektorn avfallshantering, om det finns en annan myndighet som är lämplig och redan har sådan kompetens. Utredningen föreslår därför att länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län ska vara tillsynsmyndigheter i sektorn.

Tillverkning, produktion och distribution av kemikalier

Tillverkning, produktion och distribution av kemikalier är en ny sektor i NIS2-direktivet. Ansvaret för tillsyn av kemikalier i varor, kemiska produkter och bekämpningsmedel fördelas mellan flera olika myndigheter. Kemikalieinspektionen utövar tillsyn över efterlevnaden av krav på utformningen av och innehållet i produkter. Kemikalieinspektionens tillsyn kräver särskild kompetens på det naturvetenskapliga området, bland annat har myndigheten inspektörer som är kemister, toxikologer, ekotoxikologer och agronomer. Myndigheten saknar kompetens gällande tillsyn av cybersäkerhet. För det fall Kemikalieinspektionen ska vara tillsynsmyndighet kommer det att krävas att myndigheten bygger upp en helt ny tillsynsorganisation. Tillverkning, produktion och distribution av kemikalier är en sektor som endast omfattas av reaktiv tillsyn. Utredningen anser därför att det är mest effektivt om en myndighet som även har

annat tillsynsansvar enligt cybersäkerhetsregleringen ansvarar för sektorn. Länsstyrelsen utför viss kemikalietillsyn och föreslås av utredningen som tillsynsmyndighet för flera andra sektorer. Med hänsyn till detta föreslår utredningen att länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län ska vara tillsynsmyndigheter för sektorn.

Produktion, bearbetning och distribution av livsmedel

Produktion, bearbetning och distribution av livsmedel är en ny sektor i NIS2-direktivet. Ansvaret för livsmedelskontrollen i Sverige delas mellan fler olika myndigheter. Livsmedelsverket ska leda, samordna och följa upp livsmedelskontrollen. Myndigheten är även i dag tillsynsmyndighet enligt NIS-regleringen. Utredningen föreslår därför att Livsmedelsverket ska vara tillsynsmyndighet för sektorn.

Tillverkning

Tillverkning är en ny sektor i NIS2-direktivet som innefattar sex olika delsektorer.

Den första delsektorn, tillverkning av medicintekniska produkter anknyter till sektorn hälso- och sjukvård. Läkemedelsverket är förvaltningsmyndighet för verksamhet som rör medicintekniska produkter och ansvarar för tillsyn av tillverkare av dessa produkter. IVO utövar tillsyn över hälso- och sjukvårdens användning och hantering av medicintekniska produkter. Myndigheten ansvarar också för tillsyn över de medicintekniska produkter som tillverkas inom hälso- och sjukvården, så kallad egentillverkning. Utredningen föreslår att Läkemedelsverket ska vara tillsynsmyndighet för delsektorn.

Delsektorerna tillverkning av motorfordon, släpfordon och påhängsvagnar samt tillverkning av andra transportmedel anknyter till sektorn transport där Transportstyrelsen i dag är tillsynsmyndighet. Utredningen föreslår därför att myndigheten även ska vara tillsynsmyndighet för dessa delsektorer.

Delsektorerna tillverkning av datorer, elektronikvaror och optik, tillverkning av elapparatur och tillverkning av övriga maskiner saknar tydlig koppling till någon befintlig sektor i NIS-regleringen. Tillverkning är en sektor som endast omfattas av reaktiv tillsyn. Det är ut-

redningens mening att tillsynsansvaret för dessa delsektorer bör ligga på en myndighet som redan har tillsynsansvar över någon annan sektor i regleringen. Eftersom det saknas tydlig koppling till någon sektorsmyndighet så föreslår utredningen att länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län ska vara tillsynsmyndigheter för delsektorerna. Detta följer systematiken i säkerhetsskyddsregleringen där länsstyrelsen ansvarar för tillsyn över verksamhetsutövare som inte hör till någon annan tillsynsmyndighets tillsynsområde.

Digitala leverantörer

Digitala leverantörer är en ny sektor i NIS2-direktivet som innefattar två typer av verksamhetsutövare som i NIS-direktivet benämndes leverantörer av digitala tjänster. Dessa är leverantörer av marknadsplatser online och leverantörer av sökmotorer. Leverantörer av plattformar för sociala nätverkstjänster har inte tidigare omfattats av NIS-regleringen. PTS är i dag tillsynsmyndighet för digitala tjänster. Utredningen föreslår därför att myndigheten ska vara tillsynsmyndighet för den nya sektorn.

Forskning

Forskning är en ny sektor i NIS2-direktivet och innefattar forskningsorganisationer som bedriver forskning i syfte att utnyttja resultaten i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner. Sektorn har ingen tydlig koppling till någon befintlig sektor eller tillsynsmyndighet i den nuvarande NIS-regleringen. Utredningen föreslår därför att länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län ska vara tillsynsmyndigheter i sektorn.

Lärosäten med examenstillstånd

Utredningen föreslår i avsnitt 5.2.14 att lärosäten med examenstillstånd ska omfattas av cybersäkerhetslagen. Ett flertal av dessa är även statliga myndigheter och ingår därmed i sektorn offentlig förvaltning där utredningen föreslår fyra länsstyrelser som tillsynsmyn-

digheter. Dessa länsstyrelser föreslås även som tillsynsmyndigheter för sektorn forskning. Utredningen föreslår därför att länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län ska vara tillsynsmyndigheter för lärosäten med examenstillstånd.

8.4.3 Tillsynsmyndighetens uppdrag

Utredningens förslag: Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som meddelats i anslutning till lagen följs.

Enligt artikel 31.1 ska medlemsstaterna säkerställa att deras behöriga myndigheter övervakar och vidtar de åtgärder som krävs för att säkerställa att direktivet efterlevs. En bestämmelse om att tillsynsmyndigheten ska utöva tillsyn över att den nya lagen och föreskrifter som har meddelats i anslutning till lagen följs bör därför införas. Det innebär att tillsynsmyndigheten ska utöva tillsyn över att verksamhetsutövare uppfyller kraven på riskhanteringsåtgärder, incidentrapportering och anmälan.

Enligt artikel 31.2 får medlemsstaterna tillåta sina behöriga myndigheter att prioritera tillsyn baserad på en riskbaserad metod. Mer specifikt kan sådana metoder omfatta kriterier eller riktmärken för klassificering av väsentliga entiteter i riskkategorier och motsvarande tillsynsåtgärder och tillsynsmedel som rekommenderas per riskkategori, såsom användning av frekvens för eller typ av inspektion på plats, riktade säkerhetsrevisioner eller säkerhetsskanningar, vilken typ av information som ska begäras och detaljnivån på denna information (skäl 124).

Att tillsynsmyndigheterna har möjlighet att planera sin verksamhet och prioritera vilka tillsynsinsatser som ska göras behöver enligt utredningens mening inte anges särskilt i regleringen.

8.4.4 Tillsyn över viktiga verksamhetsutövare

Utredningens förslag: Tillsynsåtgärder för viktiga verksamhetsutövare får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att cybersäkerhetslagen eller de föreskrifter som har meddelats i anslutning till lagen inte följs.

NIS2-direktivet innehåller en differentiering av tillsynssystemet mellan väsentliga och viktiga verksamhetsutövare i syfte att säkerställa en rättvis balans vad gäller skyldigheterna för dessa verksamhetsutövare och de behöriga myndigheterna. Väsentliga verksamhetsutövare bör därför enligt direktivet omfattas av ett heltäckande tillsynssystem med förhandstillsyn och efterhandstillsyn, medan viktiga verksamhetsutövare bör omfattas av enklare tillsyn, endast i efterhand (skäl 122). När medlemsstaterna får bevis, indikationer på eller information om att en viktig verksamhetsutövare påstås underlåta att fullgöra sina skyldigheter enligt direktivet ska de säkerställa att de behöriga myndigheterna vid behov vidtar åtgärder i form av tillsynsåtgärder i efterhand (artikel 33).

En motsvarande differentiering mellan samhällsviktiga och digitala tjänster finns i nuvarande 22 § NIS-lagen där det framgår att digitala tjänster endast står under reaktiv tillsyn.

Det bör därför tas in en bestämmelse i den nya lagen om att tillsynsåtgärder när det gäller viktiga verksamhetsutövare får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att en sådan verksamhetsutövare inte följer cybersäkerhetslagen eller de föreskrifter som har meddelats i anslutning till lagen.

8.4.5 Föreskrifter

Utredningens bedömning: Tillsynsmyndigheten får inom sitt tillsynsområde meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning enligt 3 kap. 1–3 §§ lagen om cybersäkerhet. Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig.

För sektorn offentlig förvaltning och lärosäten med examenstillstånd får Myndigheten för samhällsskydd och beredskap meddela föreskrifter om riskhanteringsåtgärder, systematiskt riskbase-

rat informationssäkerhetsarbete samt utbildning enligt 3 kap. 1–3 §§ lagen om cybersäkerhet.

Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om vad som utgör en betydande incident och om incidentrapportering enligt 3 kap. 5–7 §§ lagen om cybersäkerhet. Tillsynsmyndigheterna ska ges tillfälle att yttra sig.

Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om vilka verksamhetsutövare som omfattas av 1 kap. 8 § lagen om cybersäkerhet och om dessa verksamheter är väsentliga. Tillsynsmyndigheterna ska ges tillfälle att yttra sig.

Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om verksamhetsutövarnas anmälningsskyldighet enligt 2 kap. 2 § lagen om cybersäkerhet.

Utredningen föreslår att regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter i anslutning till flera bestämmelser i cybersäkerhetslagen. Nedan lämnar utredningen förslag på vilken myndighet som ska bemyndigas att meddela dessa föreskrifter.

Föreskrifter om riskhanteringsåtgärder

Som framgår av kapitel 7 föreslår utredningen att närmare krav på verksamhetsutövarnas riskhanteringsåtgärder får anges i föreskrifter. Rätten att meddela föreskrifter om säkerhetsåtgärder enligt den nuvarande regleringen är uppdelad mellan MSB och tillsynsmyndigheterna samt Socialstyrelsen. I betänkandet av utredningen som utredde införandet av NIS-direktivet anfördes att MSB redan utfärdat föreskrifter om systematiskt informationssäkerhetsarbete för statliga myndigheter och att myndigheten därför även skulle utfärda generella föreskrifter om hur ett systematiskt informationssäkerhetsarbete för samtliga sektorer kan bedrivas.[14] När det gäller föreskrifter om säkerhetsåtgärder bedömde utredningen dock att den myndighet med kunskap om verksamheten, det vill säga tillsynsmyndigheten skulle ha ansvaret för att utfärda föreskrifter.

Som framgått ovan har det tagit relativt lång tid för tillsynsmyndigheterna att besluta om föreskrifter om säkerhetsåtgärder och för sektorn Hälso- och sjukvård finns i dag inga föreskrifter. Till-

[14] SOU 2017:36 s. 133.

synsmyndigheternas föreskrifter skiljer sig också åt vad gäller både terminologi och innehåll trots att de utgår från samma grund. Det har också framförts att det funnits brister i samordningen av tillsynsmyndigheternas arbete med föreskrifter.

Utredningen har med anledning av detta övervägt om ansvaret för att ge ut föreskrifter bör flyttas från tillsynsmyndigheterna till MSB. Detta skulle innebära att det beslutas om en gemensam föreskrift som gäller för samtliga sektorer vilket skulle ge en enhetlig reglering och underlätta för verksamhetsutövare som bedriver verksamhet i flera sektorer.

MSB, Säkerhetspolisen, Transportstyrelsen och IMY har framfört till utredningen att det bör finnas en gemensam föreskrift med grundkrav som gäller för samtliga sektorer i syfte att konkretisera de riskhanteringsåtgärder som anges i cybersäkerhetslagen. Enligt myndigheterna är det ingen större skillnad på grundkraven som kan ställas rörande nätverks- och informationssystem oavsett sektor. Dessa grundkrav skulle i en sådan lösning kunna kompletteras av tillsynsmyndigheterna som också skulle ha föreskriftsrätt för respektive tillsynsområde. Detta skulle kunna utformas på motsvarande sätt som i säkerhetsskyddsregleringen där Säkerhetspolisen och Försvarsmakten får meddela föreskrifter om bland annat säkerhetsskyddsåtgärder och övriga tillsynsmyndigheter får meddela kompletterande föreskrifter inom sitt tillsynsområde.

PTS har framfört att det finns inarbetad praxis med föreskrifter för till exempel tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga kommunikationstjänster och att myndigheten även fortsättningsvis bör ha föreskriftsrätt för dessa verksamhetsutövare. I skäl 95 i NIS2-direktivet framhålls också vikten av att upprätthålla nuvarande praxis när det gäller elektronisk kommunikation. TechSverige har påpekat att sektorn precis genomgått en anpassning av LEK och att det skulle leda till onödigt stor belastning och omställningskostnader om dessa krav ändrades igen.

NIS2-direktivet är mer detaljerat än det första NIS-direktivet när det gäller vilka tekniska, driftsrelaterade och organisatoriska åtgärder som medlemsstaterna ska säkerställa att verksamhetsutövarna vidtar, se kapitel 7. Dessa åtgärder utgör krav som ska säkerställa en grundnivå på säkerhetsarbetet oberoende av sektor. Detta talar en-

ligt utredningen för att behovet av centrala myndighetsföreskrifter inte är lika stort avseende NIS2-direktivet som för NIS-direktivet.

Det finns också sektorer där det finns ett behov av sektorsspecifika krav på grund av sektorns speciella förutsättningar. NIS2-direktivet innehåller vidare större möjligheter för kommissionen att besluta om genomförandeakter som tar hänsyn till detta. När det gäller leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer, plattformar för sociala nätverkstjänster samt kvalificerade tillhandahållare av betrodda tjänster ska kommissionen enligt artikel 21.5 senast den 17 oktober 2024 anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna för de tekniska, driftsrelaterade och organisatoriska åtgärderna som anges i artikel 21.2 i direktivet. Kommissionen får även anta genomförandeakter för att fastställa tekniska och metodologiska krav samt, vid behov, sektorskrav avseende andra väsentliga och viktiga verksamhetsutövare.

När kommissionen antagit genomförandeakter kommer det alltså att finnas skillnader i de krav som ställs på olika verksamhetsutövare redan på EU-nivå. Även med en gemensam föreskrift skulle det finnas ett behov av sektorsspecifika regleringar. Dessa sektorsspecifika regleringar skulle då kunna stå i strid med den sektorsgemensamma föreskriften. Den möjlighet som finns för tillsynsmyndigheterna i 8 kap. 10 § säkerhetsskyddsförordningen att besluta om kompletterande föreskrifter har tolkats som en möjlighet att utfärda verkställighetsföreskrifter. Utredningen bedömer att verkställighetsföreskrifter inte skulle vara tillräckligt för de föreskrifter om riskhanteringsåtgärder som kan behöva utfärdas av tillsynsmyndigheterna. Detta eftersom verkställighetsföreskrifter i första hand ska vara av administrativ karaktär för tillämpningen av en lag. Det finns dock ett visst utrymme att meddela verkställighetsföreskrifter som i materiellt hänseende ”fyller ut” en lag utan att tillföra den något väsentligt nytt.[15] Utredningen menar att detta utrymme inte är tillräckligt för att en myndighet skulle skärpa eller göra undantag för ett krav i en sektorsövergripande föreskrift. Det skulle i stället innebära att en tillsynsmyndighet kan komma att utfärda föreskrifter

[15] Ds 1998:43 s. 47 ff.

som innebär att det uppstår en regelkonflikt med en sektorsövergripande föreskrift. Verksamhetsutövare som ska tillämpa båda föreskrifterna skulle därmed kunna träffas av motstridiga krav i de olika föreskrifterna. Detta skulle inte uppfylla kraven på förutsebarhet och klarhet vid normgivning och utredningen bedömer därför att en sådan lösning inte är en framkomlig väg.

Det är tillsynsmyndigheterna som har kunskap om eventuella sektorsspecifika förutsättningar som behöver beaktas i föreskrifter om riskhanteringsåtgärder. Utredningen ser också en fördel med att så långt möjligt hålla samman normgivning och tillsyn. Även om det finns fördelar med att centralisera föreskriftsrätten till en myndighet så är det utredningens sammantagna bedömning att det inte vore ändamålsenligt att centralisera föreskriftsrätten från tillsynsmyndigheterna till MSB. När det gäller rätten att meddela föreskrifter om systematiskt informationssäkerhetsarbete så anser utredningen att denna bör hållas ihop med rätten att meddela föreskrifter om riskhanteringsåtgärder. Det finns annars en risk för att det uppstår oklarheter om vilken myndighet som har föreskriftsrätt rörande en viss åtgärd. Utredningen föreslår därför att det ska vara tillsynsmyndigheterna som får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning om riskhanteringsåtgärder inom sitt tillsynsområde. Innan en tillsynsmyndighet meddelar sådana föreskrifter ska MSB ges tillfälle att yttra sig. Som framgår av avsnitt 7.1 anser utredningen också att MSB skyndsamt bör utarbeta en vägledning till stöd för tillsynsmyndigheternas föreskriftsarbete.

När det gäller hälso- och sjukvårdssektorn så föreslår utredningen att det till skillnad mot i dag ska vara IVO i egenskap av tillsynsmyndighet, och inte Socialstyrelsen, som får utfärda föreskrifter.

När det gäller sektorn offentlig förvaltning så föreslår utredningen att fyra länsstyrelser ska utöva tillsyn över sektorn. Utredningen ser dock ingen anledning till att det ska utfärdas fyra föreskrifter i sektorn varför föreskriftsrätten bör ligga på en myndighet.

MSB har beslutat om föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter och föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter i enlighet med förordningen (2022:524) om statliga myndigheters beredskap. Dessa föreskrifter anger en grundnivå som statliga myndigheter minst bör uppnå i sitt informationssäkerhetsarbete. MSB

har också tagit fram ett verktyg, *infosäkkollen*[16], som stödjer uppföljning och förbättring av systematiskt informations- och cybersäkerhetsarbete i den offentliga förvaltningen. Verktyget utgår från MSB:s föreskrifter och stödmaterial. MSB har därmed den kunskap som krävs och tillgång till information som kan nyttjas för att besluta om föreskrifter för sektorn. Utredningen bedömer därför att det bör vara MSB som får besluta om föreskrifter gällande offentlig förvaltning även om myndigheten inte är tillsynsmyndighet för sektorn.

Utredningen föreslår i avsnitt 5.2.14 att lärosäten med examenstillstånd ska omfattas av cybersäkerhetslagen. Flertalet av dessa är även statliga myndigheter och ingår därmed även i sektorn offentlig förvaltning. Utredningen anser därför att det bör vara samma myndighet som utfärdar föreskrifter för sektorn offentlig förvaltning och lärosäten med examenstillstånd.

Föreskrifter om incidentrapportering

Som framgår av avsnitt 7.3 föreslår utredningen att närmare krav om rapportering av incidenter ska anges i föreskrifter. MSB har enligt den nuvarande regleringen beslutat om föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster; MSBFS 2018:9. MSB är också den myndighet i Sverige som i egenskap av CSIRT-enhet tar emot incidentrapporter. Utredningen föreslår därför att MSB även enligt den nya lagen ska meddela föreskrifter om incidentrapportering och vad som utgör en betydande incident. Innan föreskrifterna meddelas ska MSB ge tillsynsmyndigheterna tillfälle att yttra sig.

Föreskrifter om verksamhetsutövare som inte uppfyller storlekskravet

Som framgår av avsnitt 5.2.13 föreslår utredningen en systematik med innebörd att det av lagen följer övergripande kriterier för vilka mindre verksamheter som ska omfattas trots att de inte uppfyller storlekskravet och att det i föreskrifter anges vilka verksamheter som uppfyller något kriterium.

[16] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/infosakkollen/.

MSB ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. Myndigheten ska även rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder på olika nivåer och områden i samhället. [17] MSB har också en central roll i arbetet med risk- och sårbarhetsanalyser i förordningen (2022:524) om statliga myndigheters beredskap. Myndigheten har också fått en rad uppdrag i regleringsbrev att redovisa en nationell bedömning av samhällets förmågor, risker, sårbarheter samt identifierade och genomförda åtgärder avseende krisberedskapen. Myndigheten kan därför antas ha den kunskap som behövs för att bedöma vilka verksamheter som ska omfattas av regleringen oavsett storlek. Utredningen föreslår därför att MSB ska vara den myndighet som får besluta om dessa föreskrifter. Innan föreskrifterna meddelas ska MSB ge tillsynsmyndigheterna tillfälle att yttra sig.

Föreskrifter om anmälningsskyldighet

Som framgår av avsnitt 6.2 föreslår utredningen att varje tillsynsmyndighet, inom sitt tillsynsområde, ska upprätta ett register över väsentliga och viktiga verksamhetsutövare. Som grund till registret ska alla verksamhetsutövare som omfattas av lagen lämna anmälan med uppgift om identitet, kontaktuppgifter, IP-adressintervall, verksamhet och uppgift om i vilka medlemsländer verksamhet bedrivs till tillsynsmyndigheten. Det register som tillsynsmyndigheterna upprättat ska vidarebefordras till den gemensamma kontaktpunkten som i sin tur sedan ska vidareförmedla information till kommissionen och samarbetsgruppen. Utredningen föreslår också att regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om verksamhetsutövarnas anmälningsskyldighet. Slutmottagare av uppgifterna är alltså MSB i Sverige. Med hänsyn härtill och att de uppgifter som ska lämnas är desamma oberoende av vilket tillsynsområde verksamhetsutövaren tillhör så bör samlade föreskrifter om uppgiftsskyldigheten beslutas av en central myndighet. Utredningen föreslår därför att MSB ska vara den myndighet som meddelar dessa föreskrifter.

[17] 11 a § första och tredje stycket förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

8.4.6 Tillsynsmyndighetens undersökningsbefogenheter

I detta avsnitt behandlas de befogenheter som tillsynsmyndigheten ska ha för att kunna utöva tillsyn. Tillsynsmyndighetens befogenheter att besluta om ingripanden och sanktioner behandlas i kapitel 9.

Tillgång till information och lokaler

Utredningens förslag: Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen.

Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamheten.

Tillsynsmyndigheten får förelägga den som står under tillsyn att tillhandahålla information och ge tillträde.

Ett sådant föreläggande får förenas med vite.

Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Utredningens bedömning: När en tillsynsmyndighet begär information ska tillsynsmyndigheten ange syftet med begäran och precisera vilken information som krävs.

För att kunna utöva en effektiv tillsyn krävs att tillsynsmyndigheten får tillgång till den information som behövs samt vid behov tillträde till lokal eller liknande.

Enligt artikel 32.2 och 33.2 i NIS2-direktivet ska tillsynsmyndigheterna ha befogenhet att underställa verksamhetsutövare

a) begäranden om sådan information som behövs för att bedöma de riskhanteringsåtgärder för cybersäkerhet som antagits av den berörda verksamhetsutövaren, inbegripet dokumenterade cybersäkerhetsstrategier, samt fullgörandet av skyldigheten att lämna information till de behöriga myndigheterna avseende det register som ska upprättas i enlighet med artikel 27,

b) begäranden om tillgång till uppgifter, handlingar och information som behövs för att myndigheterna ska kunna utföra sina tillsynsuppgifter,

c) begäranden om bevis på genomförandet av cybersäkerhetsstrategier, till exempel resultaten av säkerhetsrevisioner som utförts av en kvalificerad revisor och respektive underliggande bevis.

Artiklarna innebär enligt utredningens uppfattning att verksamhetsutövarna, på begäran av tillsynsmyndigheten, ska tillhandahålla den information och de handlingar som behövs för tillsynen. En bestämmelse med denna innebörd ska därför tas in i den nya lagen. De exempel på sådan information som anges i a och c ovan behöver enligt utredningens mening inte anges särskilt i lagen. Möjligheten för tillsynsmyndigheten att kräva in denna information täcks av att myndigheten har möjlighet att begära in den information som behövs för tillsynen.

Enligt artikel 32.3 och 33.3 ska tillsynsmyndigheterna när de begär information ange syftet med begäran och specificera den begärda informationen. Motsvarande bestämmelse finns i dag i 20 § NIS-förordningen. Utredningen föreslår att en motsvarande bestämmelse anges i den nya förordningen.

Enligt artikel 32.2 a och 33.2 a ska tillsynsmyndigheterna ha befogenhet att utföra tillsyn både på plats och på distans, det vill säga bedriva såväl platstillsyn som så kallad skrivbordstillsyn. För att kunna utöva en effektiv tillsyn kan tillsynsmyndigheten behöva tillträde till lokaler eller liknande. Exempelvis kan tillsynsmyndigheten behöva tillträde för att kontrollera att en verksamhetsutövare har vidtagit erforderliga säkerhetsåtgärder.

Utredningen anser därför att tillsynsmyndigheten i den utsträckning det behövs för tillsynen, ska ha rätt att få tillträde till områden, lokaler och andra utrymmen där verksamhet som omfattas av lagen bedrivs. Tillträdesrätten bör dock av integritetsskäl inte omfatta bostäder. Detta bör följa av lagen.

Om en verksamhetsutövare inte samarbetar med tillsynsmyndigheten vid tillsynen bör tillsynsmyndigheten kunna meddela de förelägganden som behövs för att förmå verksamhetsutövaren att tillhandahålla den information och ge det tillträde som behövs för tillsynen. Ett beslut om föreläggande bör kunna förenas med vite.

Allmänna bestämmelser om viten finns i lagen (1985:206) om viten, viteslagen. Där anges bland annat hur ett vitesföreläggande ska vara utformat i olika avseenden. Det framgår också att ett vitesföreläggande ska delges adressaten.

När det gäller vitesbeloppet framgår av viteslagen till exempel att detta ska fastställas till ett belopp som med hänsyn till vad som är känt om adressatens ekonomiska förhållanden och till omständigheterna i övrigt kan antas förmå honom att följa det föreläggande som är förenat med vitet (3 § viteslagen). Med omständigheterna i övrigt avses bland annat kostnaderna för föreläggandets fullgörande och omfattningen av de åtgärder som krävs. Beloppet bör vidare bestämmas med hänsyn till hur angeläget det är att föreläggandet följs. Om föreläggandet avser att tillgodose ett betydelsefullt samhällsintresse, kan ett högre belopp vara motiverat. Myndigheterna kan emellertid inom ramen för 3 § viteslagen bestämma hur högt eller lågt belopp som helst. Vitet ska som huvudregel fastställas till ett bestämt belopp. Om det är lämpligt med hänsyn till omständigheterna, får vite dock enligt 4 § viteslagen föreläggas som löpande vite. Vitet bestäms då till ett visst belopp för varje tidsperiod av viss längd under vilken föreläggandet inte har följts eller, om föreläggandet avser en återkommande förpliktelse, för varje gång adressaten underlåter att fullgöra denna. Om ett föreläggande inte följs, kan myndigheten behöva upprepa föreläggandet. Det kan i dessa fall vara lämpligt att höja vitesbeloppet.

Frågor om utdömande av viten prövas enligt 6 § viteslagen av förvaltningsrätt på ansökan av den myndighet som har utfärdat vitesföreläggandet

Enligt utredningens mening finns det inte anledning att införa bestämmelser som avviker från viteslagen.

Om en verksamhetsutövare ändå vägrar att ge tillsynsmyndigheten information eller tillträde till en lokal kan tvångsåtgärder behöva användas. För att tillsynsmyndigheten i en sådan situation ska kunna genomföra sin tillsyn bör myndigheten kunna begära handräckning av Kronofogdemyndigheten.

Säkerhetsrevisioner

Utredningens förslag: Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten.

En riktad säkerhetsrevision ska baseras på riskbedömningar som utförs av tillsynsmyndigheten, verksamhetsutövaren eller på annan tillgänglig riskrelaterad information.

Tillsynsmyndigheten får även anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare.

Regeringen får meddela föreskrifter om säkerhetsrevisioner.

Tillsynsmyndigheten ska enligt artikel 32.2 b–c och 33.2 b i direktivet ha befogenhet att underställa väsentliga verksamhetsutövare regelbundna och riktade säkerhetsrevisioner. Dessa revisioner kan utföras av ett oberoende organ eller en behörig myndighet. Tillsynsmyndigheten ska också ha befogenhet att göra ad hoc-revisioner vilket bland annat kan motiveras på grund av att verksamhetsutövaren haft en betydande incident.

När det gäller viktiga verksamhetsutövare ska tillsynsmyndigheten endast ha befogenhet att göra riktade säkerhetsrevisioner. De riktade säkerhetsrevisionerna ska baseras på riskbedömningar som utförs av tillsynsmyndigheten, den granskade verksamhetsutövaren eller på annan tillgänglig riskrelaterad information. Resultaten av alla riktade säkerhetsrevisioner ska göras tillgängliga för tillsynsmyndigheten.

Kostnaderna för riktade säkerhetsrevisioner som utförs av ett oberoende organ ska betalas av den granskade verksamhetsutövaren, utom i vederbörligen motiverade fall när tillsynsmyndigheten beslutar något annat.

Det engelska begreppet ”security audit” har i NIS2-direktivet översatts till säkerhetsrevision. Begreppet finns också i artikel 41.2 b i Europaparlamentet och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation. I översättningen av det direktivet används i stället begreppet säkerhetsgranskning i den svenska översättningen. Säker-

hetsgransking är också det begrepp som används i lagen (2022:482) om elektronisk kommunikation (LEK).

Enligt 8 kap. 2 § LEK får tillsynsmyndigheten om det finns särskilda skäl, ålägga den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst att på egen bekostnad låta ett oberoende kvalificerat organ utföra en säkerhetsgranskning av hela eller delar av verksamheten och att redovisa resultatet av granskningen för myndigheten.

NIS2-direktivet gör skillnad på regelbundna, riktade och ad hoc-säkerhetsrevisioner. När det gäller ad hoc-revisioner så anges i direktivet att dessa kan motiveras av en betydande incident eller en verksamhetsutövares överträdelse av direktivet. I övrigt saknas definitioner av de olika typerna av revisioner i direktivet. Utredningen tolkar det som att ad hoc-revision avser en typ av granskning som är oplanerad och händelsestyrd som kan motiveras av till exempel en incident eller en förändrad hotbild. En regelbunden säkerhetsrevision är i stället planerad och återkommande. Riktade säkerhetsrevisioner fokuserar på något specifikt område eller omständighet hos verksamhetsutövaren. Det kan till exempel vara någon specifik säkerhetsåtgärd eller något specifikt krav i regleringen.

Att tillsynsmyndigheten har möjlighet att utföra säkerhetsrevisioner får anses ingå i uppgiften att bedriva tillsyn och möjligheten att begära in uppgifter och handlingar som behövs för tillsynen samt att få tillgång till områden, lokaler och andra utrymmen som används i verksamhet som omfattas av lagen. Det behövs därför ingen särskild reglering av tillsynsmyndigheternas möjligheter att genomföra säkerhetsrevisioner i cybersäkerhetslagen.

När det gäller riktade säkerhetsrevisioner så ska tillsynsmyndigheten dock kunna besluta att dessa ska utföras av ett oberoende organ och att de ska betalas av den granskade verksamhetsutövaren. Denna möjlighet ska enligt direktivet finnas både vad gäller viktiga och väsentliga verksamhetsutövare.

Vid införandet av motsvarande bestämmelse i LEK framförde regeringen att en säkerhetsgranskning kan vara arbetskrävande och kostsam för den verksamhetsutövare som är skyldig att genomgå den. En sådan granskning bör därför i första hand komma i fråga om tillsynsmyndigheten tagit del av uppgifter eller bedrivit tillsyn där det framkommit att ytterligare granskning behövs. Möjligheten att kräva utförande av säkerhetsgranskningar kan enligt regeringen inte

heller vara att befria tillsynsmyndigheten från dess uppgift att upprätthålla en egen grundläggande kompetens och förmåga att granska säkerheten i verksamheter. Regeringen bedömde därför att skyldigheten endast ska få åläggas om det finns särskilda skäl.[18] Utredningen delar denna bedömning och det bör därför anges i lagen att tillsynsmyndigheten får besluta om en riktad säkerhetsrevision utförd av ett oberoende organ, och som bekostas av verksamhetsutövaren, om det finns särskilda skäl.

Med oberoende organ avses exempelvis ett företag som genomför säkerhetsrevisioner. Organet ska vara oberoende i förhållande till tillsynsmyndigheten och den verksamhetsutövare vars verksamhet ska granskas. Organet ska ha den sakkunskap som krävs för säkerhetsrevisionen. Det är upp till tillsynsmyndigheten att bedöma om lämpliga organ som ska utföra säkerhetsrevisionen bör pekas ut i samband med åläggandet eller om det kan överlåtas till verksamhetsutövaren.

Enligt direktivet ska en riktad säkerhetsrevision baseras på riskbedömningar som utförs av tillsynsmyndigheten, den granskade verksamhetsutövaren eller på annan tillgänglig riskrelaterad information. Detta bör framgå av förordning.

När det gäller väsentliga verksamhetsutövare ska tillsynsmyndigheten enligt direktivet även kunna besluta om regelbundna säkerhetsrevisioner som utförs av ett oberoende organ. Kostnaderna för dessa granskningar ska dock inte bekostas av den granskade verksamhetsutövaren. Bestämmelsen reglerar alltså endast möjligheten för tillsynsmyndigheten att använda sig av oberoende organ vid denna typ av revisioner. En bestämmelse som anger att tillsynsmyndigheten får anlita ett oberoende organ att utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare bör därför tas in i lagen.

[18] Prop. 2021/22:136 s. 318.

Säkerhetsskanningar

Utredningens förslag: Tillsynsmyndigheten får låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av cybersäkerhetslagen.

En säkerhetsskanning ska ske i samarbete med verksamhetsutövaren.

Tillsynsmyndigheten ska enligt artikel 32.2 d och 33.2 c i direktivet ha befogenhet att underställa verksamhetsutövare säkerhetsskanningar på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier, vid behov i samarbete med den berörda verksamhetsutövaren.

NIS2-direktivet innehåller ingen definition av vad som avses med en säkerhetsskanning. Utredningen bedömer att vad som avses är en typ av sårbarhetsskanning som kan göras på verksamhetsutövarens nätverks- och informationssystem i syfte att upptäcka sårbarheter eller osäkert konfigurerade delar av systemet. Sårbarhetsskanningar sker normalt med automatiserade verktyg som identifierar och klassificerar sårbarheter i datorer, nätverk och applikationer genom att matcha dem mot redan kända systembrister. Detta kan antingen göras på allmänt tillgängliga nätverks- och informationssystem eller med olika nivåer av åtkomst till systemen. Utredningen bedömer inte att begreppet säkerhetsskanning innefattar en typ av sårbarhetsbedömning där nätverks- och informationssystemet aktivt angrips i syfte att hitta sårbarheter, ett så kallat penetrationstest. En säkerhetsskanning får inte ha någon negativ inverkan på hur verksamhetsutövarnas nätverks- och informationssystem fungerar och behöver ske i samarbete med den berörda verksamhetsutövaren.

Att tillsynsmyndigheten när de fattar beslut om säkerhetsskanningar ska göra detta på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier får anses följa av förvaltningslagens krav på legalitet, objektivitet, proportionalitet och myndigheters skyldighet att motivera beslut. Någon särskild reglering om att tillsynsmyndigheten ska ta hänsyn till dessa kriterier är därför inte nödvändig.

8.4.7 Samordning och informationsutbyte

Samarbetsforum

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap ska leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

MSB leder i dag ett samarbetsforum där tillsynsmyndigheterna och Socialstyrelsen ingår. Detta har som framgår av avsnitt 8.3.2 haft flera positiva effekter för tillämpningen av den nuvarande NIS-regleringen. Implementeringen av NIS2-direktivet kommer att innebära att det tillkommer både fler sektorer och tillsynsmyndigheter. Antalet verksamhetsutövare som kommer att bedriva verksamhet i flera olika sektorer kommer därmed att öka. Dessa verksamhetsutövare kommer som en följd av detta att stå under tillsyn av flera olika myndigheter. Det är därmed sannolikt att behovet av samordning och informationsutbyte mellan myndigheterna kommer att öka. Utredningen föreslår därför att det även fortsättningsvis anges i förordning att MSB ska leda ett samarbetsforum där tillsynsmyndigheterna ingår. Utredningen föreslår ovan att möjligheten att meddela föreskrifter i Hälso- och sjukvårdssektorn flyttas från Socialstyrelsen till IVO, Socialstyrelsen behöver därför inte längre ingå i samarbetsforumet.

Tillsynsvägledning

MSB, Livsmedelsverket och Transportstyrelsen har framfört till utredningen att det finns ett behov av ökade möjligheter för MSB att vägleda tillsynsmyndigheterna och följa upp arbetet med tillsyn. Liknande synpunkter framfördes också i den utvärdering som MSB låtit göra angående implementeringen av NIS-direktivet.[19]

Tillsynsvägledning används bland annat inom miljöområdet och enligt 26 kap. 1 a § i miljöbalken (1998:808) avses med begreppet att utvärdera, följa upp och samordna tillsynen samt att ge råd och stöd till tillsynsmyndigheterna. Enligt miljötillsynsförordningen (2011:13)

[19] *Utvärdering av resultatet av Sveriges implementering av NIS-direktivet*, Myndigheten för samhällsskydd och beredskap, slutrapport 2022-12-20.

har ett flertal myndigheter ansvar för tillsynsvägledning inom sina expertområden. Till exempel ska Affärsverket svenska kraftnät ge tillsynsvägledning i frågor om dammsäkerhet enligt 11 kap. miljöbalken. Naturvårdsverket ska också ge allmän tillsynsvägledning i frågor som avser tillämpningen av 26 (tillsyn) och 30 (sanktioner) kap. miljöbalken. Enligt förarbetena till miljöbalken syftar tillsynsvägledningen till att bidra till att tillsynen bedrivs ändamålsenligt med avseende på såväl lokala som regionala och nationella förhållanden.[20]

De myndigheter som ansvarar för tillsynsvägledning på miljöområdet bedriver själva tillsyn inom sitt expertområde. Utredningens bedömning är att de tillsynsmyndigheter som utredningen föreslår är de som närmast motsvarar dessa myndigheter med tillsynsvägledningsansvar. Det är tillsynsmyndigheterna som har kunskap om det tillsynsområde som de ansvarar för. Utredningen lämnar därför inget förslag om att en central myndighet, MSB, skulle vara tillsynsvägledande myndighet för samtliga sektorer.

Den samordning som behövs för en effektiv och likvärdig tillsyn bedöms kunna bedrivas inom ramen för det samarbetsforum som MSB ansvarar för. Detta förutsätter dock de deltagande myndigheternas engagemang och att de ställer personalresurser till förfogande i de olika frågor som identifieras inom ramen för samarbetsforumet.

När det gäller uppföljning av tillsynsmyndighetens uppdrag anser utredningen att den bör ligga hos regeringen. Som framgått ovan så har det tagit relativt lång tid för flera myndigheter att komma igång med tillsynsverksamhet enligt regleringen. Utredningens bedömning är att det efter den nya lagens ikraftträdande bör ges tydliga återrapporteringskrav i samtliga tillsynsmyndigheters regleringsbrev för att ge förutsättningar för uppföljning och effektiv styrning.

MSB har framfört till utredningen att myndigheten bör få ett tydligare mandat att inrikta och stärka tillsynen genom att myndigheten görs till samordningsmyndighet på motsvarande sätt som Säkerhetspolisen och Försvarsmakten är detta i säkerhetsskyddsregleringen. Enligt 2 § säkerhetsskyddsförordningen ska Säkerhetspolisen och Försvarsmakten i samverkan följa upp, utvärdera och utveckla arbetet med tillsyn, i samråd ta fram och tillhandahålla metodstöd för tillsyn, förmedla relevant hotinformation till tillsynsmyndigheterna och leda ett samarbetsforum.

[20] Prop. 1997/98:45, del 1, s. 496.

Säkerhetspolisen och Försvarsmakten är de två huvudansvariga tillsynsmyndigheterna enligt säkerhetsskyddsregleringen och har möjlighet att ta över tillsynsansvaret för en verksamhetsutövare som hör till någon annan tillsynsmyndighets tillsynsområde. I ett sådant system är det enligt utredningen naturligt att dessa myndigheter har i uppdrag att följa upp, utvärdera och utveckla arbetet med tillsyn. Utredningen anser inte motsvarande gäller för den reglering som utredningen föreslår där MSB inte är tillsynsmyndighet.

Verksamhetsutövare som står under tillsyn av flera myndigheter

Utredningens bedömning: Om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive tillsynsmyndighet inte utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde.

I de fall en verksamhetsutövare bedriver verksamhet inom flera sektorer kan det uppstå en situation där flera myndigheter är behöriga att bedriva tillsyn över samma verksamhetsutövare. Eftersom hela verksamheten omfattas (se avsnitt 5.2.2) så innebär det att flera tillsynsmyndigheter kan komma att tillsyna samma delar av verksamheten. Detta riskerar att bli kostnadsdrivande för verksamhetsutövarna och medför en risk för oförenliga krav och sanktioner. Situationen kommer sannolikt främst uppstå när det gäller kommuner som kan bedriva verksamhet inom flera sektorer som träffas av regleringen. I många fall bedriver dock kommuner sådan verksamhet i ett kommunalt bolag. Att en verksamhetsutövare står under tillsyn av flera myndigheter bör enligt utredningen i möjligaste mån undvikas. Det bör därför införas en bestämmelse i förordningen som anger att om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive tillsynsmyndighet inte utöva tillsyn gällande den verksamhet som ingår i den sektor eller delsektor som en annan myndighet är tillsynsmyndighet för.

Det får förutsättas att tillsynsmyndigheterna samarbetar vid genomförande av tillsyn rörande verksamhetsutövare som bedriver verksamhet i flera sektorer. Detta följer av förvaltningslagen och myndighetsförordningen och behöver inte anges särskilt i regleringen.

Övrigt nationellt samarbete

Utredningens bedömning: Tillsynsmyndigheten ska samarbeta med Integritetsskyddsmyndigheten vid hantering av incidenter som även utgör personuppgiftsincidenter.

Om tillsynsmyndigheten, när den bedriver tillsyn enligt cybersäkerhetslagen, får kännedom om en omständighet som kan innebära en personuppgiftsincident som ska anmälas enligt dataskyddsförordningen ska tillsynsmyndigheten utan onödigt dröjsmål informera Integritetsmyndigheten.

Om tillsynsmyndigheten bedriver tillsyn över en verksamhetsutövare som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster enligt artikel 31 i Dora-förordningen ska tillsynsmyndigheten informera det tillsynsforum som inrättats enligt artikel 32 i samma förordning.

CER-direktivet

Enligt artikel 32.9 ska medlemsstaterna säkerställa att behöriga myndigheter informerar relevanta myndigheter enligt CER-direktivet inom samma medlemsstat när de utövar sina befogenheter med avseende på tillsyn på verksamhetsutövare som identifierats som kritisk enligt CER-direktivet. Enligt samma artikel får en CER-myndighet när så är lämpligt begära att en tillsynsmyndighet enligt NIS2-direktivet bedriver tillsyn över en sådan verksamhetsutövare. Enligt kommittédirektivet är utgångspunkten att samma myndighet som utövar tillsyn enligt NIS2-direktivet även utövar tillsyn enligt CER-direktivet. Vid en sådan ordning behövs ingen reglering av samarbetet. Utredningen återkommer till denna fråga i slutbetänkandet.

Dora-förordningen

Enligt artikel 32.10 och 33.6 ska medlemsstaterna säkerställa att de behöriga myndigheterna enligt NIS2-direktivet samarbetar med de relevanta behöriga myndigheterna i den berörda medlemsstaten en-

ligt Dora-förordningen.[21] Medlemsstaterna ska särskilt säkerställa att deras behöriga myndigheter enligt NIS2-direktivet informerar det tillsynsform som inrättats enligt artikel 32.1 i Dora-förordningen när de utövar tillsyn mot en väsentlig eller viktig verksamhetsutövare som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster enligt artikel 31 i Dora-förordningen.

En kritisk tredjepartsleverantör av IKT-tjänster är enligt artikel 2.2 i Dora-förordningen inte en så kallad finansiell entitet. En sådan leverantör omfattas inte av kraven på finansiella entiteter och omfattas därmed inte av undantaget för sektorsspecifika unionsakter.[22] En sådan leverantör kan därför komma att tillsynas av en tillsynsmyndighet enligt NIS2-direktivet.

För att införliva artikel 32.10 och 33.6 bör det tas in en bestämmelse i förordning som anger att om tillsynsmyndigheten utövar tillsyn mot en verksamhetsutövare som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster enligt Dora-förordningen ska tillsynsmyndigheten informera det tillsynsforum som inrättats enligt artikel 32.1 i samma förordning.

Personuppgiftsincidenter

Enligt artikel 31.3 ska tillsynsmyndigheterna ha ett nära samarbete med tillsynsmyndigheterna enligt dataskyddsförordningen[23] när de behandlar incidenter som medför personuppgiftsincidenter. Enligt artikel 35.1 ska tillsynsmyndigheten också utan onödigt dröjsmål informera tillsynsmyndigheten enligt dataskyddsförordningen om den får kännedom om en överträdelse av direktivet som även kan innebära en personuppgiftsincident. Av 35.3 framgår att om tillsynsmyndigheten som är behörig enligt dataskyddsförordningen är etablerad i en annan medlemsstat ska tillsynsmyndigheten enligt NIS2-direktivet informera tillsynsmyndigheten som är etablerad i Sverige. IMY är Sveriges nationella tillsynsmyndighet för behandling av personuppgifter.

[21] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.
[22] Se avsnitt 5.4.
[23] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Utredningen bedömer att en bestämmelse med denna innebörd bör införas i den nya förordningen.

Frågan om samordning med IMY rörande administrativa sanktionsavgifter behandlas i avsnitt 9.6.3.

Säkerhetsskyddslagen

Enligt utredningens förslag i kapitel 5 undantas säkerhetskänslig verksamhet från hela eller delar av cybersäkerhetslagens tillämpningsområde. Verksamhetsutövaren behöver inte heller lämna säkerhetsskyddsklassificerade uppgifter till tillsynsmyndigheten. Cybersäkerhetslagen gäller dock för övrig verksamhet som verksamhetsutövaren bedriver. Detta innebär att en tillsynsmyndighet kan bedriva tillsyn hos en verksamhetsutövare som även bedriver säkerhetskänslig verksamhet. Gränsdragningen rörande vad som utgör säkerhetskänslig verksamhet kan därmed bli avgörande för vilka delar av verksamheten som tillsynsmyndigheten kan tillsyna. För flera tillsynsområden kommer det att vara samma tillsynsmyndighet som bedriver tillsyn enligt säkerhetsskyddsregleringen och NIS2-regleringen. För några sektorer och verksamhetsutövare kommer det dock att vara olika tillsynsmyndigheter. Det finns därmed ett behov av samarbete mellan tillsynsmyndigheten för säkerhetsskyddslagen och tillsynsmyndigheten för cybersäkerhetslagen i de fall en verksamhetsutövare bedriver säkerhetskänslig verksamhet. Enligt 8 § förvaltningslagen (2017:900) ska en myndighet inom sitt verksamhetsområde samverka med andra myndigheter. Enligt 6 § myndighetsförordningen (2007:515) ska myndigheten också verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet. Mot den bakgrunden bedömer utredningen att det inte behövs någon särskild bestämmelse för att reglera myndigheternas samverkan.

Internationellt samarbete

Utredningens bedömning: Tillsynsmyndigheten ska samarbeta med och bistå tillsynsmyndigheter i andra medlemsstater inom EES när det gäller verksamhetsutövare som erbjuder tjänster i mer än en medlemsstat eller erbjuder tjänster i en eller flera med-

lemsstater och dess nätverks- och informationssystem finns i en eller flera medlemsstater.

Tillsynsmyndigheten får avslå en begäran om bistånd om myndigheten inte är behörig att tillhandahålla biståndet, om biståndet inte är proportionerligt i förhållande till tillsynsmyndighetens uppgifter eller om begäran avser information eller omfattar verksamhet som om den skulle lämnas ut eller utförs, skulle inverka skadligt på Sveriges säkerhetsintressen, allmänna säkerhet eller försvar.

Innan tillsynsmyndigheten avslår en begäran om bistånd ska tillsynsmyndigheten samråda med övriga berörda behöriga myndigheter samt, på begäran av de berörda medlemsstaterna, med kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa).

Om en verksamhetsutövare tillhandahåller tjänster i mer än en medlemsstat eller tillhandahåller tjänster i en eller flera medlemsstater och dess nätverks- och informationssystem finns i en eller flera medlemsstater ska de behöriga myndigheterna i de berörda medlemsstaterna vid behov samarbeta med och bistå varandra. Detta samarbete ska åtminstone omfatta följande:

a) Att tillsynsmyndigheten i en medlemsstat via den gemensamma kontaktpunkten informerar och samråder med de behöriga myndigheterna i övriga berörda medlemsstater om det tillsynsåtgärder som vidtagits.

b) Att en behörig myndighet får begära att en annan behörig myndighet vidtar tillsynsåtgärder.

c) Att en behörig myndighet, efter att ha mottagit en motiverad begäran från en annan behörig myndighet, ska tillhandahålla ömsesidigt bistånd till den andra behöriga myndigheten i proportion till sina egna resurser så att tillsyn kan genomföras på ett ändamålsenligt, effektivt och konsekvent sätt.

Det ömsesidiga biståndet får omfatta begäranden om information och tillsynsåtgärder. En behörig myndighet får inte avslå begäran om det inte fastställs att myndigheten antingen inte är behörig att tillhandahålla det begärda biståndet, att det begärda biståndet inte står i proportion till den behöriga myndighetens tillsynsuppgifter eller att begäran avser information eller omfattar verksamhet som, om

den lämnas ut eller utförs, skulle strida mot den medlemsstatens väsentliga nationella säkerhetsintressen, allmänna säkerhet eller försvar. Innan den behöriga myndigheten avslår en sådan begäran ska den samråda med övriga berörda behöriga myndigheter samt, på begäran av de berörda medlemsstaterna, med kommissionen och Enisa.

När så är lämpligt får behöriga myndigheter från olika medlemsstater i samförstånd genomföra de gemensamma tillsynsåtgärderna (artikel 37).

Artikeln innebär en skyldighet för nationella tillsynsmyndigheter att samarbeta med och vid behov bistå behöriga myndigheter i andra medlemsstater. Detta samarbete och bistånd får omfatta informationsutbyte mellan de berörda myndigheterna och begäranden om att vidta tillsynsåtgärder i en annan medlemsstat. Det ska därför tas in en bestämmelse i förordningen som anger att tillsynsmyndigheten ska samarbeta med och bistå tillsynsmyndigheter i andra medlemsstater inom EES när det gäller verksamhetsutövare som tillhandahåller tjänster i mer än en medlemsstat eller tillhandahåller tjänster i en eller flera medlemsstater och dess nätverks- och informationssystem finns i en eller flera medlemsstater. En bestämmelse om att tillsynsmyndigheten ska samarbeta och bistå tillsynsmyndigheter i andra medlemsstater finns i dag i 19 § NIS-förordningen när det gäller tillhandahållare av digitala tjänster.

Vidare innehåller artikeln omständigheter då en tillsynsmyndighet får avslå en begäran om bistånd från en annan medlemsstats tillsynsmyndighet samt en skyldighet att samråda innan ett sådant beslut om avslag. Utredningen anser att även dessa förutsättningar bör anges i förordningen.

9 Ingripanden och sanktioner

9.1 Inledning

9.1.1 Bakgrund

Av NIS2-direktivet följer en skyldighet för medlemsstaterna att införa verktyg i syfte att uppnå effektiv tillsyn och efterlevnadskontroll. Tillsynsmyndigheternas befogenheter för att genomföra tillsyn behandlas i kapitel 8. Vidare ska medlemsstaterna fastställa regler om sanktioner för överträdelser av nationella regler som antagits med stöd av NIS2-direktivet och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. De nationella sanktionsbestämmelserna ska anmälas till kommissionen senast den 17 januari 2025 och eventuella ändringar som berör dem ska anmälas utan dröjsmål.[1]

NIS2-direktivet anger ett antal sanktioner för tillsynsmyndigheterna som i dagsläget saknas i NIS-lagen. Vidare anger NIS2-direktivet vissa miniminivåer avseende sanktionsavgifternas storlek, vilket saknades i NIS-direktivet. Dessa förändringar medför ett behov av att se över systemet för sanktioner, och i den mån det behövs föreslå förändringar och tillägg till dessa. Utredningen föreslår i det följande åtgärder som kompletterar tillsynsåtgärderna som föreslagits i kapitel 8.

9.1.2 Sammanfattning av utredningens förslag i denna del

Utredningens bedömning: Tillsynsmyndigheten ska i varje enskilt fall avgöra vilken sanktion som är mest lämplig att använda och hur den ska utformas. Avhjälpande åtgärder kan förenas med sanktioner. Om tillsynsmyndigheten inte har anledning att in-

[1] Se artikel 36 NIS2-direktivet.

gripa på något annat sätt ska den meddela en anmärkning mot verksamhetsutövaren. Den kan i särskilda fall avstå från att ingripa.

Utredningens förslag: Tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter enligt lagen om cybersäkerhet, eller föreskrifter som har meddelats med stöd av bestämmelserna om

1. skyldighet att utse företrädare enligt 1 kap. 6 §,
2. anmälningsskyldighet enligt 2 kap. 2 §,
3. riskhanteringsåtgärder enligt 3 kap. 1 §,
4. utbildning enligt 3 kap. 3 §, eller
5. incidentrapportering enligt 3 kap. 5–7 §§.

Tillsynsmyndigheten får avstå från att ingripa om någon annan har vidtagit åtgärder mot verksamhetsutövaren eller den fysiska personen med anledning av överträdelsen och tillsynsmyndigheten bedömer att dessa åtgärder är tillräckliga.

Tillsynsmyndigheten är skyldig att ingripa mot överträdelser av de skyldigheter som anges och avgöra på vilket sätt den ska ingripa, samt hur ingripandet ska utformas. Med ingripande avses ageranden som innebär att tillsynsmyndigheten använder sig av en eller flera av de angivna sanktionerna (föreläggande, förbud, sanktionsavgift eller anmärkning). Vid dessa bedömningar ska samtliga relevanta omständigheter beaktas, men vissa anges särskilt i lagen (se vidare avsnitt 9.4.2). Genom de ingripandemöjligheter som föreslås kommer det finnas ett stort utrymme för tillsynsmyndigheten att agera inom. Den lindrigaste formen av ingripande kommer att utgöras av att anmärkning beslutas, och detta ska vara obligatoriskt om inte något annat ingripande görs (se vidare avsnitt 9.5.7 nedan). Den allvarligaste formen av ingripande kommer att kunna bestå av en kombination av förelägganden, förbud och sanktionsavgift. I särskilda fall kan tillsynsmyndigheten avstå från att ingripa (se vidare avsnitt 9.3.1 nedan).

9.2 Administrativa sanktioner eller straffrättsliga påföljder?

Utredningens bedömning: Tillsynsmyndigheten ska kunna besluta om administrativa sanktioner för överträdelser av bestämmelser i förslaget till den nya cybersäkerhetslagen och föreskrifter som har meddelats med stöd av den lagen.

I NIS2-direktivet (skäl 131 och 132) anges bland annat att medlemsstaterna ska kunna fastställa straffrättsliga påföljder och administrativa sanktioner för överträdelser av direktivets bestämmelser. Det överlämnas åt medlemsstaterna att i nationell rätt fastställa om påföljderna ska vara av administrativ eller straffrättslig natur.

Vid genomförandet av NIS-direktivet gjordes bedömningen att överträdelser inte skulle förenas med straffrättsliga påföljder, utan att påföljderna i stället skulle utgöras av administrativa sanktioner.[2] Som skäl för sin bedömning angav utredningen bland annat att straffrättsliga sanktioner bör väljas som en sista utväg och om exempelvis administrativa sanktioner inte kan anses tillräckligt effektiva för att uppnå det aktuella ändamålet. Vidare bedömde utredningen att NIS-direktivets syften kunde uppnås minst lika effektivt genom administrativa sanktioner i jämförelse med att införa bestämmelser om straffansvar. Som följd bedömde utredningen att genomförandet av NIS-direktivets sanktioner skulle föreslås vara av administrativt slag i svensk rätt. Regeringen anslöt sig till denna slutsats och bedömde att det var effektivare och i övrigt lämpligare med administrativa sanktioner än med straff.[3] Därutöver har regeringen tidigare bedömt att sanktionsavgifter inte anses ingå i det straffrättsliga systemet och att det därför i princip saknas krav på att utforma sanktionsavgifter i enlighet med straffrättsliga principer.[4]

Den nu aktuella utredningen saknar skäl att göra någon annan bedömning avseende NIS2-direktivets genomförande, och ansluter sig till den argumentation som framfördes i NIS-utredningen. Som följd bör de sanktioner som införs till följd av NIS2-direktivet vara av administrativt slag.

[2] SOU 2017:36 s. 183 ff.
[3] Prop. 2017/18:205 s. 64 f.
[4] Skr. 2009/10:79 s. 46.

9.3 Vilka överträdelser kan läggas till grund för sanktioner?

Utredningens förslag: Tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter enligt cybersäkerhetslagen, eller föreskrifter som har meddelats med stöd av bestämmelserna om

1. skyldighet att utse företrädare enligt 1 kap. 6 §,
2. anmälningsskyldighet enligt 2 kap. 2 §,
3. riskhanteringsåtgärder enligt 3 kap. 1 §,
4. utbildning enligt 3 kap. 3 §, eller
5. incidentrapportering enligt 3 kap. 5–7 §§.

Av artikel 31.4 NIS2-direktivet följer en skyldighet för medlemsstaterna att införa befogenheter för tillsynsmyndigheterna som möjliggör ingripanden mot överträdelser av direktivet. Sådana överträdelser avser skyldigheterna att utse företrädare, vidta riskhanteringsåtgärder för cybersäkerhet, utbildning, incidentrapportering (se kapitel 7) och skyldigheten för verksamhetsutövare att anmäla sig till tillsynsmyndigheten (se avsnitt 6.2).

Rörande skyldigheterna att vidta riskhanteringsåtgärder inklusive utbildning och att incidentrapportera anser utredningen att samtliga sanktioner ska finnas tillgängliga för tillsynsmyndigheterna.

Avseende verksamhetsutövarens skyldighet att anmäla sig finns en motsvarande bestämmelse i dag (23 § NIS-lagen) och tillsynsmyndigheterna har enligt gällande rätt endast möjlighet att utfärda sanktionsavgifter mot verksamhetsutövare som underlåtelser att anmäla sig (29 § 1). Enligt utredningens uppfattning ska underlåtelse att anmäla sig även fortsättningsvis vara en sanktionsgrundande överträdelse. Till skillnad från vad som gäller i dag anser utredningen dock att en sådan överträdelse inte bara ska kunna angripas med sanktionsavgift, utan tillsynsmyndigheterna ska även ha möjlighet att meddela exempelvis förelägganden förenat med vite (se vidare avsnitt 9.5.1 nedan) i syfte att framtvinga en anmälan. I dag finns även en skyldighet för gränsöverskridande verksamhetsutövare som erbjuder tjänster inom EU men som saknar etablering inom unionen att anmäla en

företrädare i någon av de medlemsstater där tjänsterna erbjuds.[5] Motsvarande skyldighet följer också av artikel 26.3 i NIS2-direktivet och bör även fortsättningsvis gälla och vara grund för sanktioner om den inte uppfylls.

9.3.1 Tillsynsmyndigheten ska kunna avstå från att ingripa i särskilda fall

Utredningens förslag: Tillsynsmyndigheten får avstå från att ingripa om någon annan har vidtagit åtgärder mot verksamhetsutövaren eller den fysiska personen med anledning av överträdelsen och tillsynsmyndigheten bedömer att dessa åtgärder är tillräckliga.

Av artikel 4 i Europakonventionens sjunde tilläggsprotokoll följer bland annat det s.k. dubbelprövningsförbudet. Det innebär en rätt att inte bli lagförd eller straffas två gånger för samma brott (gärning). Eftersom en verksamhetsutövare kan bedriva flera verksamheter som faller under olika tillsynsmyndigheter riskerar en överträdelse att kunna angripas av flera tillsynsmyndigheter parallellt. På motsvarande sätt medför bestämmelserna om jurisdiktion (se avsnitt 5.3.2 ovan) att en enskild verksamhetsutövare kan omfattas av flera länders jurisdikton. Detta kan innebära att flera NIS2-tillsynsmyndigheter kan ingripa mot samma överträdelse. Om någon annan tillsynsmyndighet – svensk eller utländsk – ingriper mot samma överträdelse riskerar agerandet att bryta mot dubbelprövningsförbudet. Eftersom utredningen föreslår att tillsynsmyndigheten alltid ska ingripa mot överträdelser behöver en ventil skapas för att dubbelprövningsförbudet inte ska överträdas. Enligt utredningens mening ska det dock råda stark presumtion för ingripande. Som följd ska ventilen utformas på så sätt att det är möjligt att ingripa även om en annan myndighet ingripit, så länge dubbelprövningsförbudet inte överträds. Exempelvis skulle en överträdelse – som faller inom två tillsynsmyndigheters ansvarsområden – av den ena tillsynsmyndigheten kunna leda till ett åtgärdsföreläggande för att åtgärda överträdelsen och att den därefter avslutar sitt ingripande. Den andra tillsynsmyndigheten är då oförhindrad att meddela en sanktionsavgift till följd av samma överträdelse. Föreläggandet var av reparativ art (upphöra med en

[5] Se 10 och 28 §§ NIS-lagen.

överträdelse) medan sanktionsavgiften är en påföljd för att överträdelsen över huvud taget skett. Ventilen skulle även kunna tillämpas när samma incident redan lett till kännbara sanktioner enligt något annat regelverk, t.ex. enligt säkerhetsskyddslagen.[6]

9.4 Gemensamma bestämmelser för sanktionerna

I denna del kommer utredningen att redogöra för de bestämmelser som är gemensamma i fråga om val av sanktion och utformning av dem.

9.4.1 Val av sanktion och generella krav på sanktionernas utformning

Utredningens bedömning: Det behöver inte införas särskilda bestämmelser i svensk rätt för att tillgodose NIS2-direktivets generella krav på sanktionernas utformning.

Tillsynsmyndighetens möjligheter att meddela sanktioner ska framgå av lag.

Av artikel 36 i NIS2-direktivet följer att de sanktioner som en tillsynsmyndighet meddelar ska vara effektiva, proportionella och avskräckande. Utredningen anser att dessa aspekter ska vara vägledande för tillsynsmyndigheternas ingripanden inom ramen för NIS2-bestämmelserna i fråga om vilken sanktion som ska väljas och vid utformningen av den. Vad gäller kravet på att åtgärden ska vara effektiv och proportionerlig framgår sådana krav redan av 5 § tredje stycket förvaltningslagen (2017:900). Det saknar enligt utredningens mening därför skäl att införa särskilda bestämmelser till följd av NIS2-direktivet. I fråga om att sanktionerna ska ha en avskräckande effekt anser utredningen att ett sådant krav uppfylls genom det handlingsutrymme som tilldelas tillsynsmyndigheterna i fråga om val av åtgärd och dess utformning.[7] Vidare bedömer utredningen att NIS2-direktivets krav (artikel 32.8) på motivering av beslut och kommunicering med mera för svenska myndigheter redan följer av förvaltningslagen. Som följd anser utredningen att det inte behöver införas särskilda bestämmel-

[6] Se prop. 2017/18:205 s. 71 f.
[7] Se till exempel prop. 2020/21:194 s. 89 och 103.

ser i svensk rätt för att genomföra NIS2-direktivets krav avseende sanktionernas utformning eller det processuella förfarandet knutet till dem.

Precis som gäller i dag bör sanktionerna – som är ingripande åtgärder – regleras i lag för att uppfylla regeringsformens krav på normgivning.[8]

9.4.2 Vad ska beaktas särskilt vid val av sanktion och utformningen av dem?

Utredningens bedömning: Vid valet av sanktion, utformningen av den och vid bestämmande av en sanktionsavgifts storlek ska tillsynsmyndigheten beakta samtliga relevanta omständigheter. Därutöver ska vissa omständigheter beaktas särskilt.

Utredningens förslag: Vid val och utformning av ingripandeåtgärder ska hänsyn tas till hur allvarlig överträdelsen är, hur länge den har pågått, samt den skada eller risk för skada som uppstått till följd av överträdelsen.

Vid bedömningen ska särskilt beaktas

1. de åtgärder verksamhetsutövaren vidtagit för att förhindra eller minska skadan,
2. verksamhetsutövarens samarbete med tillsynsmyndigheten,
3. om överträdelsen begåtts med uppsåt eller oaktsamhet, och
4. den ekonomiska fördel som verksamhetsutövaren fått till följd av överträdelsen.

Enligt artiklarna 32.7, 33.5 och 34.3 i NIS2-direktivet ska medlemsstaterna tillgodose att tillsynsmyndigheterna åtminstone tar hänsyn till vissa omständigheter (angivna i artikel 32.7) när de beslutar om ett ingripande, eller om en sanktionsavgift ska påföras och dess storlek. Dessa omständigheter är:

[8] Jfr 8 kap. 2 § första stycket 2 regeringsformen, se vidare SOU 2017:36 s. 189.

a) Överträdelsens allvar och betydelsen av de bestämmelser som har överträtts, med beaktande av att bland annat följande alltid ska anses vara en allvarlig överträdelse:

i) Upprepade överträdelser.

ii) Underlåtenhet att underrätta om eller avhjälpa betydande incidenter.

iii) Underlåtenhet att avhjälpa brister enligt bindande instruktioner från behöriga myndigheter.

iv) Hindrande av revisioner eller övervakningsverksamhet som den behöriga myndigheten beordrat efter det att en överträdelse konstaterats.

v) Tillhandahållande av falsk eller grovt felaktig information i fråga om riskhanteringsåtgärder för cybersäkerhet eller rapporteringsskyldigheter enligt artiklarna 21 och 23.

b) Överträdelsens varaktighet.

c) Eventuella tidigare relevanta överträdelser från den berörda entitetens sida.

d) Den materiella eller immateriella skada som uppstått, inbegripet finansiella eller ekonomiska förluster, effekter på andra tjänster och det antal användare som berörs.

e) Uppsåt eller oaktsamhet från den som har gjort sig skyldig till överträdelsen.

f) De åtgärder som entiteten har vidtagit för att förhindra eller begränsa den materiella eller immateriella skadan.

g) Efterlevnad av godkända uppförandekoder eller godkända certifieringsmekanismer.

h) I vilken utsträckning de fysiska eller juridiska personer som hålls ansvariga samarbetar med de behöriga myndigheterna.

Dessa bestämmelser saknar motsvarighet i NIS-direktivet och NIS-lagen. Omständigheterna i 32.7 NIS2-direktivet är många, tar sikte på olika händelsetyper (överträdelser och incidenter) och kan innebära att en överträdelse ska bedömas som allvarlig. Utredningen anser att dessa omständigheter bör anges i lag med de anpassningar som behövs, i syfte att främja en enhetlig tillämpning hos tillsynsmyndigheterna. En sådan ordning skapar också ökad förutsebarhet

även för de verksamhetsutövare som omfattas av regleringen. Utredningen anser dock inte att uppräkningen ska uppfattas som uttömmande kring vilka omständigheter ska beaktas vid prövningen, utan ska ses som styrning kring vilka omständigheter som särskilt ska beaktas. Utredningen bedömer att skyldigheten att beakta samtliga relevanta omständigheter – utöver de nyss uppräknade – följer av 23 § förvaltningslagen (2017:900) och den så kallade omsorgsprincipen.[9] Som följd behöver en sådan skyldighet inte regleras särskilt i den föreslagna cybersäkerhetslagen. Enligt utredningens uppfattning bör den bärande principen vid bestämmandet av ett ingripande eller en sanktionsavgift vara en sammanvägd bedömning av omständigheterna i det enskilda fallet.

Av systematiken i NIS2-direktivet följer att vissa omständigheter ska anses innebära en allvarlig överträdelse. Utredningen anser att en överträdelse kan anses allvarlig även om sådana omständigheter saknas. Som följd bör tillsynsmyndigheten beakta vissa omständigheter särskilt, och förekomsten av dem ska innebära en presumtion för att överträdelsen är allvarlig, men även andra omständigheter kan göra att en överträdelse ska bedömas som allvarlig. Mot bakgrund av detta föreslår utredningen en ordning där vissa omständigheter ska beaktas, och de kan i det enskilda fallet innebära förmildrande, neutrala eller försvårande omständigheter. Vidare ska vissa omständigheter alltid beaktas som förmildrande, medan andra alltid som försvårande. Slutligen ska förekomsten av vissa omständigheter alltid medföra att överträdelsen ska beaktas som allvarlig.

Omständigheter som ska beaktas

Hur allvarlig överträdelsen är och hur länge den har pågått

Vid bedömningen av en överträdelses allvarsgrad ska överträdelsens omfattning vägas in. Allvarlighetsbedömningen kan även påverkas av särskilda bedömningsgrunder som redogörs för senare i detta avsnitt. Vidare bör tiden som överträdelsen pågått vägas in. Här ska noteras att en överträdelse som inträffar vid en viss tidpunkt men upptäcks långt senare och åtgärdas omedelbart ändå kan vara att betrakta som en allvarlig överträdelse. I gengäld bör ett sådant skynd-

[9] Se prop. 2016/17:180 s. 148 f.

samt agerande att åtgärda den allvarliga överträdelsen kunna vägas in i mildrande riktning.

Uppkommen (risk för) skada

Omfattningen av den skada, eller risk för skada, som har uppstått till följd av överträdelsen är en faktor som ska beaktas särskilt. I NIS2-direktivet anges att skadan kan avse både materiell och immateriell skada, inklusive finansiella eller ekonomiska förluster, effekter på andra tjänster och det antal användare som berörs. Utredningen bedömer att dessa exempel kan vara vägledande, men det saknas skäl att begränsa tillsynsmyndighetens bedömning till dessa aspekter. I stället ska begreppet ”skada” ses ur ett brett perspektiv utifrån omständigheterna i det enskilda fallet. Utredningen föreslår vidare att bedömningsgrunden inte ska vara begränsad till faktisk skada, utan även risk för skada som överträdelsen kan ha medfört.

Vidtagna åtgärder för att minimera skada

Många gånger kommer omfattningen av ett ingripande att påverkas av vilka åtgärder som verksamhetsutövaren har vidtagit för att minska eller helt förhindra skadan som (hade kunnat) uppstått till följd av överträdelsen. Det ska enligt utredningens bedömning röra sig om verksamma åtgärder för att bestämmelsen ska kunna leda till en mildrande påverkan av vilken sanktion som tillgrips och utformningen av den (exempelvis en sanktionsavgifts storlek). Bedömningspunkten kommer kunna ha ett nära samband med punkten *Uppkommen (risk för) skada* ovan, enligt vilken det kan ha uppstått en risk för skada, men där faktisk skada har undvikits eller minimerats tack vare att verksamhetsutövaren vidtagit skyndsamma och verkningsfulla åtgärder.

Verksamhetsutövarens samarbete med tillsynsmyndigheten i utredningen

En ytterligare aspekt att beakta är i vilken utsträckning verksamhetsutövaren samarbetat med tillsynsmyndigheten inom ramen för den aktuella utredningen. Att verksamhetsutövaren har incident-

rapporterat är således inte i sig en åtgärd som tyder på samarbetsvilja eftersom det utgör en skyldighet för verksamhetsutövaren. Om verksamhetsutövaren motverkat eller inte bidragit i utredningen bör detta beaktas i försvårande riktning, medan ett aktivt samarbete där verksamhetsutövaren rättar sig efter tillsynsmyndighetens anvisningar och rekommendationer ska beaktas som förmildrande.

Uppsåt eller oaktsamhet hos verksamhetsutövaren

Ingripande mot en oavsiktlig och oaktsam överträdelse ska som utgångspunkt ske mildare än en avsiktlig och genomtänkt överträdelse. Detta hänger även samman med att överträdelser av regelverket i vissa fall kommer vara enklare att konstatera än i andra. Som följd kan oavsiktliga överträdelser av regelverket uppstå trots att verksamhetsutövaren har försökt att efterleva detsamma. På omvänt sätt ska en grovt oaktsam eller uppsåtlig överträdelse betraktas i starkt försvårande riktning. Vid sådana överträdelser anser utredningen att tillsynsmyndigheten bör betrakta överträdelsen som allvarlig och anpassa sitt ingripande därefter.

Ekonomiska fördelar genom överträdelsen

Av 31 § NIS-lagen följer bland annat att de kostnader som verksamhetsutövaren har undvikit till följd av överträdelsen ska beaktas vid bestämmande av en sanktionsavgifts storlek. Denna aspekt saknar grund i NIS-direktivet och NIS2-direktivet innehåller inte heller någon liknande punkt att beakta. Utredningen bedömer dock att den aktuella bedömningsgrunden har visat sig effektiv och anser att den ska överföras även till den nya lagen med vissa modifieringar. Även om bedömningsgrunden troligen är mest relevant i fråga om bestämmande av sanktionsavgifters storlek kan det inte uteslutas att den även kan vara relevant vid andra bedömningar av en överträdelse. Utredningen föreslår vidare att begreppet ”ekonomisk fördel” ska användas i stället för ”vinst” eller ”kostnad” som förekommer i annan författning.[10] Fördelen med begreppet ”ekonomisk fördel” är att det

[10] Se 7 kap. 5 § säkerhetsskyddslagen (2018:585).

enligt utredningens mening både inbegriper fastställbara vinster och undvikna kostnader till följd av överträdelser.[11]

Om en verksamhetsutövare genom sin överträdelse fått någon ekonomisk fördel ska detta därmed beaktas som försvårande vid bestämmande av sitt ingripande. Exempelvis ska en sanktionsavgifts storlek kunna anpassas för att eliminera de ekonomiska fördelar som verksamhetsutövaren dragit av sitt agerande, till exempel genom att inte bekosta en viss skyddsåtgärds genomförande.

Omständigheter som ska påverka i försvårande respektive mildrande riktning

Utredningens förslag: Vid bedömningen av en överträdelse ska det beaktas som försvårande om verksamhetsutövaren tidigare har begått en överträdelse.

I förmildrande riktning ska beaktas om verksamhetsutövaren har följt godkända uppförandekoder eller godkända certifieringsmekanismer.

Tidigare överträdelser

Om en verksamhetsutövare tidigare begått en eller flera överträdelser ska tillsynsmyndigheten överväga om de kan anses utgöra en försvårande omständighet vid bedömningen av den nu aktuella överträdelsen. Denna bedömning tar sikte på en bredare krets av överträdelser än sådana som kan leda till att det kan anses röra sig om *upprepade överträdelser* (se vidare nedan). De tidigare överträdelserna bör bedömas vara relevanta, men de behöver inte vara identiska med den nu aktuella. Tiden sedan den föregående och relevanta överträdelsen begicks bör också vägas in i bedömningen, där en lång tid bör tala i mildrande riktning och vice versa. Om verksamhetsutövaren gjort sig skyldig till likartade överträdelser som dessutom ligger nära i tiden ska detta bedömas som försvårande. Samma slutsats bör gälla om tillsynsmyndigheten bedömer att överträdelserna har skett på ett närmast systematiskt sätt.

[11] Jfr prop. 2016/17:22 s. 386.

Efterlevnad till godkända uppförandekoder eller certifieringsmekanismer

En omständighet som alltid ska beaktas i förmildrande riktning är om en verksamhetsutövare har valt att följa uppförandekoder eller certifieringsmekanismer som tagits fram baserat på EU:s arbete. En tillsynsmyndighet skulle kunna bedöma att en verksamhetsutövare som tillämpar en sådan uppförandekod har begått en överträdelse i ett visst avseende. Vid granskning bedömer man dock att skälet till att överträdelsen har uppstått är att uppförandekoden följts. I ett sådant läge där en lojal tillämpning av en uppförandekod medför en överträdelse av NIS2-direktivets skyldigheter anser utredningen att det alltid ska påverka i mildrande riktning.

Omständigheter som ska göra att en överträdelse är allvarlig

Utredningens förslag: En överträdelse ska betraktas som allvarlig om verksamhetsutövaren

1. har begått upprepade överträdelser,
2. inte har rapporterat eller avhjälpt en betydande incident,
3. inte har följt ett tidigare föreläggande från en tillsynsmyndighet,
4. har hindrat säkerhetsrevisioner eller tillsynsåtgärder som tillsynsmyndigheten beslutat om, eller
5. har lämnat oriktiga uppgifter avseende riskhanteringsåtgärder eller rapporteringsskyldigheter enligt 3 kap. 1 eller 5–7 §§.

Utredningen anser mot bakgrund av NIS2-direktivets exemplifiering att förekomsten av någon av följande omständigheter ska göra att överträdelsen är att betrakta som allvarlig.

Upprepade överträdelser

Om verksamhetsutövaren har begått överträdelser som är av samma eller likartad art kan den aktuella överträdelsen bedömas utgöra ett led i upprepade överträdelser. En upprepad överträdelse ska alltid innebära att överträdelsen är att betrakta som allvarlig. För att kunna avgöra om en överträdelse är upprepad bör både överträdelsens art och tiden mellan den föregående och nu aktuella överträdelsen beaktas. Detta skulle exempelvis kunna innebära att en verksamhetsutövare har gjort sig skyldig till två tidigare identiska överträdelser, men att de har skett med två års mellanrum varje gång. Det rör sig då förvisso om identiska överträdelser som har upprepats, men det är inte säkert att de ska bedömas som upprepade enligt den aktuella bedömningsgrunden, utan det kan ligga närmare till hands att beakta dem som *tidigare överträdelser* enligt ovan. Om överträdelserna tyder på att verksamhetsutövaren begått dem på ett systematiskt sätt bör det anses utgöra en upprepad överträdelse.

Underlåtelse att rapportera eller avhjälpa betydande incidenter

Om en verksamhetsutövare underlåter att rapportera eller avhjälpa en betydande incident[12] ska en sådan överträdelse bedömas som allvarlig. En sådan överträdelse ska enligt utredningen anses föreligga både om verksamhetsutövaren inte rapporterar eller avhjälper över huvud taget, eller om det avseende rapporteringen sker men efter de tidsramar som anges i cybersäkerhetslagen.

Om tidigare föreläggande inte följts

En överträdelse som har sitt ursprung i att en verksamhetsutövare inte har följt ett föreläggande från en tillsynsmyndighet (se avsnitt 9.5.1 nedan) ska anses utgöra en allvarlig överträdelse. Bedömningen kan komma att behöva nyanseras av tillsynsmyndigheten, exempelvis om verksamhetsutövaren uppenbart försökt följa föreläggandet på ett lojalt sätt, men inte lyckats fullt ut. Åt andra hållet kan uppenbart motstånd, exempelvis genom att ingen åtgärd vidtagits alls, beaktas som försvårande.

[12] Se artikel 23 i NIS2-direktivet.

Hindrat verkställighet av tillsynsmyndighetens tillsynsåtgärder m.m.

Även sådana ageranden som innebär att verksamhetsutövaren har hindrat säkerhetsrevisioner eller andra åtgärder som en tillsynsmyndighet har beslutat om ska anses utgöra en allvarlig överträdelse av bestämmelserna. För att ageranden ska kunna utgöra en sådan överträdelse krävs enligt utredningens mening att agerandet bestått av någon form av passiv eller aktiv obstruktion av åtgärden, till exempel genom att vägra tillsynsmyndigheten tillträde till verksamhetsutövarens lokaler. Det kan därmed inte röra sig om att överklaga tillsynsmyndighetens beslut.

Oriktiga uppgifter

Slutligen ska även oriktiga uppgifter beaktas särskilt och leda till att en överträdelse ska bedömas som allvarlig. Bestämmelsen bör inte ta sikte på oriktiga uppgifter i alla skeden, utan begränsas till sådana som lämnas avseende riskhanteringsåtgärder eller rapporteringsskyldigheter. Motsvarande begränsning finns bland annat inom säkerhetsskyddsbestämmelserna.[13] Med ”oriktig uppgift” avses felaktiga eller missvisande uppgifter, men även utelämnade uppgifter som borde ha lämnats.[14]

Effekten av att en överträdelse är att betrakta som allvarlig

NIS2-direktivet anger inte vad följden av att en överträdelse bedöms som allvarlig ska vara. Enligt utredningens mening får en sådan klassificering ses i ljuset av de grundläggande principerna i direktivet om att sanktioner ska vara effektiva, proportionella och avskräckande med beaktande av omständigheterna i varje enskilt fall. Att en överträdelse är allvarlig bör innebära att mer ingripande och avskräckande sanktioner anses uppfylla proportionalitetskravet. Det bör således innebära att tillsynsmyndigheten dels ska kunna tillgripa mer långtgående sanktionstyper (exempelvis förbudssanktionen, se avsnitt 9.5.6), dels utforma sanktionerna på ett mer ingripande sätt. Det senare kan exempelvis ske genom att tillsynsmyndigheten bestämmer ett vite

[13] Se 7 kap. 1 § 5 och 2 § 3 säkerhetsskyddslagen (2018:585).
[14] Jfr 49 kap. 5 § skatteförfarandelagen (2011:1244).

eller en sanktionsavgift till ett högre beloppsintervall, för att på så vis öka graden av avskräckande. Enligt utredningens uppfattning saknas det dock skäl att föra in dessa konsekvenser i författning, utan dessa ska i stället beaktas som en del av tillsynsmyndigheternas helhetsprövning.

9.5 Vilka administrativa sanktioner och andra möjligheter till ingripande ska finnas?

Utredningens bedömning: De sanktioner och ingripandemöjligheter som i dag finns i NIS-lagen (föreläggande och sanktionsavgift) ska anpassas och överföras till den föreslagna nya cybersäkerhetslagen. Fyra nya sanktioner ska införas: anmärkning, information till användare om betydande cyberhot, offentliggörande av överträdelser, respektive förbud för personer att utöva ledningsfunktioner. Maximinivåerna för sanktionsavgifter ska höjas till de nivåer som följer av NIS2-direktivet.

Som tidigare redovisats bygger NIS2-direktivet vidare på de skyldigheter och ingripandemöjligheter som togs fram i NIS-direktivet och som genomförts i svensk rätt. Utredningens uppfattning är att dessa ingripandemöjligheter har visat sig ändamålsenliga och att de bör därför överföras till den nya regleringen, med de modifikationer och tillägg som föranleds av NIS2-direktivet. Övervägandena och ingripandemöjligheterna kommer att redovisas i det följande.

9.5.1 Föreläggande som kan förenas med vite

Utredningens förslag: Tillsynsmyndigheten får meddela de förelägganden som behövs för att verksamhetsutövare ska uppfylla skyldigheterna som följer av 5 kap. 1 § i den föreslagna cybersäkerhetslagen.

Ett föreläggande får förenas med vite.

Utredningen har i avsnitt 8.4.6 bedömt att tillsynsmyndigheten ska få meddela förelägganden vid vite. Föreläggande med vitesmöjlighet är ett centralt verktyg för att tillsynsmyndigheterna ska kunna tillse att de aktuella reglerna efterlevs.[15] Sanktionen syftar till att den som står under tillsyn ska lämna viss information som behövs för tillsynen eller efterlevnadskontrollen. Utredningen bedömer att sanktionen även ska kunna användas för att förmå en aktör att vidta – eller avstå från att vidta – vissa åtgärder.

Motsvarande reglering återfinns i dag i 28 § NIS-lagen. Utredningen bedömer att motsvarande bestämmelse ska föreslås även i cybersäkerhetslagen. För att sanktionen ska kunna vara både effektiv och avskräckande bedömer utredningen att den även fortsättningsvis ska kunna förenas med vite. Om vite föreläggs är lagen (1985:206) om viten tillämplig, vilket bland annat innebär att proportionalitetskrav kommer att behöva beaktas vid fastställande av vitets storlek (se avsnitt 8.4.6). Lagen innehåller inte några beloppsbegränsningar, vilket medför att tillsynsmyndigheterna kan fastställa vitesbeloppet till den nivå man finner lämpligt för att den avsedda effekten ska uppnås.

Åtgärden ska kunna riktas mot offentliga aktörer. Utredningen förutsätter visserligen att offentliga aktörer kommer att rätta sig efter tillsynsmyndighetens anmaningar frivilligt, och därmed att viteshotet endast undantagsvis kommer att behöva realiseras. Möjligheten bör dock ändå finnas där för tillsynsmyndigheterna, till exempel för situationen när det finns en betydande risk i nätverks- eller informationssystem och där tillsynsmyndigheten misstänker att riskhanteringsåtgärder inte har vidtagits. Det kan också röra sig om att åtgärder måste vidtas skyndsamt i syfte att uppnå avsedd effekt.

9.5.2 Informera användare om betydande cyberhot

Utredningens förslag: Tillsynsmyndigheten får förelägga en verksamhetsutövare att informera de användare som kan påverkas av ett betydande cyberhot om hotet och vilka skydds- eller motåtgärder de kan vidta. Ett sådant föreläggande ska få förenas med vite.

[15] Se skr. 2009/10:79 s. 44.

Enligt artiklarna 32.4 e och 33.4 e NIS2-direktivet ska medlemsstaterna säkerställa att tillsynsmyndigheterna har möjlighet att ålägga verksamhetsutövare att informera de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller utför verksamheter som potentiellt kan beröras av ett betydande cyberhot om hotets karaktär och om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa fysiska eller juridiska personer kan vidta som svar på hotet. Bestämmelsen saknar motsvarighet i NIS-direktivet. Enligt NIS2-direktivet ansluter ingripandemöjligheten till förekomsten av ett *betydande cyberhot*, vilket definieras i artikel 6.11. Av detta följer att informationsskyldigheten inte kräver att en viss incident har inträffat, utan ett cyberhot är tillräckligt. Om ett sådant förekommer ska verksamhetsutövaren kunna göras skyldig att informera de som använder verksamhetsutövarens tjänster om cyberhotets karaktär och de åtgärder som kan vidtas av användaren för att undvika eller minska effekterna av hotet. En liknande bestämmelse återfinns i 8 kap. 4 § LEK. Utredningen bedömer att det finns anledning att det ska införas en möjlighet för NIS2-tillsynsmyndigheterna att meddela förelägganden för att framtvinga att en verksamhetsutövare informerar om cyberhot på det sätt som direktivet anger. Ett sådant föreläggande ska kunna förenas med vite.

9.5.3 Offentliggörande av överträdelser av direktivet

Utredningens förslag: Tillsynsmyndigheten får förelägga en verksamhetsutövare att offentliggöra information på det sätt som tillsynsmyndigheten beslutar rörande överträdelser av cybersäkerhetslagen och föreskrifter som har meddelats med stöd av lagen. Ett sådant föreläggande ska få förenas med vite.

Enligt artikel 32.4 h i NIS2-direktivet ska medlemsstaterna säkerställa att tillsynsmyndigheterna har möjlighet att ålägga de berörda verksamhetsutövarna att offentliggöra aspekter av överträdelser av direktivet på ett specificerat sätt. Bestämmelsen saknar motsvarighet i NIS-direktivet och någon liknande befogenhet har inte införts tidigare. Utredningen bedömer att den aktuella sanktionen kan anses täckas av möjligheterna i svensk rätt att meddela föreläggande. I andra lagstiftningsärenden där liknande – men inte identiska – bestämmelser

genomförts i svensk rätt har dock sanktionen angivits särskilt, utöver den allmänna möjligheten till förelägganden.[16] Utredningen bedömer mot denna bakgrund att NIS2-sanktionen bör anges särskilt. Det bör ankomma på tillsynsmyndigheterna att närmare besluta var ett offentliggörande ska ske och vilka uppgifter offentliggörandet ska innehålla.

9.5.4 Utse övervakningsansvarig hos tillsynsmyndigheten

Utredningens bedömning: Det behöver inte införas någon särskild rätt för tillsynsmyndigheten att utse en övervakningsansvarig hos tillsynsmyndigheten.

I artikel 32.4 g NIS2-direktivet anges att medlemsstaterna ska säkerställa att de behöriga myndigheterna har befogenhet att utse en övervakningsansvarig med väldefinierade uppgifter för en fastställd tidsperiod för att övervaka att de berörda verksamhetsutövarna efterlever artiklarna 21 och 23 i direktivet. Bestämmelsen ger en grund för tillsynsmyndigheten att peka ut en tjänsteman hos sig att fullgöra de angivna uppgifterna. Utredningen bedömer att sådana möjligheter redan föreligger för tillsynsmyndigheten utan att detta behöver anges särskilt. Som följd behöver inte några förslag lämnas för att genomföra den aktuella bestämmelsen i svensk rätt.

9.5.5 Tillfälligt upphävande av auktorisation eller certifiering

Utredningens bedömning: Det ska inte införas en möjlighet till tillfälligt upphävande av en väsentlig verksamhetsutövares auktorisation eller certifiering.

[16] Se till exempel 8 kap. 3 § andra stycket lagen (2022:482) om elektronisk kommunikation, jfr 5 kap. 6 c § i den upphävda lagen (2003:389) om elektronisk kommunikation.

Finns behov av att införa sanktionen?

Enligt artikel 32.5 a NIS2-direktivet ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenhet att tillfälligt upphäva eller begära att ett certifierings- eller auktorisationsorgan, eller en domstol, i enlighet med nationell rätt, tillfälligt upphäver en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls eller verksamheter som utövas av den väsentliga verksamhetsutövaren. Redan den omständigheten att sanktionen är en sådan som enligt NIS2-direktivet ska genomföras av medlemsstaterna talar med styrka för att det finns ett behov av att en sådan sanktion ska föreslås. Frågan är dock om en sådan sanktion kan anses ha någon praktisk verkan i det svenska systemet som föreslås.

Någon motsvarande bestämmelse finns inte i NIS-direktivet, men övervägdes ändå att införas i samband med det ursprungliga direktivets genomförande.[17] Både NIS-utredningen och regeringen valde dock att inte föreslå någon sådan sanktion. Som skäl angavs bland annat att merparten av de aktörer som omfattas av NIS-lagen inte är beroende av tillstånd för att bedriva sin verksamhet, och att en sådan sanktion därmed inte är användbar för ingripanden i de flesta fall.[18]

Utredningen delar uppfattningen även avseende NIS2-direktivet att de flesta verksamhetsutövare som träffas av regleringen inte är beroende av ett visst tillstånd för att bedriva sin verksamhet. Detta skulle kunna tala för att behovet av att införa den aktuella sanktionen är begränsat. Utredningen noterar dock att genom formuleringen i NIS2-direktivet är sanktionen inte begränsad till ”tillstånd”, utan rör ”certifiering eller auktorisation”. Det framstår dock som oklart vilka former av auktorisationer eller certifieringar som avses. En sanktion som medger tillfälligt upphävande av certifiering eller auktorisation är en ingripande åtgärd som enligt utredningens mening ställer höga krav på att förutsägbarhets- och rättssäkerhetsperspektiv kan upprätthållas. Som följd behöver räckvidden av skrivningen tolkas. I brist på annat tillgängligt underlag bedömer utredningen i det finns åtminstone två olika tolkningar kring räckvidden.

Den första tolkningen är att sanktionen tar sikte på *tillstånd att bedriva verksamhet som faller under direktivets tillämpning*. Utredningen kan konstatera att varken NIS- eller NIS2-direktivet ställer

[17] SOU 2017:36 s. 185 och prop. 2017/18:205 s. 66.
[18] Prop. 2017/18:205 s. 66.

krav på att en verksamhetsutövare ska beviljas tillstånd för att få bedriva den verksamhet som gör att de träffas av direktiven. Det går inte att utesluta att andra medlemsländer har infört nationella bestämmelser om tillståndsplikt för NIS-verksamhet, och att sanktionen skulle kunna ta sikte på sådana länder. Några motsvarande krav finns dock inte i svensk rätt. Att införa ett sådant krav med tillhörande sanktionsmöjlighet skulle därför framstå som främmande. Detta talar enligt utredningen med styrka emot att införa sanktionsmöjligheten på denna grund.

Den andra tolkningen innebär att de certifieringar eller auktorisationer som avses är sådana som kan vara av betydelse för att uppnå en hög gemensam cybersäkerhetsnivå inom EU (artikel 1). Av artikel 35.2 NIS2-direktivet framgår dock inte någon exemplifiering på vilka certifieringar/auktorisationer detta skulle kunna avse, varför det behöver tolkas.

En extensiv tolkning av innebörden skulle som utgångspunkt innebära en rätt för tillsynsmyndigheterna att begära att alla former av certifieringar/auktorisationer ska kunna upphävas tillfälligt, så länge dessa till någon del kan påverka verksamhetsutövarens möjlighet att upprätthålla en verksamhet av betydelse för NIS2-direktivet. Detta skulle exempelvis kunna inkludera en verksamhetsutövares frivilliga certifiering enligt ISO 27000-serien, eller en mobiltelefonioperatörs tillstånd att använda radiosändare och som meddelats med stöd av lagen (2022:482) om elektronisk kommunikation. Upphävande av dessa typer av certifieringar eller auktorisationer skulle förvisso kunna påverka verksamhetsutövarnas möjligheter att utöva verksamhet enligt NIS2. En sådan räckvidd av sanktionen framstår dock som allt för ingripande i förhållande till vad den är tänkt att uppnå (jfr artikel 1), och det saknas stöd i NIS2-direktivet för att en sådan verkan har varit avsedd. Att ge verktyget en sådan långtgående verkan skulle också göra att det inte går att förutse vilken typ av ingripanden som skulle kunna ske med stöd av det. Detta skulle innebära oöverblickbara konsekvenser ur förutsägbarhets- och rättssäkerhetssynpunkt för de som kan drabbas av sanktionen, och därtill vålla avsevärda tillämpningssvårigheter för tillsynsmyndigheterna. Utredningen bedömer att ett sådant tillsynsverktyg inte kan föreslås införas i svensk rätt.

En restriktiv tolkning skulle enligt utredningens uppfattning kunna ta sikte på sådana auktorisationer och certifieringar som har en tydligare koppling till NIS2-direktivet.[19] Utredningen har kunnat identifiera två exempel på sådana, nämligen eIDAS[20] respektive europeiska cybersäkerhetscertifikat (nedan *ECC*). Båda dessa regelverk har sin grund i EU-förordningar, och i Sverige finns det endast en myndighet (PTS avseende eIDAS, FMV avseende ECC) som är behörig att fatta beslut med stöd av respektive regelverk.[21] Om den nu aktuella NIS2-sanktionen ska införas behöver den därför utformas som en möjlighet för tillsynsmyndigheterna att ansöka hos behörig myndighet om tillfälligt upphävande av viss certifiering eller auktorisation. Ett sådant tillfälligt upphävande ska dessutom endast gälla till dess att verksamhetsutövaren har avhjälpt de aktuella bristerna eller uppfyllt de aktuella kraven från tillsynsmyndigheten. Således måste ett tillfälligt upphävande också kunna upphöra i förtid om förutsättningarna för det är uppfyllda. Förutsättningarna för en sådan mekanism ska undersökas i det följande.

Inget av regelverken innehåller någon fristående möjlighet att tillfälligt upphäva certifikat/auktorisation till följd av överträdelser enligt NIS2-direktivet. Detta innebär att en begäran om upphävande i stället skulle prövas enligt de ordinarie bestämmelserna i respektive regelverk. Detta talar enligt utredningen emot att en sanktion ska införas, givet att respektive regelverk inte har de övriga mekanismer som artikel 32.5 i NIS2-direktivet förutsätter. Inom ramen för eIDAS saknas möjligheten till tillfälliga upphävanden, där en *återkallelse* i stället gäller till dess att en status beviljats på nytt.[22] Genom att möjligheten till tillfälligt upphävande saknas[23] kan den aktuella sanktionen därmed inte heller återställas på NIS-tillsynsmyndighetens initiativ. Detta kan inte anses följa den systematik som artikel 32.5 förutsätter för att kunna tillämpas. Utredningen bedömer därför att

[19] Se artiklarna 6.24–27 och 13.4–5 respektive 24.2 i NIS2-direktivet.
[20] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.
[21] Se 4 § lagen (2016:561) jämte 4 § förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, respektive 2 § lagen (2021:553) jämte 3 § förordningen (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.
[22] Jfr artiklarna 3.16–17, 3.20, 17.4 g och 20.3 i eIDAS-förordningen. Se även 4 § lagen (2016:561) jämte 4 § i den anslutande förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.
[23] Ett arbete med att ta fram en ny eIDAS-förordning pågår för närvarande inom EU, och det är än så länge oklart om någon möjlighet till tillfälligt upphävande av status kommer att införas i den nya förordningen.

NIS2-direktivets koppling till eIDAS-regelverket inte ger skäl för att införa den aktuella sanktionen.

Avseende ECC har kommissionen givits rätt att komplettera direktivet genom att göra cybersäkerhetscertifiering obligatorisk för vissa verksamhetsutövare.[24] I dag är det frivilligt för aktörer att ansöka om sådan certifiering. För denna typ av certifikat finns möjlighet för den nationella tillsynsmyndigheten att begränsa, återkalla eller tillfälligt upphäva certifikat.[25] Här kan noteras att mekanismen ”tillfälligt upphäva” finns angiven, vilket ansluter till NIS2-direktivets aktuella begrepp och systematik. Detta gör enligt utredningen att den kan anses ha en närmare koppling till NIS2:s mekanismer än vad eIDAS har. Som tidigare konstaterats ska dock prövningen av så väl tillfälligt upphävande som återställande ske enligt andra bedömningskriterier än de som återfinns i NIS2-direktivet. När NIS2-tillsynsmyndigheten bedömer att det inte längre finns grund för sanktionen ska den upphöra. Det kommer dock vara upp till FMV att avgöra om förutsättningarna för att häva sanktionen är uppfyllda. Det saknas därmed garantier för att sanktionen kommer att upphävas, trots NIS2-tillsynsmyndighetens begäran om det. Som följd anser utredningen att inte heller denna systematik motsvarar vad som förutsätts enligt artikel 32.5. Inte heller kopplingen mellan NIS2 och ECC är därför tillräcklig för att utredningen ska föreslå ett genomförande av den aktuella sanktionen.

Utredningen har inte kunnat identifiera några andra certifieringar eller auktorisationer med tydlig koppling till NIS2 och som skulle kunna komma i fråga att angripa med sanktionen. Som följd anser utredningen att sanktionen inte skulle få avsedd verkan om den genomfördes. Mot denna bakgrund saknas det tillräckligt underlag för att föreslå att sanktionen ska genomföras i svensk rätt i detta skede.

[24] Artiklarna 24.2 och 38.2 i NIS2-direktivet.
[25] Artikel 58.7 e i cybersäkerhetsakten samt 2 och 7 §§ lagen (2021:553) jämte 3 § förordningen (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

9.5.6 Förbud att utöva ledningsfunktion

Allmänna överväganden

Utredningens bedömning: Det ska införas en möjlighet för tillsynsmyndigheten att ansöka hos domstol om att en person med ledningsansvar hos en väsentlig verksamhetsutövare ska förbjudas att utöva ledningsfunktioner där.

Ett sådant beslut ska kunna riktas mot den som är styrelseledamot, verkställande direktör eller ersättare för någon av dessa, eller på motsvarande sätt är befattningshavare enligt 3 § andra stycket lagen (2014:836) om näringsförbud.

Bolagsverket ska ansvara för att avregistrera en person med ett meddelat förbud och hindra en person med förbudssanktion från att registreras på nytt under förbudstiden. Om verksamhetsutövaren är en stiftelse ska den registreringsansvariga länsstyrelsen fullgöra motsvarande uppgifter i stället för Bolagsverket.

Enligt artikel 32.5 b NIS2-direktivet ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenhet att begära att relevanta organ eller domstolar, i enlighet med nationell rätt, inför ett tillfälligt förbud för varje fysisk person som på nivån för verkställande direktör eller juridiskt ombud har ledningsansvar i en väsentlig verksamhet att utöva ledningsfunktioner i den. Till skillnad från övriga sanktioner som riktar sig mot verksamhetsutövaren som juridisk person är denna sanktion riktad mot en fysisk person. Sanktionen är en yttersta åtgärd för att framtvinga ett visst agerande hos en väsentlig verksamhetsutövare genom att en fysisk person hålls ansvarig för en verksamhetsutövares överträdelser. Sanktionen har ett samband med de befogenheter motsvarande ledningspersoner förväntas ha för att kunna säkerställa verksamhetsutövarens regelefterlevnad (jfr artikel 32.6). Utredningen anser därför att sanktionen är central för systematiken i NIS2-direktivet. Utredningen bedömer dock att det bör vara synnerligen ovanligt att denna typ av sanktion behöver tillgripas av en tillsynsmyndighet. Den aktuella sanktionen behöver därmed införas, trots bedömningen att den bara kommer att tillgripas i extrema undantagsfall. Frågan är då hur en sådan sanktion ska utformas.

Sanktionen ska innebära ett tillfälligt förbud för en person att utöva ledningsansvar hos en verksamhetsutövare. Av detta följer enligt utredningens bedömning att förbudet endast ska träffa sådant arbete som innebär att ”utöva ledningsansvar” och därtill enbart hos den aktuella verksamhetsutövaren. Sanktionen behöver alltså inte medföra ett generellt förbud att verka i ledningsfunktioner hos andra verksamhetsutövare, eller i andra roller än ledningsfunktion hos den aktuella verksamhetsutövaren. Den ska därutöver kunna vara tillfällig och upphävas när avsedd effekt är uppnådd. Dessa aspekter behöver beaktas vid utformningen av sanktionen.

Jämförelse med liknande sanktioner

Utredningen kan konstatera att sanktionen till del påminner om ett näringsförbud enligt lagen (2014:836) om näringsförbud. I jämförelse med ett näringsförbud har sanktionen dock begränsad omfattning eftersom den inte utgör ett generellt förbud att utöva näringsverksamhet, utan ett specifikt förbud att utöva ledningsfunktion hos en viss väsentlig verksamhetsutövare. Därtill medför ett näringsförbud ett förbud mot att vara anställd i den verksamhet där överträdelsen skett, vilket inte följer av NIS2-direktivet. Dessa två faktorer gör att ett näringsförbud skiljer sig väsentligt mot de effekter den aktuella sanktionen syftar till att uppnå. Som följd kan näringsförbud inte anses överlappa med den tänkta sanktionen i en sådan utsträckning att det saknas skäl att införa NIS2-sanktionen. Denna bedömning ligger även i linje med regeringens uppfattningar rörande liknande sanktionstyper som har införts i svensk rätt.[26] Därutöver anser utredningen att sanktionen inte kan anses lika ingripande som ett näringsförbud, och därmed bör den kunna tillgripas vid lindrigare överträdelser än sådana som hade kunnat leda till näringsförbud.

Motsvarande sanktion återfinns i andra EU-rättsakter[27] som har genomförts i svensk rätt, exempelvis i lagen (2007:528) om värdepappersmarknaden och lagen (2004:297) om bank- och finansieringsrörelse, genom vilka en fysisk person kan hållas ansvarig för en juridisk

[26] Se till exempel prop. 2014/15:57 s. 45.
[27] Se till exempel artikel 67.2 d i Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG.

persons överträdelser av vissa regelverk. Utredningen uppmärksammar dock några större skillnader mellan dessa regelverk och NIS2.

Systematiken i de finansiella regelverken bygger på att verksamhetsutövaren bedriver tillståndspliktig verksamhet. Ett sådant tillstånd kan ytterst återkallas om verksamhetsutövaren inte tillser att förbudet verkställs. Det går även att rikta sanktioner mot andra ledningspersoner som på olika sätt bidragit till att ett förbud inte verkställts. För det andra utgör förbudssanktionen inom de finansiella regelverken sektorsspecifik lagstiftning. Sanktionen medför ett förbud som inte är begränsat till uppdrag inom ett specifikt bolag, utan omfattar i stället sådana uppdrag i alla bolag av den aktuella typen (exempelvis värdepappersinstitut eller värdepappersbolag). På det sättet är sanktionens räckvidd smalare än ett näringsförbud, men bredare än den sanktion som framgår av NIS2-direktivet. Därtill är NIS2-sanktionen tvärsektoriell och tar sikte på cybersäkerheten inom ett stort antal sektorer av olika slag.

Slutligen kan utredningen notera ett antal processuella överväganden. Den aktuella sanktionen beslutas enligt de finansiella regelverken genom sanktionsföreläggande. Förenklat innebär det att tillsynsmyndigheten (Finansinspektionen) utfärdar ett föreläggande mot en person i ett företags ledning, genom vilket personen förbjuds att vara verksam i företagsledningen. Personen kan välja att godta föreläggandet, och då gäller det godtagna föreläggandet som en lagakraftvunnen dom. Om personen motsätter sig föreläggandet kan tillsynsmyndigheten ansöka hos domstol om att sanktionen ska dömas ut. En sådan lösning innebär en kombination av ett snabbare förfarande (om ett föreläggande godtas) och möjligheten att tillvarata rättssäkerhetsaspekter genom en domstolsprövning i andra fall.[28] Att tillsynsmyndigheten getts möjlighet att besluta om sådana förelägganden förefaller dock till huvudsak ha motiverats utifrån att det rört sig om en tillsynsmyndighet med större vana av denna typ av beslut.[29] I fråga om NIS2 är utredningens förslag att det ska finnas elva tillsynsmyndigheter och argumentet kan därför enligt utredningens uppfattning endast få begränsad räckvidd.

Med dessa bedömningar som grund kan utredningen konstatera att det finns begränsad ledning att hämta från befintliga sanktioner vid utformningen av den nu aktuella sanktionen.

[28] Se prop. 2014/15:57 s. 59.
[29] Prop. 2014/15:57 s. 59.

Vilken personkrets ska kunna träffas av sanktionen?

Av artikel 32.5 b följer att sanktionen ska kunna träffa varje fysisk person som på nivån för verkställande direktör eller juridiskt ombud har ledningsansvar i den väsentliga verksamhetsutövaren. NIS2-direktivet definierar inte begreppen ”ledningsansvar” eller ”ledningsfunktioner”. Av systematiken i artikel 20 följer att det är verksamhetsutövarnas ledningsorgan som ska kunna hållas ansvariga för överträdelser av direktivet. Som utredningen funnit i avsnitt 7.2 anses ”ledningsorgan” i Sverige primärt omfatta styrelsen i ett aktiebolag.[30] Utredningen noterar att begreppen i artikel 20 och 32.5 b skiljer sig åt, och att kretsen avseende sanktionen kan uppfattas som snävare genom exemplifieringen med verkställande direktör, vilket skulle kunna utesluta styrelsen från kretsen. Det är oklart varför denna diskrepans finns i direktivet, men utredningen anser att det ligger närmare till hands att låta sanktionen träffa den bredare krets som avses i artikel 20. Genom att låta sanktionen träffa en bredare krets bedömer utredningen att den avsedda systematiken i artikel 20 kan upprätthållas. Utredningen anser mot samma bakgrund att kretsen även ska omfatta ersättare, till exempel suppleanter. Som följd ska den aktuella sanktionen i fråga om aktiebolag kunna tillämpas på styrelsen eller verkställande direktör samt deras ersättare, samt motsvarande i fråga om andra associationsrättsliga former. För att definiera personkretsen avseende andra associationsrättsliga former anser utredningen att samma krets ska användas i detta sammanhang som anges i 3 § andra stycket lagen (2014:836) om näringsförbud. En hänvisning till bestämmelsen bör därför föras in i den föreslagna lagen.

Utredningen anser att förbudet inte ska uppfattas som att det påverkar eventuella andra anställningsförhållanden som den förbudsdrabbade har, exempelvis att den utöver att vara styrelseledamot även är personalchef. Förbudssanktionen ska uppfattas som en begränsning i att utöva uppdraget som bolagsfunktionär (styrelseledamot, vd, ersättare eller motsvarande). Det utgör således inte ett förbud att fortsatt ha en anställning hos verksamhetsutövaren.

[30] Se prop. 2013/14:228 s. 166 f. och prop. 2014/15:57 s. 40 och 68.

Vad innebär förbudet?

För att kunna utforma sanktionen behöver en tolkning göras av begreppet ”utöva ledningsfunktion”. Utredningen anser att det bör omfatta det ansvar som följer av ett formellt ansvar, till exempel i egenskap av att vara styrelseledamot eller verkställande direktör i ett aktiebolag (se beskrivningen ovan av personkretsen). Förbudet ska avse en sådan funktionärs rätt att utöva sin formella behörighet i egenskap av funktionär, dvs. de rättigheter som tillkommer denne genom sin befattning.[31]

Sanktionens utformning

Utredningens förslag: Om ett föreläggande inte följts får tillsynsmyndigheten ingripa mot en person som ingår i verksamhetsutövarens ledning. Ingripande sker genom att tillsynsmyndigheten ansöker hos allmän förvaltningsdomstol om att en person inte ska få vara befattningshavare hos en viss verksamhetsutövare (förbud).

Ett sådant ingripande får riktas mot den som är befattningshavare enligt 3 § andra stycket lagen (2014:836) om näringsförbud.

Ett ingripande får endast göras om överträdelsen som ligger till grund för föreläggandet är allvarlig och om personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Utredningen har övervägt två olika metoder för ingripande, men väljer att endast lämna förslag om att sanktionen utformas i enlighet med den ena metoden. Det lämnade förslaget innebär en möjlighet för tillsynsmyndigheten att ansöka om att en persons status som funktionär hos verksamhetsutövaren ska upphävas.

Den första metoden innebär att funktionären ska begränsas i sina befogenheter i fråga om vad den får göra hos verksamhetsutövaren. Funktionären får fortsatt vara aktiv inom bolaget och exempelvis utöva sina åtaganden i egenskap av att vara funktionär, men inte i sådana angelägenheter som faller inom ramen för NIS2. Med sådana angelägenheter avses alla former av påverkan på verksamhetsutövarens skyldigheter att vidta riskhanteringsåtgärder eller incidentrap-

[31] Sådant ansvar i ett aktiebolag följer av 8 kap. 4 § aktiebolagslagen (2005:551) avseende styrelseledamöter och av 8 kap. 28 och 29 §§ samma lag avseende verkställande direktör och vice verkställande direktör.

portering. Ett exempel på innebörden av en sådan begränsning kan vara att en styrelseledamot inte får delta i beslut som rör fastställande av strategier för riskanalys. Frågan är hur sådan befogenhetsinskränkning skulle kunna verkställas och av vem. Genom att ingripandet inte påverkar funktionärens formella behörighet finns betydande begränsningar i verksamhetsutövarens möjligheter att hindra funktionären från att delta i sådana beslut. Den förbudsdrabbade funktionären skulle fortfarande vara formellt behörig att delta i alla former av beslut, och i vissa fall att teckna verksamhetsutövarens firma. Detta medför även att exempelvis en styrelseledamot i ett aktiebolag fortfarande är skyldig att fullgöra de förpliktelser som följer av aktiebolagslagen, och kan hållas ansvarig för överträdelser och underlåtelser (exempelvis enligt 25 kap. 18 § aktiebolagslagen). Att en förbudsdrabbad funktionär skulle fortsätta att utöva sin behörighet bör enligt utredningen därför som utgångspunkt inte kunna leda till att sanktioner riktas mot verksamhetsutövaren. Som följd bör incitament i stället finnas för att funktionären ska välja att avstå från att utöva sin formella behörighet i NIS2-frågor. Utredningen anser att sådana incitament kan vara svåra att skapa och därtill svåra att kontrollera efterlevnaden av. Som följd finns stora nackdelar med denna typ av system.

Den andra metoden får till följd att en bolagsfunktionär ska avregistreras från Bolagsverkets företagsregister. Ett sådant ingripande medför att funktionären blir av med sin formella behörighet genom att avregistreras. Genom avregistreringen görs funktionären således omedelbart obehörig att utöva ledningsfunktioner inom verksamhetsutövaren, och inte bara i NIS2-frågor. Detta är en mycket ingripande åtgärd som får omedelbara associationsrättsliga effekter, vars konsekvenser blir beroende på vilken typ av juridisk person det rör sig om och förhållandena i det enskilda fallet.

Ett sådant beslut om avregistrering går inte att tidsbegränsa eller återkalla. Om funktionären ska registreras på nytt krävs således att verksamhetsutövaren ansöker om sådan registrering till Bolagsverket. Detta går utöver NIS2-direktivets krav, men utredningen har inte kunnat identifiera några alternativa lösningar som kan uppnå samma effekt men med mindre ingripande medel. NIS2-direktivet är därtill ett minimidirektiv, varför Sverige inte är förhindrat att införa mer ingripande regler.

Att ett aktiebolag förlorar en styrelseledamot kan i förlängningen innebära att reglerna om tvångslikvidation aktualiseras (25 kap. 11 § aktiebolagslagen). Motsvarande bestämmelser gäller även för andra associationsrättsliga former, exempelvis om ett handelsbolag har reducerats till att bestå av en bolagsman (jfr 2 kap. 28 § lagen [1980:1102] om handelsbolag och enkla bolag). Ett ingripande kan således få mycket långtgående konsekvenser för verksamhetsutövaren. Det får därutöver stora konsekvenser för den enskilde funktionären. Dessa långtgående konsekvenser talar enligt utredningens mening med styrka för att rättssäkerhetsaspekter behöver väga tungt vid tillämpandet av denna sanktion, vilket behöver beaktas i det följande.

Särskilda förutsättningar för att sanktionen ska komma i fråga

Av artikel 32.5 NIS2-direktivet följer att sanktionen ska kunna användas om andra sanktioner är ineffektiva, och verksamhetsutövaren har förelagts att vidta åtgärder inom viss tidsfrist men att detta inte har skett. I svenska förhållanden motsvarar detta att ett föreläggande inte följts, och övriga ingripanden är ineffektiva. Det senare ledet väcker frågan om övriga sanktioner måste ha prövats först och konstaterats vara ineffektiva, eller om det bör räcka med att tillsynsmyndigheten har skäl att anta att andra sanktioner är ineffektiva. Det följer av sanktionens systematik att tillsynsmyndigheterna inte kan använda sig av förbudet som en inledande åtgärd, utan det måste föregås av åtminstone ett föreläggande. Först när ett sådan inte följts kan förbudssanktionen övervägas. Den avsedda effekten är att verksamhetsutövaren ska följa ett föreläggande. Övriga sanktioner (offentliggörande av överträdelse, anmärkning och sanktionsavgift) har till sin natur en begränsat framåtsyftande effekt. Deras effekter utgör därför inte typiskt sett desamma som uppnås genom föreläggande eller förbud. Utredningen bedömer därför att det är tillräckligt att tillsynsmyndigheten har anledning att anta att andra sanktioner inte är effektiva för att uppnå den avsedda effekten. Att övriga sanktioner inte måste ha använts behöver dock balanseras på annat sätt för att tillgodose rättssäkerhetsintressen.

Förbudssanktionen kan bara bli aktuell om det går att visa att det är en ledningsperson som är orsaken till att föreläggandet inte följts (se nedan om det subjektiva rekvisitet). Det rör sig således om en

sanktion som tar sikte på ett unikt problem som bara borde kunna uppstå i undantagsfall. Sanktionen kan förväntas få stora konsekvenser för både den enskilde och den väsentliga verksamhetsutövaren som behöver hantera de organisatoriska följderna av förbudet. Utredningens utgångspunkt är därför att ingripanden mot enskilda individer endast bör förekomma i fall av allvarliga överträdelser.

Till följd av sanktionens straffrättsliga karaktär bör den därtill förenas med ett subjektivt rekvisit som förutsättning för att få användas.[32] En sådan utformning ligger därtill i linje med NIS2-direktivets krav på lämpliga rättssäkerhetsgarantier vid tillämpningen (artikel 32.5). En förutsättning för att sanktionen ska kunna tillgripas ska därför vara att individen med ledningsansvar på något vis har visat uppsåt eller grov oaktsamhet till den överträdelse som är i fråga. Det kan enligt utredningens uppfattning till exempel röra sig om att den verkställande direktören underlåtit att tillse att det finns en organisation för den incidentrapportering som förutsätts enligt NIS2-direktivets bestämmelser. Det kan också röra sig om medvetna risktaganden i fråga om vilka riskhanteringsåtgärder som vidtagits i relation till exempelvis samhälleliga konsekvenser, eller om uppföljning inte har skett av verksamhetsutövarens efterlevnad av NIS2-direktivets bestämmelser.

Förfarandet för att ett förbud ska meddelas

Utredningens förslag: Ett beslut om förbud fattas av förvaltningsrätten på ansökan från tillsynsmyndigheten. En ansökan ska innehålla uppgifter om

1. den person som ansökan avser,
2. verksamhetsutövaren,
3. överträdelsen och de omständigheter som behövs för att kännetecknа den, och
4. de bestämmelser som är tillämpliga på överträdelsen.

Ett förbud ska tidsbegränsas till lägst ett år och högst tre år och ska upphävas omedelbart när föreläggandet har följts.

[32] Se till exempel prop. 2014/15:57 s. 42 och prop. 2016/17:173 s. 368 f.

Förbud får inte riktas mot offentliga verksamhetsutövare.

Ansökan ska prövas skyndsamt av domstolen.

Förvaltningsrätten ska pröva om ett beslutat förbud ska upphävas om tillsynsmyndigheten eller den enskilde begär det, eller om det annars finns skäl för det. Den enskilde ska upplysas om sin rätt att begära att ett förbud ska upphävas.

Om tillsynsmyndigheten bedömer att det inte längre finns förutsättningar för förbudet ska den omedelbart begära att förvaltningsrätten ska upphäva förbudet.

När ett beslut om förbud har fått laga kraft ska domstolen underrätta Bolagsverket och verksamhetsutövaren om beslutet och dess innehåll. Om verksamhetsutövaren är en stiftelse ska den länsstyrelse som är registreringsmyndighet för stiftelsen underrättas i stället för Bolagsverket.

Domstolen ska skicka motsvarande underrättelser om ett sådant förbud upphävs.

När Bolagsverket eller en länsstyrelse som är registreringsmyndighet har fått en underrättelse om förbud ska de avregistrera personen som befattningshavare hos verksamhetsutövaren i det aktuella registret.

Bolagsverket eller en länsstyrelse som är registreringsmyndighet ska säkerställa att personen inte registreras på nytt som befattningshavare hos verksamhetsutövaren under förbudstiden.

Förbudet får endast meddelas av domstol

Utredningen har övervägt om förbudssanktionen ska få meddelas av tillsynsmyndigheten, eller om ett sådant förbud lämpligen bör meddelas av domstol. I tidigare lagstiftningsärenden har framhållits att kännbara ingripanden mot fysiska personer bör beslutas av domstol, medan det kan finnas ett större utrymme för administrativt bestämda påföljder om påföljden träffar ett företag.[33] Givet den nu aktuella sanktionens straffrättsliga karaktär och att den, till skillnad från övriga föreslagna sanktioner, riktar sig mot en enskild individ anser utredningen att rättssäkerhetsskäl talar starkt för att prövningen inte

[33] Se till exempel prop. 2004/05:142 s. 47.

ska få göras av en förvaltningsmyndighet. Utredningen bedömer även att denna slutsats följer svensk rättstradition.[34]

Som tidigare nämnts förekommer dock i liknande regelverk att tillsynsmyndigheten får besluta om sanktionsföreläggande avseende denna sanktionstyp, men i dessa fall finns det endast en tillsynsmyndighet. Utredningen bedömer att detta skiljer sig väsentligt från den nu föreslagna lösningen med elva tillsynsmyndigheter för NIS2. Utredningen anser därför att det inte finns skäl att frångå utgångspunkten att förbudet ska beslutas av domstol som första instans. För att åstadkomma en enhetlig, rättssäker och effektiv reglering bör prövningen göras av domstol efter ansökan av tillsynsmyndigheten. Ett meddelat förbud ska även kunna upphävas efter ansökan från tillsynsmyndigheten eller den enskilde.

I fråga om vilken domstol som ska göra denna prövning finner utredningen att både allmän domstol och allmän förvaltningsdomstol kan övervägas. Vad gäller övrig prövning enligt den föreslagna lagen föreslås att den ska ske i allmän förvaltningsdomstol. Utredningen finner att det finns starkt vägande skäl som talar emot att prövningen av samma otillåtna agerande (verksamhetsutövarens överträdelse) ska kunna ske i två typer av domstolar. Att samma typ av domstol ska handlägga alla överträdelser enligt den föreslagna lagen skapar dessutom samordningsfördelar inom domstolarna. Detta talar för att handläggningen ska ske i allmän förvaltningsdomstol. Därtill kan den enskildes behov av muntlig förhandling tillvaratas även i förvaltningsdomstol trots att förfarandet som huvudregel är skriftligt. Vidare talar möjligheterna till aktiv processledning för att den enskildes rättssäkerhetsintressen tillgodoses.[35] Mot denna bakgrund anser utredningen att prövningen om sanktionen ska dömas ut ska göras av allmän förvaltningsdomstol.

Sanktionen ska begränsas i tid

Av NIS2-direktivet (artikel 35.2) följer vidare att den aktuella sanktionen ska vara tillfällig och endast tillämpas till dess att de sanktionsgrundande bristerna eller kraven är åtgärdade. Av detta följer dels att ett sanktionsbeslut behöver begränsas i tid, dels att det ska

[34] Jfr prop. 2014/15:58 s. 57.
[35] Jfr 8 och 9 §§ förvaltningsprocesslagen (1971:291).

upphävas när skäl för sanktionen inte längre föreligger, även innan det att tidsbegränsningen uppnåtts. Detta skiljer sig från hur andra genomföranden av motsvarande EU-rättsligt grundade sanktioner har skett, där motsvarande sanktioner enbart förenats med en förutbestämd tidsbegränsning.[36] I flera av dessa fall har tidsbegränsningen satts till samma spann som gäller i fråga om näringsförbud, tre till tio år.[37] Som följd får denna åtgärd anses ha en framåtsyftande verkan. Utredningen bedömer att motsvarande tid kan vara vägledande i fråga om NIS2-sanktionen, men anser att den nu aktuella sanktionen i princip saknar framåtsyftande verkan och är av en betydligt mer tillfällig art genom att den är kopplad till att ett föreläggande ska följas. Detta ger skäl att bestämma sanktionens omfattning till lägre än vad som gäller i andra fall. Utredningen anser att förbudet ska tidsbegränsas. Som redogjorts för ovan kan dock inte verkställighetsåtgärden (avregistrering) tidsbegränsas, vilket skulle kunna anses tala emot behovet av tidsbegränsning av sådana beslut. Utredningen bedömer dock att det ändå finns skäl att kunna ange att ett sådant förbud ska gälla under viss tid. Att en funktionär avregistreras innebär nämligen inte något hinder mot att verksamhetsutövaren begär att funktionären ska registreras på nytt hos Bolagsverket. Ett beslut om förbud bör därför innebära att funktionären avregistreras och inte får registreras på nytt så länge förbudet gäller. Enligt utredningens uppfattning bör denna typ av förbud kunna tidsbestämmas till mellan ett och tre år. Som tidigare anförts ska den dock upphävas omedelbart när syftet med sanktionen har uppnåtts.

Sanktionen ska inte få användas mot offentliga verksamhetsutövare

Enligt artikel 32.5 NIS-direktivet ska den aktuella sanktionen inte kunna tillämpas på offentliga verksamhetsutövare. Utredningen delar denna uppfattning varför en sådan begränsning ska anges i bestämmelsens tillämpningsområde.

[36] Se till exempel 15 kap. 1 a § fjärde stycket lagen (2004:297) om bank- och finansieringsrörelse och 18 kap. 2 a § försäkringsrörelselagen (2010:2043).
[37] Se 10 § första stycket lagen (2014:836) om näringsförbud.

Ansökningsprocessen, handläggning och upphävande av ett beslut

Utredningen anser att processen ska inledas genom att tillsynsmyndigheten lämnar in en ansökan. Ansökan ska lämnas in till den domstol inom vars domsaga tillsynsmyndigheten är belägen. Av ansökan ska ett antal uppgifter framgå. Ledning för vilka dessa uppgifter bör vara kan hämtas i rättegångsbalkens regler om strafföreläggande (46 kap. 6 §) och anpassas för att omfatta de uppgifter som krävs för den nu aktuella prövningen. Domstolen ska pröva om det föreligger förutsättningar för att meddela ett förbud. Ett beslut ska som tidigare nämnts upphävas omedelbart när det inte längre finns skäl för det, t.ex. för att föreläggandet har följts. Det bör därför åvila tillsynsmyndigheten att omedelbart meddela domstolen när detta har skett. Vidare bör även den enskilde ha möjlighet att begära att förbudet ska upphävas. Vid sådan handläggning finns möjlighet att begära muntlig förhandling enligt 9 § förvaltningsprocesslagen (1971:291). Mot bakgrund av förbudets tillfälliga art anser utredningen att så väl beslut om förbud samt upphävande av det bör behandlas med förtur. Detta motiveras även av syftet med förbudet. En överträdelse som inte upphör riskerar att leda till fler och allvarligare konsekvenser än om den åtgärdas snabbt. Om en befattningshavares agerande är skälet till att ett föreläggande (som syftar till att få överträdelsen att upphöra) inte följs måste förbudssanktionen kunna handläggas skyndsamt för att få avsedd effekt och minska konsekvenserna av överträdelsen.

Verkställigheten av ett beslut

Effekten av ett beslut om förbud ska vara att personen avregistreras som funktionär hos verksamhetsutövaren ur aktuellt register, och inte får registreras på nytt under tiden beslutet gäller. Beslutet bör därför få verkställas först när det fått laga kraft. Domstolen ska därför underrätta Bolagsverket om att ett beslut fått laga kraft för att verkställighet (avregistrering) ska kunna ske. För det fall verksamhetsutövaren är en stiftelse ska registreringsansvarig länsstyrelse underrättas i stället för Bolagsverket, samt fullgöra motsvarande skyldigheter.[38] Även verksamhetsutövaren ska underrättas om att ett beslut fått laga kraft.

[38] Jfr 3 § andra stycket 8 lagen (2014:836) om näringsförbud samt 10 kap. 1 § och 9 kap. 1 § stiftelselagen (1994:1220) jämte 4 a § stiftelseförordningen (1995:1280).

Utredningen noterar att det inom andra regelverk inte verkar finnas någon uttrycklig bestämmelse som anger att effekten av en sådan underrättelse till Bolagsverket är att avregistrering ska ske.[39] Att en sådan avregistrering ska ske av Bolagsverket respektive länsstyrelsen bör enligt utredningens mening anges uttryckligen. Bolagsverket respektive länsstyrelsen ska även tillse att den enskilde inte får registreras på nytt som funktionär hos verksamhetsutövaren under tiden ett beslut är giltigt. På motsvarande sätt ska både Bolagsverket (alternativt länsstyrelsen) och verksamhetsutövaren underrättas om ett förbud upphävs.

9.5.7 Anmärkning

Utredningens bedömning: Det ska införas en möjlighet för tillsynsmyndigheten att meddela anmärkningar mot verksamhetsutövare som har överträtt den föreslagna cybersäkerhetslagen eller föreskrifter som har meddelats med stöd av den lagen.

Utredningens förslag: Om tillsynsmyndigheten inte finner skäl att ingripa på något annat sätt ska den i stället meddela verksamhetsutövaren en anmärkning.

Enligt artikel 32.4 a och 33.4 a NIS2-direktivet ska tillsynsmyndigheterna ha möjlighet att utfärda varningar om verksamhetsutövares överträdelser av direktivets skyldigheter. Motsvarande bestämmelser saknas i dag. Utredningen kan dock konstatera att liknande system finns i svensk rätt.[40] Vidare kan utredningen se att en sådan sanktion kan vara av värde för tillsynsmyndigheterna i deras uppdrag och för NIS2-regleringens efterlevnad i stort. Det kan exempelvis vara relevant för situationen när en inträffad överträdelse inte bedöms vara av sådan art eller svårighetsgrad att något av de andra ingripandena kan komma i fråga. Det skulle leda till att tillsynsmyndigheten inte kan vidta någon åtgärd mot överträdelsen. Utredningen anser att en sådan ordning inte är önskvärd, och att det i stället ska vara obligatoriskt för tillsynsmyndigheten att meddela en anmärkning om något annat ingripande inte görs, givet att den inte valt att avstå från att

[39] Se till exempel 5 kap. 1 § förordningen (2007:572) om värdepappersmarknaden.
[40] Se exempelvis lagen (2005:405) om försäkringsförmedling.

ingripa.[41] Detta leder till att en överträdelse av NIS2-regleringen i princip inte kan leda till att en verksamhetsutövare undgår ingripande, men valet av ingripandeåtgärd avgörs av hur allvarlig överträdelsen är och anmärkning utgör den lindrigaste åtgärden.

Varning som sanktion förekommer på flera håll i svensk rätt, ofta med den alternativa möjligheten att meddela anmärkning.[42] Sanktionen används då huvudsakligen som ett sätt att ingripa mot en aktör som bedriver tillståndspliktig verksamhet, men där återkallelse av tillståndet bedöms vara oproportionerlig i relation till den aktuella överträdelsen. Utredningen bedömer att varningssanktionen som anges i NIS2-direktivet har större likheter med hur anmärkning används inom svensk rätt. Som följd föreslås att begreppet anmärkning ska användas även i den föreslagna cybersäkerhetslagen.

9.6 Sanktionsavgifter

9.6.1 För vilka överträdelser ska sanktionsavgifter införas och när får sanktionsavgift tas ut?

Utredningens bedömning: Sanktionsavgift får tas ut av en verksamhetsutövare som har åsidosatt sina skyldigheter enligt cybersäkerhetslagens bestämmelser om att utse företrädare, anmälningsplikt, riskhanteringsåtgärder, utbildning och incidentrapportering (1 kap. 6 §, 2 kap. 2 § och 3 kap. 1 och 3 §§ samt 5–7 §§), eller enligt föreskrifter som meddelats med stöd av dessa bestämmelser.

Enligt artikel 34.2 NIS2-direktivet ska sanktionsavgifter påföras utöver någon av de åtgärder som anges i artikel 32.4 a–h, 32.5 eller 33.4 a–g. Utredningens tolkning av bestämmelsen är att om något av de tillgängliga sanktionsverktygen tillgrips till följd av en verksamhetsutövares överträdelse av skyldigheterna ska tillsynsmyndigheten även kunna besluta om sanktionsavgift. Utredningen anser även att sanktionsavgift ska kunna tillämpas trots att någon av de övriga sanktionerna inte har använts. Den nuvarande regleringen i NIS-lagen (29 §) innebär att det är tillsynsmyndigheten som fattar beslut

[41] Om den avstått från att ingripa ska anmärkning inte meddelas (se avsnitt 9.3.1 ovan).
[42] Se exempelvis 15 kap. 1 § andra stycket lagen (2004:297) om bank- och finansieringsrörelse och 25 kap. 1 § lagen (2007:528) om värdepappersmarknaden.

om sanktionsavgift och att tillsynsmyndigheten ska fatta sådant beslut till följd av att en verksamhetsutövare inte följt lagens eller anslutande författningsbestämmelser. Ordningen bygger på ett system med strikt ansvar, dvs. att sanktionsavgift ska tas ut oavsett om överträdelsen skett av oaktsamhet eller uppsåt. Utredningen noterar i detta sammanhang att sådant strikt ansvar nyligen underkänts av EU-domstolen i fråga om GDPR-överträdelser.[43] Utredningen bedömer dock att medlemsstaternas handlingsutrymme är större i fråga om direktiv än förordningar, med följden att ett system med strikt ansvar i fråga om sanktionsavgifter kan föreslås avseende NIS2-direktivets genomförande i svensk rätt. Vidare anser utredningen att det, precis som i fråga om överträdelser av nuvarande NIS-lagen,[44] finns en stark presumtion för att överträdelser av NIS2-direktivet sker av oaktsamhet eller uppsåtligen. Det föreslagna systemet bör därför bygga på strikt ansvar. En sådan systematik kräver dock ventiler för att kunna fånga upp överträdelser som skett utan vållande. Utredningen föreslår därför att tillsynsmyndigheten i varje enskilt fall ska avgöra om sanktionsavgift ska tas ut.

Att sanktionsavgift ska kunna användas medför dock ett krav på att det ska vara enkelt för verksamhetsutövaren att förstå hur den ska agera för att undvika att drabbas av sanktionen, och motsatsvis att det ska vara lätt för tillsynsmyndigheten att konstatera att en överträdelse har skett.[45] Utredningen bedömer att dessa villkor kan anses uppfyllda genom de föreslagna kraven om riskhanteringsåtgärder respektive incidentrapportering. I fråga om anmälningsplikten bedömer utredningen att det i många fall kommer att vara lätt för både verksamhetsutövare och tillsynsmyndighet att avgöra om en viss verksamhet omfattas av NIS2-direktivets bestämmelser. Detta kan exempelvis anses gälla för en verksamhetsutövare som anmält till PTS att den erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster.[46] I sådana fall följer även anmälningsskyldighet enligt NIS2-direktivet. På motsvarande sätt bör det inte råda någon tvekan kring vilka verksamhetsutövare som är att bedöma som offentliga. Utredningen bedömer dock att samma typ av enkla bedömningar inte nödvändigtvis

[43] Se EU-domstolens domar av den 5 december 2023 i mål nr C-683/21 (ECLI:EU:C:2023:949) och C-807/21 (ECLI:EU:C:2023:950).
[44] Prop. 2017/18:205 s. 68 ff.
[45] Se prop. 2007/08 :107 s. 18 f. och prop. 2015/16:118 s. 17 f.
[46] Jfr 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation.

gör sig gällande inom alla de sektorer som träffas av NIS2-direktivet. Det kan därför med fog ifrågasättas om det är försvarligt att införa ett system där sanktionsavgift ska tas ut för samtliga överträdelser, trots att sådana inte alltid är enkla för den enskilde att förutse, eller för tillsynsmyndigheten att konstatera. Utredningen bedömer att en sådan ordning skulle riskera att underminera sanktionsavgiftens legitimitet. Detta kan lösas på flera sätt.

Systemet med obligatorisk sanktionsavgift skulle kunna överföras från NIS-lagen, men då skulle det mot bakgrund av tolkningarna ovan behöva införas begränsningar kring vilka överträdelser som ska kunna leda till sanktionsavgift. Detta hade kunnat vara en tilltalande lösning genom att exkludera exempelvis anmälningsplikten som en sanktionsavgiftsgrundande överträdelse. Som utredningen bedömt ovan finns dock ett antal överträdelser av anmälningsplikten som är lätta att förutse och konstatera. Att inte kunna ta ut sanktionsavgift för dessa överträdelser framstår därför inte som en tilltalande lösning. Som följd anser utredningen att tillsynsmyndigheten förvisso ska kunna ta ut sanktionsavgifter vid samtliga typer av överträdelser av lagen, men att den inte ska vara skyldig att meddela sanktionsavgifter. Detta medför att tillsynsmyndigheten får avgöra i varje enskilt fall om förutsättningarna för att ta ut sanktionsavgift är uppfyllda. Av detta följer även att en tillsynsmyndighet inte ska ta ut en sanktionsavgift av en verksamhetsutövare som inte anmält sig, men där det varit oklart om verksamhetsutövaren varit anmälningspliktig. Tolkningsutrymmet för vilka som omfattas av anmälningsplikt bör kunna minska när tillsynsmyndigheten har publicerat vägledning i fråga om sektorsbeskrivningarna (se avsnitt 5.2.12).

9.6.2 Sanktionsavgiftens storlek ska förändras

Utredningens bedömning: Sanktionsavgiften för väsentliga verksamhetsutövare ska bestämmas till lägst 5 000 kronor och högst till det högsta av:

1. 2 procent av den väsentliga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 10 000 000 euro.

Sanktionsavgiften för viktiga verksamhetsutövare ska bestämmas till lägst 5 000 kronor och högst till det högsta av:

1. 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 7 000 000 euro.

Sanktionsavgiften för offentliga verksamhetsutövare ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

När sanktionsavgiftens storlek bestäms ska tillsynsmyndigheten särskilt beakta de omständigheter som följer av 5 kap. 3–5 §§ i den föreslagna cybersäkerhetslagen.

Av NIS2-direktivet följer en skyldighet för medlemsstaterna att säkerställa att de administrativa sanktionsavgifter som påförs verksamhetsutövare med stöd av direktivet är effektiva, proportionerliga och avskräckande med beaktande av omständigheterna i varje enskilt fall.[47] Skyldigheterna i den föreslagna cybersäkerhetslagen kommer att träffa både offentliga och privata verksamhetsutövare. Verksamhetsutövarnas storlek och ekonomiska förutsättningar kommer som följd att skilja sig åt beroende på vilken aktörstyp och sektor den är verksam inom. Förutsättningarna kommer även att kunna skilja sig mellan aktörer inom samma sektor. Som följd behöver sanktionsavgifternas storlek kunna anpassas för att i varje enskilt fall anses effektiva, proportionerliga och avskräckande.

Av NIS-direktivet följde inte några beloppsgränser för medlemsstaterna att förhålla sig till vid genomförandet av direktivet. Som följd ska sanktionsavgifter enligt NIS-lagen bestämmas inom beloppsintervallet 5 000–10 000 000 kronor.

NIS2-direktivet anger inte något minimibelopp för sanktionsavgifternas storlek. Det lägsta beloppet för sanktionsavgift motsvarar vad som i dag utgör lägsta belopp vid åläggande av företagsbot, vilket även var vägledande för NIS-utredningens förslag.[48] Storleken på företagsboten har sedan dess ändrats avseende maximibelopp (höjt från 10 miljoner kronor till 500 miljoner kronor), men minimibeloppet har lämnats oförändrat.[49] Utredningen har övervägt om det

[47] Se artikel 32.1, 33.1 och 34.1 samt skäl 132 NIS2-direktivet.
[48] Se SOU 2017:36 s. 190 ff.
[49] 36 kap. 8 § andra stycket brottsbalken, se vidare prop. 2018/19:164.

finns skäl att förändra denna lägstanivå i fråga om överträdelser av NIS2-direktivet, men inte funnit några sådana skäl. Som följd bör lägstanivån för sanktionsavgift även fortsättningsvis vara 5 000 kronor.

Avseende maximinivån för sanktionernas storlek så inför NIS2-direktivet två olika beräkningsgrunder och belopp, där valet av beräkningsgrund avgörs av om verksamhetsutövaren i fråga är väsentlig (artikel 34.4) eller viktig (artikel 34.5). Maximibeloppen är avsevärt högre än vad som gäller i dag.

För väsentliga verksamhetsutövare ska takbeloppet för sanktionsavgiften uppgå till det högsta alternativet av:

- 10 000 000 euro, eller
- 2,0 procent av den totala globala årsomsättningen under föregående räkenskapsår.

För viktiga verksamhetsutövare ska motsvarande belopp uppgå till det högsta alternativet av:

- 7 000 000 euro, eller
- 1,4 procent av den totala globala årsomsättningen under föregående räkenskapsår.

Utredningen bedömer att maximinivån för sanktionsavgifter åtminstone behöver höjas till en nivå som är i paritet med de som anges i NIS2-direktivet för att Sverige ska kunna anses ha implementerat direktivet fullt ut. Sådana maximibelopp skapar därtill stor handlingsfrihet för tillsynsmyndigheterna att i varje enskilt fall avgöra vilken nivå på sanktionsavgiften som krävs för att uppnå syftet med den. Det går därutöver att resonera kring om maximinivåerna borde sättas ännu högre för att uppnå avsedd effekt. Utredningen har dock inga uppgifter som tyder på att de i direktivet angivna maximinivåerna skulle vara otillräckliga för de största aktörerna som träffas av regleringen. Maximibeloppen i NIS2-direktivet framstår därför som väl avvägda för att kunna bli kännbara även för aktörer med stora ekonomiska resurser. Att överföra de i NIS2-direktivet angivna nivåerna i svensk rätt får vidare antas bidra till att sanktionssystemet får liknande utformning inom EU. Som följd bör de aktuella maximibeloppen anges i förslaget till ny cybersäkerhetslag. När storleken på

en sanktionsavgift ska bestämmas ska de omständigheter som framgår av avsnitt 9.4.2 beaktas särskilt.

Av artikel 34.7 NIS2-direktivet följer att medlemsstaterna får välja om och i vilken utsträckning sanktionsavgifter ska kunna påföras offentliga verksamhetsutövare. Utredningen bedömer att det är påkallat att införa sanktionsavgifter för sådana aktörer, men att det inte är motiverat att ha ett lika högt maximibelopp som gäller för andra verksamhetsutövare. De offentliga verksamhetsutövarna kan förväntas styras av andra målsättningar än att göra vinst eller göra besparingar på bekostnad av sin säkerhet.[50] Även en lägre satt maximinivå för dessa sanktionsavgifter bör kunna få avsedd effekt. Inom andra områden har motsvarande maximinivåer satts till 10 miljoner kronor.[51] Utredningen finner denna nivå som lämplig och ändamålsenlig även för att uppnå de i NIS2-direktivet angivna syftena för de offentliga verksamhetsutövarna. Som följd ska en sådan maximinivå framgå av tillämpningsbestämmelsen.

9.6.3 Hinder mot att ta ut sanktionsavgift

Utredningens bedömning: Tillsynsmyndigheten får inte besluta om sanktionsavgift om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Tillsynsmyndigheten får inte heller besluta om sanktionsavgift för samma överträdelse som lett till att verksamhetsutövaren har påförts en sanktionsavgift enligt Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

I avsnitt 9.3.1 ovan har dubbelprövningsförbudet beskrivits. Det kan även anses innefatta förbud mot att bli påförd både straff och sanktionsavgift, eller sanktionsavgift och vite.[52] I en situation där ett vite

[50] Se prop. 2020/21:94 s. 103, jfr prop. 2017/18:232 s. 326.
[51] Se 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och 7 kap. 4 § säkerhetsskyddslagen (2018:585).
[52] Se motsvarande bedömningar i tidigare lagstiftningsärenden, exempelvis prop. 2007/08:107 s. 24, prop. 2012/13:143 s. 69 och prop. 2016/17:22 s. 133.

har dömts ut ska därför inte en sanktionsavgift kunna tas ut för samma händelse som låg till grund för vitet. På motsvarande sätt ska inte en sanktionsavgift få beslutas om den aktuella händelsen även ligger till grund för en ansökan om utdömande av vite.[53] Detta motsvarar vad som gäller enligt nuvarande NIS-lagen (33 §). Utredningen anser att bestämmelsen bör överföras i sin nuvarande form till den nya lagen.

Om den myndighet som utgör tillsynsmyndighet enligt dataskyddsförordningen (i Sverige, IMY)[54] har påfört sanktionsavgift enligt dataskyddsförordningen får inte en NIS2-tillsynsmyndighet påföra sanktionsavgift för samma överträdelse. Denna bestämmelse saknar motsvarighet i NIS-direktivet och utredningen anser att en sådan bestämmelse bör tas in i den nya lagen. Det bör noteras att det nyss sagda inte medför något hinder för NIS2-tillsynsmyndigheten att besluta någon av de andra sanktionerna än sanktionsavgift.[55]

9.6.4 Betalning, verkställighet och preskription

Utredningens bedömning: En sanktionsavgift får endast tas ut om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum. Beslut om sanktionsavgift ska delges.

Sanktionsavgiften ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning ska verkställighet få ske enligt utsökningsbalken. Sanktionsavgift tillfaller staten.

En beslutad sanktionsavgift ska falla bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

[53] Jfr prop. 2016/17:22 s. 228 och prop. 2017/18:205 s. 72 f.
[54] Jfr lagen (2018:218) och 3 § förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[55] Se artikel 35.2 NIS2-direktivet.

Bestämmelser kring förfarandet vid beslut om sanktionsavgift finns i dag i 34–36 §§ NIS-lagen. Dessa kompletterar de allmänna reglerna i förvaltningslagen (2017:900) om vad som krävs för att en förvaltningsmyndighet ska kunna fatta beslut, till exempel i fråga om kommunikation (25 §), beslutsfattande (28 §), dokumentation (31 §) och motivering av beslut (32 §). Utredningen har inte funnit skäl att föreslå några ändringar till de nuvarande bestämmelserna. Som följd bör de existerande bestämmelserna i NIS-lagen överföras även till den nya lagen.

9.7 Omedelbar verkställighet av förelägganden

Utredningens bedömning: Tillsynsmyndigheten ska få bestämma att ett beslut om föreläggande ska gälla omedelbart.

Enligt 38 § NIS-lagen kan en tillsynsmyndighet besluta om att ett föreläggande enligt lagen ska gälla omedelbart. Sådana regler återfinns även i 35 § tredje stycket förvaltningslagen (2017:900). Utredningen bedömer att en sådan ordning är förenlig med artikel 32.8 i NIS2-direktivet. Omedelbar verkställighet kan till exempel motiveras av att tillsynsmyndigheten omedelbart behöver tillförsäkra sig tillgång till en verksamhetsutövares lokaler eller dokumentation i syfte att tillsynen ska kunna genomföras på ett ändamålsenligt sätt. Sådana beslut kan bland annat underlätta bevissäkringsåtgärder genom att beslutet inte behöver invänta laga kraft för att kunna verkställas. Rättssäkerhetsgarantier för den enskilde finns genom möjligheten att överklaga beslutet och att en allmän förvaltningsdomstol kan besluta om så kallad inhibition som innebär att tillsynsmyndighetens beslut tills vidare inte får verkställas.[56] Utredningen bedömer att möjligheten till omedelbar verkställighet ska överföras till den nya lagen i sin nuvarande form.

[56] Se 28 § förvaltningsprocesslagen (1971:291).

9.8 Överklagande

Utredningens bedömning: Tillsynsmyndighetens beslut enligt lagen eller anslutande föreskrifter får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är tillsynsmyndigheten motpart i domstolen. Prövningstillstånd krävs vid överklagande till kammarrätten.

De beslut som tillsynsmyndigheterna fattar avseende enskilda kan antas påverka deras civila rättigheter och skyldigheter enligt artikel 6 i Europakonventionen. Som följd behöver det finnas möjligheter att få sådana beslut prövade av domstol. En sådan möjlighet finns i dag i NIS-lagen och den bör även finnas i den nya lagen. Överklagandena bör även fortsättningsvis prövas av allmän förvaltningsdomstol. Rätten till överklagande bör även omfatta myndigheter och andra offentliga aktörer som tillsynsmyndigheten riktar beslut emot. Som följd bör tillsynsmyndigheten även i dessa fall anges utgöra motpart till den klagande.[57]

Utredningen har identifierat åtminstone två tänkbara alternativ avseende forumregler för överklagande. Det första alternativet följer huvudregeln som innebär att överklagandet ska prövas av den förvaltningsdomstol inom vars domkrets ärendet först prövats.[58] Genom utredningens förslag på tillsynsmyndigheter (se avsnitt 8.4.2) och deras geografiska spridning kommer därmed flera förvaltningsrätter och kammarrätter bli behöriga att pröva sådana mål, och Högsta förvaltningsdomstolen utgör högsta prövningsinstans. Detta alternativ motsvarar dagens ordning enligt NIS-lagen.[59] Det andra alternativet innebär att en viss förvaltningsrätt (och därmed kammarrätt) pekas ut som ensamt behörig att pröva av mål enligt lagen. Alternativet skulle medföra en koncentrering av målhanteringen och skulle motsvara den ordning som i huvudsak följer enligt säkerhetsskyddslagstiftningen.[60] Utredningen bedömer dock att det inte framkommit några särskilda skäl som talar för en sådan lösning. Som följd bör den nuvarande ordningen överföras till den nya lagen.

[57] Jfr 7 a § förvaltningsprocesslagen (1971:291).
[58] Se 14 § andra stycket lagen (1971:289) om allmänna förvaltningsdomstolar.
[59] 39 § NIS-lagen.
[60] Se 8 kap. 4 § första stycket säkerhetsskyddslagen (2018:585), se vidare prop. 2020/21:194 s. 109 f.

Att domstolens beslut om förbud (avsnitt 9.5.6) går att överklaga följer av 33 § förvaltningsprocesslagen (1971:291) och behöver inte anges särskilt i den nu aktuella lagen.

10 Gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet

10.1 Gemensam kontaktpunkt

10.1.1 Inledning

Enligt NIS2-direktivet ska varje medlemsstat utse eller inrätta en gemensam kontaktpunkt. Den gemensamma kontaktpunkten ska utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater och, när det är lämpligt, kommissionen och Enisa samt ett sektorsövergripande samarbete med andra behöriga myndigheter i medlemsstaten (artikel 8.3 och 8.4).

Enligt kommittédirektivet bör utgångspunkten för utredarens uppdrag vara att MSB ska vara gemensam kontaktpunkt.

10.1.2 Gemensam kontaktpunkt i Sverige

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap ska vara gemensam kontaktpunkt.

Enligt 22 § NIS-förordningen är MSB gemensam nationell kontaktpunkt i Sverige. Vid implementeringen av NIS-direktivet konstaterade regeringen att MSB har den struktur och kompetens som krävs både för att samordna frågor om säkerhet i nätverks- och informationssystem och för att ansvara för kommunikation och gränsöverskridande samarbete i anslutning till detta.[1] Detta innebär att MSB

[1] Prop. 2017/18:205 s. 77.

i dag samverkar med gemensamma kontaktpunkter i andra medlemsstater och fullgör de uppgifter som följer av det första NIS-direktivet. Myndigheten företräder också Sverige i den samarbetsgrupp som inrättades genom NIS-direktivet (NIS Cooperation Group). MSB leder vidare ett samarbetsforum där samtliga tillsynsmyndigheter och Socialstyrelsen ingår samt en privat-offentlig samverkansgrupp där de reglerade sektorerna ingår.

Mot bakgrund av att MSB i dag fullgör de uppgifter som följer av att vara gemensam kontaktpunkt samt myndighetens uppgift att stödja och samordna arbetet med samhällets informationssäkerhet anser utredningen att MSB även fortsatt ska vara gemensam kontaktpunkt i Sverige.

Utredningen anser att regleringen av vilken myndighet som ska utgöra gemensam kontaktpunkt och dess uppgifter bör ske i förordning. Detta följer även den generella systematik i den föreslagna regleringen, som innebär att regeringen har möjlighet att förändra utpekade myndigheter och deras uppdrag utan att en lagändring krävs.

10.1.3 Den gemensamma kontaktpunktens uppgifter

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap ska fullgöra de uppgifter som åligger den gemensamma kontaktpunkten enligt NIS2-direktivet samt de uppgifter som regeringen bestämmer.

Den gemensamma kontaktpunkten ska:

1. Utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete med myndigheter i andra medlemsstater, kommissionen och Enisa samt ett sektorsövergripande samarbete med tillsynsmyndigheterna.
2. På begäran av CSIRT-enheten vidarebefordra incidentrapporter till de gemensamma kontaktpunkterna i andra medlemsstater.
3. Var tredje månad lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud.

4. Underrätta kommissionen och samarbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare som förtecknats för varje sektor och delsektor.
5. Informera kommissionen och samarbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare samt deras verksamhet som identifierats enligt 1 kap. 8 § lagen om cybersäkerhet.
6. Upprätta ett särskilt register över gränsöverskridande verksamhetsutövare och ge in det skyndsamt till Enisa. Vidare ska den gemensamma kontaktpunkten löpande underrätta Enisa om uppgifter avseende gränsöverskridande verksamhetsutövare.

Den gemensamma kontaktpunkten ska utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater och, när det är lämpligt kommissionen och Enisa. Den ska också säkerställa ett sektorsövergripande samarbete med andra behöriga myndigheter i Sverige (artikel 8.4).

En del av det sektorsövergripande samarbetet mellan den gemensamma kontaktpunkten och tillsynsmyndigheterna är det samarbetsforum som föreslås i avsnitt 8.4.7 men det kan också innebära att tillsynsmyndigheten, när sådant behov uppstår, bistår den gemensamma kontaktpunkten med utskick av information till verksamhetsutövare inom tillsynsområdet.

På begäran av CSIRT-enheten eller den behöriga myndigheten ska den gemensamma kontaktpunkten vidarebefordra incidentrapporter till de gemensamma kontaktpunkterna i andra berörda medlemsstater (artikel 23.8).

Den gemensamma kontaktpunkten ska var tredje månad lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud som rapporterats av verksamhetsutövarna (artikel 23.9).

Enisa ska skapa och upprätta ett register över gränsöverskridande verksamhetsutövare på sätt som beskrivs i avsnitt 6.2. Medlemsstaterna ska ålägga dessa verksamhetsutövare att lämna nödvändiga uppgifter till tillsynsmyndigheterna. Den gemensamma kontaktpunkten ska efter att ha tagit emot uppgifterna utan dröjsmål vidarebefordra informationen till Enisa (artikel 27).

Som beskrivs i avsnitt 6.2 ska den gemensamma kontaktpunkten senast den 17 april 2025 och därefter vartannat år underrätta kommissionen och samarbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare som förtecknats för varje sektor och delsektor. Vidare ska myndigheten informera om antalet väsentliga och viktiga verksamhetsutövare samt deras verksamhet som identifierats enligt 1 kap. 8 §.

Utredningen bedömer att dessa uppgifter bör anges i förordning.

Som framgår i avsnitt 8.4.7 ska tillsynsmyndigheterna vid behov samarbeta med och bistå tillsynsmyndigheter i andra medlemsstater. Detta ska bland annat omfatta att via den gemensamma kontaktpunkten informera och samråda med tillsynsmyndigheter i övriga berörda medlemsstater om de tillsynsåtgärder som vidtagits (artikel 37.1 a). Denna uppgift ingår i den gemensamma kontaktpunktens uppgift att utöva en sambandsfunktion och behöver enligt utredningen inte regleras särskilt.

Samarbetsgrupp

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap ska företräda Sverige i den samarbetsgrupp som inrättats enligt artikel 14 i NIS2-direktivet.

Tillsynsmyndigheten ska lämna stöd till Sveriges representant i samarbetsgruppen.

Genom NIS-direktivet inrättades en samarbetsgrupp på EU-nivå (NIS Cooperation Group). Enligt artikel 14.1 i NIS2-direktivet ska samarbetsgruppen underlätta strategiskt samarbete och informationsutbyte mellan medlemsstaterna samt stärka förtroende och tillit. Samarbetsgruppen ska bestå av företrädare för medlemsstater, kommissionen och Enisa. Europeiska utrikestjänsten ska delta som observatör. Samarbetsgruppens uppgifter listas i artikel 14.4 a–s. Till stor del motsvarar dessa uppgifter de som angavs i NIS-direktivet men det har också tillkommit nya uppgifter, till exempel att genomföra samordnade riskbedömningar av kritiska leveranskedjor.

MSB är i dag Sveriges representant i samarbetsgruppen vilket anges i 23 § NIS-förordningen. Det framgår av kommittédirektivet att MSB även fortsatt bör representera Sverige i samarbetsgruppen

och utredningen saknar skäl att göra någon annan bedömning. Uppdraget bör anges i den nya förordningen.

Av 19 § 5 i NIS-förordningen framgår att tillsynsmyndigheterna ska lämna stöd till Sveriges representant i samarbetsgruppen. Samarbetsgruppen har sedan den inrättats bildat ett flertal arbetsgrupper. Dessa arbetsgrupper är i flera fall sektorsspecifika och behandlar frågor där kunskapen finns hos tillsynsmyndigheterna. Det är tillsynsmyndigheterna som till största del representerat Sverige i de sektorsspecifika arbetsgrupperna. Det bör enligt utredningen även fortsättningsvis vara möjligt för tillsynsmyndigheterna att delta i dessa arbetsgrupper. För närvarande deltar PTS, Energimyndigheten, IVO och Transportstyrelsen i sex arbetsgrupper och MSB deltar i åtta. Det bör därför även i den nya förordningen anges att tillsynsmyndigheterna ska lämna stöd till Sveriges representant i samarbetsgruppen.

10.2 Enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet)

10.2.1 Inledning

Varje medlemsstat ska utse eller inrätta en eller flera CSIRT-enheter (Computer Security Incident Response Team). CSIRT-enheterna ska uppfylla de krav som anges i artikel 11.1, ska omfatta minst de sektorer, delsektorer och typer av verksamhetsutövare som avses i NIS2-direktivets bilagor och ska ansvara för incidenthantering i enlighet med ett tydligt fastställt förfarande (artikel 10.1). Enligt kommittédirektivet bör utgångspunkten för utredarens uppdrag vara att MSB även enligt den nya regleringen ska ha rollen som CSIRT-enhet.

10.2.2 CSIRT-enhet i Sverige

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap ska vara CSIRT-enhet.

MSB ansvarar för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. Arbetet sker genom MSB:s CERT-verksamhet[2] som har benämningen CERT-SE. Till uppgifterna hör bland annat att agera skyndsamt vid inträffade it-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbetet som krävs för att avhjälpa eller lindra effekter av det inträffade samt samverka med myndigheter med särskilda uppgifter inom cybersäkerhetsområdet. MSB/CERT-SE är Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder.

Enligt 12 § NIS-förordningen är MSB CSIRT-enhet och ska bland annat ta emot incidentrapporter som lämnas enligt NIS-lagen samt uppfylla de krav och fullgöra de uppgifter som följer av bilaga 1 till NIS-direktivet. MSB ska även ta emot de it-incidentrapporter som statliga myndigheter lämnar enligt 14 § i förordningen (2022:524) om statliga myndigheters beredskap. MSB har tagit fram ett digitalt rapporteringsverktyg där incidenterna kan rapporteras.

Mot bakgrund av de uppdrag MSB har i dag och den kompetens som finns inom myndigheten så bedömer utredningen att MSB även fortsatt ska vara CSIRT-enhet i Sverige. Utredningen anser att regleringen av vilken myndighet som ska vara CSIRT-enhet och dess uppgifter bör ske i förordning.

10.2.3 CSIRT-enhetens uppgifter

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap ska uppfylla de krav och fullgöra de uppgifter som åligger CSIRT-enheten enligt artikel 11 i NIS2-direktivet.

När CSIRT-enheten utför sina uppgifter ska den,

1. säkerställa en hög nivå av tillgänglighet för sina kommunikationskanaler,
2. ha lokaler och informationssystem på säkra platser,
3. ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar,

[2] Computer Emergency Response Team.

4. vara ständigt tillgänglig och säkerställa att personalen har fått lämplig utbildning,
5. ha redundanta system och reservlokaler för att säkerställa kontinuiteten i tjänsterna, och
6. ha en säker och motståndskraftig kommunikations- och informationsinfrastruktur för utbyte av information med verksamhetsutövare och andra relevanta intressenter.

CSIRT-enheten ska,

1. övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå och tillhandahålla varningar och information,
2. erbjuda stöd avseende realtidsövervakning av nätverks- och informationssystem,
3. ta emot incidentrapporter, vidta åtgärder och erbjuda stöd,
4. om en incident kan antas ha sin grund i en brottslig gärning skyndsamt uppmana verksamhetsutövaren att anmäla incidenten till Polismyndigheten,
5. tillgängliggöra informationen i incidentrapporter utan dröjsmål för tillsynsmyndigheten,
6. samla in och analysera forensiska uppgifter,
7. tillhandahålla dynamiska risk- och incidentanalyser samt lägesuppfattning,
8. på begäran av en verksamhetsutövare utföra en proaktiv skanning av den berörda verksamhetsutövarens nätverks- och informationssystem,
9. delta i det nätverk som inrättats enligt artikel 15 i NIS2-direktivet (CSIRT-nätverket),
10. vara samordnare för samordnad delgivning av information om sårbarheter, och
11. upprätta samarbetsförbindelser med relevanta intressenter inom privat och offentlig sektor samt bidra till samverkan rörande cybersäkerhet.

CSIRT-enheten får utföra proaktiva, icke-inkräktande skanningar av verksamhetsutövarnas allmänt tillgängliga nätverks- och informationssystem i syfte att upptäcka sårbara eller osäkert konfigurerade system.

Kraven på CSIRT-enheten framgår av artikel 11.1 i NIS2-direktivet. CSIRT-enheten ska uppfylla följande krav:

a) CSIRT-enheterna ska säkerställa en hög nivå av tillgänglighet för sina kommunikationskanaler genom att undvika felkritiska systemdelar och ska kunna kontaktas och kontakta andra när som helst och på flera olika sätt. De ska tydligt ange kommunikationskanalerna och underrätta användargrupper och samarbetspartner om dessa.

b) CSIRT-enheternas lokaler och de informationssystem som de använder sig av ska vara belägna på säkra platser.

c) CSIRT-enheterna ska ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar, särskilt för att underlätta ändamålsenliga och effektiva överlämnanden.

d) CSIRT-enheterna ska säkerställa verksamhetens konfidentialitet och trovärdighet.

e) CSIRT-enheterna ska ha tillräckligt med personal för att säkerställa att deras tjänster är ständigt tillgängliga och de ska säkerställa att personalen har fått lämplig utbildning.

f) CSIRT-enheterna ska utrustas med redundanta system och reservlokaler för att säkerställa kontinuiteten i deras tjänster.

Artikeln innebär bland annat krav på tillgänglighet, informationssystem, lokaler utbildning, konfidentialitet och trovärdighet. Enligt artikel 10.3 ska medlemsstaterna också säkerställa att CSIRT-enheten har tillgång till en lämplig, säker och motståndskraftig kommunikations- och informationsstruktur för utbyte av information med verksamhetsutövarna och andra relevanta intressenter. Det bör anges i den nya förordningen att CSIRT-enheten ska uppfylla dessa krav.

Kravet på att CSIRT-enheten ska säkerställa verksamhetens konfidentialitet och trovärdighet behöver enligt utredningen inte anges särskilt i förordningen. Att verksamheten ska vara trovärdig får an-

ses följa av de generella kraven på förvaltningsmyndigheters arbete enligt förvaltningslagen (2017:900). Krav på konfidentialitet följer av offentlighets- och sekretesslagen (2009:400).

CSIRT-enhetens uppgifter anges i artikel 11.3 i NIS2-direktivet och är följande:

a) Övervakning och analys av cyberhot, sårbarheter och incidenter på nationell nivå och, på begäran, tillhandahållande av stöd till berörda väsentliga och viktiga verksamhetsutövare avseende realtidsövervakning eller nära realtidsövervakning av deras nätverks- och informationssystem.

b) Tillhandahållande av tidiga varningar, larm, meddelanden och spridning av information till väsentliga och viktiga verksamhetsutövare samt till behöriga myndigheter och andra relevanta intressenter om cyberhot, sårbarheter och incidenter, om möjligt i nära realtid.

c) Vidtagande av åtgärder till följd av incidenter och, i tillämpliga fall, tillhandahållande av stöd till de berörda väsentliga och viktiga verksamhetsutövarna.

d) Insamling och analys av forensiska uppgifter och tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet när det gäller cybersäkerhet.

e) Tillhandahållande, på begäran av den väsentliga eller viktiga verksamhetsutövaren, av en proaktiv skanning av den berörda verksamhetsutövarens nätverks- och informationssystem i syfte att upptäcka sårbarheter med en potentiellt betydande påverkan.

f) Deltagande i CSIRT-nätverket och ömsesidigt bistånd i enlighet med CSIRT-enhetens kapacitet och befogenheter till andra medlemmar i CSIRT-nätverket.

g) I tillämpliga fall fungera som processamordnare för den samordnade delgivningen av information om sårbarheter enligt artikel 12.1.

h) Bidra till införandet av säkra verktyg för informationsutbyte enligt artikel 10.3.

Enligt artikel 11 får CSIRT-enheterna också utföra en proaktiv, icke-inkräktande skanning av väsentliga och viktiga verksamhetsutövares allmänt tillgängliga nätverks- och informationssystem. Sådan skanning ska utföras för att upptäcka sårbara eller osäkert konfigurerade nätverks- och informationssystem och informera de berörda verksamhetsutövarna. Sådan skanning får inte ha någon negativ inverkan på hur verksamhetsutövarnas tjänster fungerar.

När CSIRT-enheterna utför uppgifterna som anges i NIS2-direktivet får de prioritera särskilda uppgifter på grundval av en riskbaserad metod.

Artikeln innehåller ett stort antal uppgifter som CSIRT-enheten ska ha. Nedan redogör utredningen för vilka uppgifter som bör anges i förordning.

Övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå och tillhandahålla varningar och information

CSIRT-enheten ska på nationell nivå övervaka och analysera cyberhot, sårbarheter och incidenter. Detta innebär bland annat att samla in information om sårbarheter. CSIRT-enheten ska också tillhandahålla varningar, larm, meddelanden och information till de verksamhetsutövare som omfattas av cybersäkerhetslagen, tillsynsmyndigheter och andra relevanta intressenter.

Erbjuda stöd avseende realtidsövervakning av nätverks- och informationssystem

På begäran av en verksamhetsutövare ska CSIRT-enheten erbjuda stöd avseende realtidsövervakning eller nära realtidsövervakning av deras nätverk- och informationssystem. Stödet kan avse till exempel anvisningar, råd och tekniskt stöd. Uppgiften innebär en stödjande roll för CSIRT-enheten men påverkar inte verksamhetsutövarens ansvar för säkerheten i de nätverk- och informationssystem som den använder.

Ta emot incidentrapporter, vidta åtgärder och erbjuda stöd

CSIRT-enheten ska ta emot incidentrapporter, se avsnitt 7.3. Beroende på vilken information incidentrapporten innehåller kan CSIRT-enheten behöva vidta åtgärder. Detta kan ske genom anvisningar, råd och stöd till den som rapporterat incidenten. Det kan också innefatta att bistå en verksamhetsutövare i incidenthanteringen. Det är dock alltid verksamhetsutövaren som ansvarar för incidenthanteringen och att nödvändiga åtgärder vidtas.

Av artikel 23.5 framgår att CSIRT-enheten utan onödigt dröjsmål och om möjligt inom 24 timmar ska lämna ett svar till den rapporterande verksamhetsutövaren med initial återkoppling. På begäran av verksamhetsutövaren ska CSIRT-enheten även lämna operativa råd, vägledning och tekniskt stöd.

Om incidenten misstänks vara av brottslig art ska verksamhetsutövaren få vägledning om anmälan till brottsbekämpande myndigheter. Detta framgår i dag av 12 § NIS-förordningen och utredningen bedömer därför att det även fortsättningsvis bör framgå av den nya förordningen.

När så är lämpligt, och särskilt om incidenten berör två eller flera medlemsstater, ska enligt artikel 23.6 andra berörda medlemsstater och Enisa informeras under förutsättning att verksamhetsutövarens säkerhets- och affärsintressen och informationens konfidentialitet kan bevaras. Som framgår ovan kan CSIRT-enheten använda sig av den gemensamma kontaktpunkten för att lämna sådan information.

Av artikel 23.7 framgår att CSIRT-enheten eller tillsynsmyndigheten efter samråd med den berörda verksamhetsutövaren får informera allmänheten om en betydande incident eller ålägga verksamhetsutövaren att göra detta om det behövs för att förhindra en betydande incident eller för att hantera en pågående betydande incident. Utredningen bedömer att CSIRT-enhetens möjlighet att informera täcks av bestämmelsen om att tillhandahålla varningar och information. När det gäller möjligheten att ålägga verksamhetsutövaren att informera allmänheten så bedömer utredningen att en sådan möjlighet inte ska införas för CSIRT-enheten eftersom det skulle innebära ett avsteg från den stödjande rollen.

Enligt artikel 23.10 ska CSIRT-enheten förse de behöriga myndigheterna enligt CER-direktivet med information om betydande incidenter, incidenter, cyberhot och tillbud. Enligt 12 § i den nuvar-

ande NIS-förordningen ska CSIRT-enheten utan dröjsmål tillgängliggöra informationen i incidentrapporter för tillsynsmyndigheterna och Socialstyrelsen. En motsvarande bestämmelse bör enligt utredningen införas i den nya förordningen. Bestämmelsen innebär att informationen ska tillgängliggöras för den tillsynsmyndighet som ansvar för tillsyn i den sektor som incidentrapporten avser. Enligt kommittédirektivet ska det som utgångspunkt vara samma myndighet som utövar tillsyn över verksamhetsutövare som omfattas av NIS2- och CER-direktiven och vid en sådan ordning behövs inget tillägg för tillsynsmyndigheter enligt CER-direktivet. Om det inte skulle vara samma myndigheter behöver det läggas till i förordningen att även tillsynsmyndigheter enligt CER-direktivet ska informeras. Utredningen återkommer till denna fråga i samband med att CER-direktivet behandlas.

Samla in och analysera forensiska uppgifter

CSIRT-enheten ska samla in och analysera information om cyberhot, sårbarheter och incidenter. Det kan till exempel avse digitala bevis, angreppsindikatorer (IOC) eller andra tekniska kännetecken och spår som har samband med en incident. Informationen kan till exempel samlas in i samband med att CSIRT-enheten bistår en verksamhetsutövare eller från något av de olika nätverk där CSIRT-enheten deltar.

Tillhandahålla dynamiska risk- och incidentanalyser samt lägesuppfattning

CSIRT-enheten ska tillhandahålla dynamiska risk- och incidentanalyser och situationsmedvetenhet när det gäller cybersäkerhet. Uppgiften innebär till exempel att utarbeta risk- och incidentanalyser utifrån information i de incidentrapporter som lämnas eller information som CSIRT-enheten inhämtar på annat sätt. Att de ska vara dynamiska innebär att de ska uppdateras vid behov. Den engelska termen ”situational awareness” har i NIS2-direktivet översatts till situationsmedvetenhet. Utredningen anser att begreppet lägesuppfattning bättre beskriver vad som avses och bör användas i stället i förordningen. Att tillhandahålla lägesuppfattning innebär bland annat att ta fram lägesbilder.

Proaktiv skanning av verksamhetsutövarnas nätverks- och informationssystem

På begäran av en verksamhetsutövare ska CSIRT-enheten utföra en proaktiv skanning av den berörda verksamhetsutövarens nätverks- och informationssystem i syfte att upptäcka sårbarheter med en potentiellt betydande påverkan.

Enligt artikel 11 får CSIRT-enheten också utföra proaktiva, icke-inkräktande skanningar av verksamhetsutövarnas allmänt tillgängliga nätverks- och informationssystem i syfte att upptäcka sårbara eller osäkert konfigurerade system. CSIRT-enheten ska informera de berörda verksamhetsutövarna om något upptäcks. Det bör vara upp till CSIRT-enheten att avgöra vad som motiverar att verksamhetsutövaren kontaktas. Att skanningarna ska vara icke-inkräktande innebär att de till exempel kan avse att skicka förfrågningar till ett nätverks- och informationssystem för att upptäcka öppna portar eller oskyddade tekniska lösningar i systemet. De kan också användas för att samla in information om tekniska lösningar för att fastställa om sårbara eller oskyddade tekniska lösningar används. En proaktiv skanning får däremot inte innebära ett intrång i ett nätverks- och informationssystem till exempel genom att en sårbarhet utnyttjas. En proaktiv skanning får inte heller ha någon negativ inverkan på hur verksamhetsutövarens tjänster fungerar.

Delta i det nätverk som inrättats enligt artikel 15 i NIS2-direktivet (CSIRT-nätverket)

Genom NIS-direktivet inrättades CSIRT-nätverket. Nätverket ska enligt artikel 15.1 i NIS2-direktivet bidra till utvecklingen av förtroende och tillit och främja ett snabbt och ändamålsenligt operativt samarbete mellan medlemsstater. Nätverket ska enligt artikel 15.2 bestå av företrädare för de CSIRT-enheter som utsetts enligt direktivet och incidenthanteringsorganisationen för unionens institutioner, organ och byråer (Cert-EU). Kommissionen ska delta som observatör och Enisa ska tillhandahålla sekretariat och aktivt bidra med stöd till samarbetet mellan CSIRT-enheterna.

CSIRT-enheten ska delta i nätverket och, i enlighet med deras kapacitet och befogenheter, bistå andra medlemmar i CSIRT-nätverket på deras begäran.

Säkra verktyg för informationsutbyte

Som framgår ovan ska medlemsstaterna enligt artikel 10.3 säkerställa att CSIRT-enheten har tillgång till en lämplig, säker och motståndskraftig kommunikations- och informationsstruktur för utbyte av information med verksamhetsutövarna och andra relevanta intressenter. Medlemsstaterna ska därför säkerställa att CSIRT-enheten bidrar till införandet av säkra verktyg för informationsutbyte. I artikel 11.3 h anges som en uppgift för CSIRT-enheten att bidra till införandet av säkra verktyg för informationsutbyte enligt artikel 10.3. Utredningen bedömer att eftersom det i den föreslagna förordningen anges krav på att CSIRT-enheten ska ha tillgång till säkra verktyg för informationsutbyte så behöver det inte också anges som en uppgift för CSIRT-enheten att bidra till införandet av dessa.

Vara samordnare för samordnad delgivning av information om sårbarheter

Utnyttjandet av sårbarheter i nätverks- och informationssystem kan orsaka betydande störningar och skada. Det är därför viktigt att snabbt identifiera och åtgärda sådana sårbarheter. Eftersom sårbarheter ofta upptäcks och meddelas av tredjeparter bör tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster införa nödvändiga förfaranden för att ta emot sårbarhetsinformation från tredjeparter. En stärkt samordning mellan rapporterande fysiska och juridiska personer och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster är viktig för att underlätta frivillig delgivning av information om sårbarheter. Samordnad delgivning av information om sårbarheter specificerar en strukturerad process genom vilken sårbarheter rapporteras till tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna. Rapporteringen ska ske på ett sätt som gör det möjligt för leverantören att åtgärda sårbarheten innan detaljerad information om sårbarheten meddelas tredjeparter eller allmänheten. Samordnad delgivning av information om sårbarheter bör även inbegripa samordning mellan den rapporterande fysiska eller juridiska personen och tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna vad gäller tidpunkten för åtgärdandet och offentliggörandet av sårbarheter (skäl 58).

Enligt NIS2-direktivet ska medlemsstaterna anta en nationell strategi för cybersäkerhet. Strategin ska bland annat innehålla riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter. Framtagandet av den nationella strategin ingår enligt kommittédirektivet inte i utredningens uppdrag.

Varje medlemsstat ska även utse en CSIRT-enhet till samordnare för den samordnade delgivningen av informationen om sårbarheter. CSIRT-enheten ska fungera som betrodd mellanhand och vid behov underlätta interaktionen mellan en fysisk eller juridisk person som rapporterar en sårbarhet och tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna, på begäran av endera parten. Den CSIRT-enhet som utsetts till samordnare ska bland annat

a) identifiera och kontakta de berörda entiteterna,

b) stödja de fysiska eller juridiska personer som rapporterar en sårbarhet, och

c) förhandla om tidsramar för delgivning av information och hantera sårbarheter som påverkar flera entiteter.

Medlemsstaterna ska säkerställa att fysiska eller juridiska personer anonymt kan rapportera en sårbarhet till den CSIRT-enhet som utsetts till samordnare. Den CSIRT-enhet som utsetts till samordnare ska säkerställa att skyndsamma uppföljningsåtgärder vidtas. Om en rapporterad sårbarhet kan ha en betydande påverkan på entiteter i fler än en medlemsstat, ska CSIRT-enheten, när det är lämpligt, samarbeta med andra CSIRT-enheter som utsetts till samordnare inom CSIRT-nätverket (artikel 12).

Enligt utredningens förslag är MSB CSIRT-enhet och ska därmed även fungera som samordnare för delgivning av sårbarheter. Detta bör anges i förordning.

Riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter ingår i den nationella strategin för cybersäkerhet som ska tas fram i särskild ordning och som inte ingår i utredningens uppdrag.

Upprätta samarbetsförbindelser med relevanta intressenter inom privat och offentlig sektor samt bidra till samverkan rörande cybersäkerhet

Enligt artikel 11.4 ska CSIRT-enheten upprätta samarbetsförbindelser med relevanta intressenter inom den privata sektorn i syfte att uppnå målen med direktivet. För att underlätta samarbetet ska CSIRT-enheten främja antagande och användning av gemensamma eller standardiserade metoder, klassificeringssystem och taxonomier när det gäller förfaranden för incidenthantering, krishantering och samordnad delgivning av sårbarheter.

Enligt artikel 29 ska medlemsstaterna säkerställa att verksamhetsutövare och andra relevanta aktörer på frivillig basis har möjlighet att utbyta information om cybersäkerhet sinsemellan. Informationsutbytet syftar till att förebygga, upptäcka, reagera på och återhämta sig från incidenter samt att höja cybersäkerhetsnivån.

CSIRT-enheten bedriver i dag ett omfattande arbete med samverkan för att sprida information samt vid behov samordna åtgärder. Myndigheten driver ett flertal forum för informationsdelning rörande cybersäkerhet i olika sektorer.

Det bör anges i förordningen att CSIRT-enheten ska upprätta samarbetsförbindelser med relevanta intressenter inom privat och offentlig sektor samt bidra till samverkan rörande cybersäkerhet.

Prioritering av uppgifter

När CSIRT-enheten utför sina uppgifter får de enligt NIS2-direktivet prioritera särskilda uppgifter på grundval av en riskbaserad metod. Innebörden av detta är att CSIRT-enheten kan prioritera till exempel cyberhot som kan få allvarliga konsekvenser eller med stor sannolikhet kommer att realiseras. Utredningen bedömer att en sådan möjlighet redan finns för CSIRT-enheten i Sverige och att det därför inte behöver anges särskilt i regleringen.

10.3 Cyberkrishanteringsmyndighet

10.3.1 Inledning

Varje medlemsstat ska enligt artikel 9.1 utse eller inrätta en eller flera myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter). Enligt kommittédirektivet bör utgångspunkten för utredarens uppdrag vara att MSB utses till cyberkrishanteringsmyndighet.

10.3.2 Cyberkrishanteringsmyndighet i Sverige

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap ska vara cyberkrishanteringsmyndighet.

Mot bakgrund av de uppdrag MSB har i dag och den kompetens som finns inom myndigheten bedömer utredningen att MSB ska vara cyberkrishanteringsmyndighet i Sverige. Utredningen anser att regleringen av vilken myndighet som ska vara cyberkrishanteringsmyndighet och dess uppgifter bör ske i förordning.

MSB:s uppdrag regleras i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

MSB har enligt 1 § ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka, kris, krig eller krigsfara. Myndigheten ska

- utveckla och stödja arbetet med civilt försvar,
- utveckla och stödja samhällets beredskap mot olyckor och kriser och vara pådrivande i arbetet med förebyggande och sårbarhetsreducerande åtgärder,
- arbeta med och verka för samordning mellan berörda samhällsaktörer för att förebygga och hantera olyckor, kriser och konsekvenser av krig och krigsfara,
- samordna kommunerna på nationell nivå och stödja dem med råd och information i deras verksamhet enligt lagen (2003:778) om skydd mot olyckor samt utföra tillsyn enligt samma lag,

- bidra till att minska konsekvenser av olyckor, kriser, krig och krigsfara,
- följa upp och utvärdera samhällets arbete med krisberedskap och civilt försvar,
- se till att utbildning och övningar kommer till stånd inom myndighetens ansvarsområde, och
- företräda det civila försvaret på central nivå i frågor som har betydelse för avvägningen mellan civila och militära behov av samhällets resurser om inte något annat följer av annan författning.

När det gäller förebyggande och förberedande arbete ska myndigheten enligt 2 § i samverkan med myndigheter, kommuner, regioner, organisationer och företag identifiera och analysera sådana sårbarheter, hot och risker i samhället som kan anses vara särskilt allvarliga. Myndigheten ska vidare tillsammans med de ansvariga myndigheterna genomföra en övergripande planering av åtgärder som bör vidtas. Myndigheten ska värdera, sammanställa och rapportera resultatet av arbetet till regeringen.

När det gäller samordning och stöd vid olyckor och kriser ska myndigheten enligt 7 § stödja berörda myndigheters samordning av åtgärder vid en kris eller höjd beredskap. Myndigheten ska se till att berörda aktörer under sådana förhållanden, när det gäller krishantering och civilt försvar, får tillfälle att

- samordna åtgärder,
- samordna information till allmänhet och medier,
- effektivt använda samhällets resurser och internationella förstärkningsresurser, och
- samordna stödet till centrala, regionala och lokala organ i fråga om information och lägesbilder.

Myndigheten ska också bistå Regeringskansliet med underlag om information av betydelse för myndighetens ansvarsområde i samband med allvarliga olyckor och kriser samt under höjd beredskap.

Enligt 7 a § ska MSB utifrån en nationell riskbild upprätthålla beredskap med stödresurser för att kunna bistå i samband med allvarliga olyckor och kriser och vid höjd beredskap.

För uppföljning, utvärdering och lärande ska myndigheten enligt 10 § beredskapssektorsvis, geografiskt områdesvis och på en övergripande samhällsnivå följa upp och utvärdera krisberedskap och civilt försvar och bedöma om vidtagna åtgärder fått önskad effekt.

Myndigheten ska enligt 11 § se till att erfarenheter tas till vara från inträffade olyckor och kriser. Till stöd för detta ska myndigheten tillhandahålla tvärsektoriella och samlade bilder och bedömningar samt utveckla kompetens och metodik inom området som tillgodoser nationella, regionala och lokala behov.

10.3.3 Cyberkrishanteringsmyndighetens uppgifter

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap ska fullgöra de uppgifter som åligger cyberkrishanteringsmyndigheten enligt NIS2-direktivet samt de uppgifter som regeringen bestämmer.

Myndigheten för samhällsskydd och beredskap ska delta i det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe).

Varje medlemsstat ska anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser där mål och villkor för hanteringen av storskaliga cybersäkerhetsincidenter och kriser fastställs. Planen ska bland annat innehålla cyberkrishanteringsmyndighetens uppgifter och ansvarsområden. Utformningen av den nationella planen omfattas enligt kommittédirektivet inte av utredningens uppdrag. Cyberkrishanteringsmyndighetens uppgifter bör därför anges i förordning efter att den nationella planen för hantering av storskaliga cybersäkerhetsincidenter tagits fram. Utredningen lämnar därför inget förslag i denna del.

EU-CyCLONe

Genom artikel 16.1 inrättas ett europeiskt kontaktnätverk för cyberkriser (EU-CyCLONe) för att stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser och säkerställa informationsutbyte mellan medlemsstaterna och EU:s institutioner. EU-CyCLONe bör fungera som mellanhand mellan den tekniska och

politiska nivån under storskaliga cybersäkerhetsincidenter och kriser och bör stärka samarbetet och stödja beslutsfattandet på politisk nivå. I samarbete med kommissionen, och med beaktande av kommissionens behörighet inom krishantering, bör EU-CyCLONe ta fasta på CSIRT-nätverkets slutsatser och använda sin egen kapacitet för att göra en konsekvensanalys av storskaliga cybersäkerhetsincidenter och kriser (skäl 71). EU-CyCLONe ska bestå av företrädare för medlemsstaternas cyberkrishanteringsmyndigheter samt i vissa fall kommissionen (artikel 16.2).

MSB ska i egenskap av cyberkrishanteringsmyndighet företräda Sverige i nätverket vilket bör anges i förordningen.

11 NIS2-direktivet och LEK

11.1 Inledning

Den 21 december 2018 trädde direktivet om inrättande av en europeisk kodex för elektronisk kommunikation[1] i kraft (nedan ”kodexen”). Kodexen har genomförts i svensk rätt, huvudsakligen genom lagen (2022:482) om elektronisk kommunikation (nedan ”LEK”). Genom NIS2-direktivet upphävs artikel 40 och 41 i kodexen med verkan från och med den 18 oktober 2024 och ersätts med bestämmelserna som följer av NIS2-direktivet.[2] Dessa artiklar i kodexen ligger till grund för bestämmelserna i 8 kap. 1–4 §§ LEK. Konsekvenserna för bestämmelserna i LEK av att kodexen upphävs behöver analyseras.

11.2 Bestämmelserna i LEK, kodexen och NIS2

11.2.1 Allmänt

Utredningen behöver inledningsvis bedöma om de individuella bestämmelserna i LEK även innehåller andra bestämmelser än de som är avsedda att genomföra artiklarna 40 och 41 i kodexen. I samband med det svenska genomförandet av kodexen har även en portalbestämmelse införts i LEK och som innebär att bland annat Sveriges säkerhet ska beaktas vid all tillämpning av lagen.[3] Portalbestämmelsen kan därför påverka hur andra materiella bestämmelser såsom 8 kap. 1–4 §§ LEK ska tillämpas, men det är oklart i vilken utsträckning. Någon motsvarande portalbestämmelse har inte föreslagits av utredningen avseende NIS2. Utredningen saknar möjlighet att inom den snäva tidsram som råder vidare utreda konsekvenserna av denna skillnad.

[1] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning).
[2] Se skäl 92 och artikel 43 i NIS2-direktivet.
[3] Se 1 kap. 1 § tredje stycket LEK.

Utredningen anser dock att avsaknaden av en motsvarande portalbestämmelse i den föreslagna cybersäkerhetslagen inte innebär ett hinder mot att 8 kap. 1–4 §§ LEK upphävs med anledning av att artiklarna 40 och 41 i kodexen upphör att gälla.

11.2.2 Kretsen som ska tillämpa kraven

8 kap. 1–4 §§ LEK ska tillämpas av den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst (nedan ”tillhandahållare”). Innebörden av dessa begrepp anges i 1 kap. 7 § LEK och motsvarar materiellt definitionerna av motsvarande begrepp i kodexen.[4] I NIS2-direktivet används samma begrepp som i kodexen, och hänvisar också till kodexens definitioner.[5] En allmänt tillgänglig elektronisk kommunikationstjänst utgör i sig inte ett nätverks- och informationssystem enligt NIS2-direktivets definition.[6] Det följer dock att alla tillhandahållare antingen är väsentliga eller viktiga verksamhetsutövare, beroende på om de uppfyller det aktuella storlekskravet.[7] Som följd är sådana aktörer skyldiga att följa den kravmassa som följer av direktivet. Utredningen bedömer mot denna bakgrund att det inte råder någon skillnad i vilken krets som träffas av kodexens respektive NIS2-direktivets bestämmelser.

11.2.3 Riskhanteringsåtgärder

Av 8 kap. 1 § LEK följer tillhandahållares skyldighet att vidta riskhanteringsåtgärder:

> [Tillhandahållare] ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar säkerheten i nät och tjänster.
>
> Åtgärderna ska säkerställa en nivå på säkerheten i nät och tjänster som är lämplig i förhållande till riskerna. Åtgärder ska vidtas särskilt för att förebygga och minimera säkerhetsincidenters påverkan på användare och på andra nät och tjänster.

[4] Se artiklarna 2.1, 2.4 och 2.8 i kodexen samt prop. 2021/2022:136 s. 406 f.
[5] Jfr artiklarna 6.1 a och 6.36 och 6.37 i NIS2-direktivet.
[6] Artikel 6.1 ec i NIS2-direktivet.
[7] Artiklarna 2.2 a, 3.1 c och 3.2, jfr bilaga 1 och sektorn *Digital infrastruktur* i NIS2-direktivet.

Bestämmelsen utgör ett nationellt genomförande av både artikel 40.1 och 108 (delvis) i kodexen.[8]

Artikel 40

Av artikel 40.1 första stycket i kodexen följer skyldigheten att vidta riskhanteringsåtgärder:

> [Tillhandahållare ska] vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar näts och tjänsters säkerhet. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en nivå på säkerheten som är lämplig i förhållande till den föreliggande risken. I synnerhet ska åtgärder, inbegripet kryptering när så är lämpligt, vidtas för att förhindra och minimera säkerhetsincidenters inverkan på användare och på andra nät och tjänster.

På motsvarande sätt följer av artikel 21.1 i NIS2-direktivet att:

> [Väsentliga och viktiga verksamhetsutövare ska] vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster.
>
> Med beaktande av de senaste, och i tillämpliga fall, relevanta europeiska och internationella standarder samt genomförandekostnaderna, ska de åtgärder som avses i första stycket säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken. Vid bedömningen av dessa åtgärders proportionalitet ska vederbörlig hänsyn tas till entitetens grad av riskexponering, entitetens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser.

Utredningen bedömer att ”ändamålsenliga” (kodexen) och ”lämpliga” (NIS2) i denna kontext har likvärdig innebörd. Begreppet ”lämpliga” har av utredningen bedömts snarlikt ”proportionell” och i förslaget till cybersäkerhetslag har därför *proportionell* använts i stället (se avsnitt 7.2). I NIS2-skrivningen anges utöver tekniska och organi-

[8] Se prop. 2021/22:136 s. 493.

satoriska åtgärder även driftsrelaterade sådana, vilket i vart fall inte kan uppfattas som en avsmalning i relation till kodexen.[9]

Vidare anges vad det är som ska skyddas från hoten, nämligen ”näts och tjänsters säkerhet” (kodexen) och ”säkerheten i nätverks- och informationssystem” (NIS2). Begreppet *säkerhet för nät och tjänster* definieras i artikel 2.21 i kodexen på följande sätt.

> Elektroniska kommunikationsnäts och tjänsters förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos dessa nät och tjänster, hos lagrade eller överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät och tjänster.

I artikel 6.2 i NIS2-direktivet definieras motsvarande begrepp, *säkerhet i nätverks- och informationssystem*, på följande sätt.

> Nätverks- och informationssystems förmåga att med en viss tillförlitlighetsnivå motstå händelser som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem.

Även med beaktande av vissa semantiska skillnader, till exempel ”motstå åtgärder” och ”integriteten” (kodexen) kontra ”motstå händelser” och ”autenticiteten” (NIS2) bedömer utredningen att säkerhetsbegreppet i de två direktiven är att betrakta som likvärdiga.[10]

Därutöver anges i NIS2 att säkerheten ska avse sådana system som verksamhetsutövaren använder för sin verksamhet eller för att tillhandahålla sina tjänster. Åtgärderna ska således vidtas både för system som används i verksamhetsutövarens verksamhet men inte nödvändigtvis för att erbjuda NIS-tjänsten, och sådana system som används för att erbjuda NIS-tjänsten. Detta är enligt utredningen ett förtydligande i relation till motsvarande definition i det ursprungliga NIS-direktivet (artikel 4.2). Kodexen saknar motsvarande skrivning och utredningen bedömer att NIS2-direktivets krav åtminstone är likvärdiga med kodexen i denna del.

Nivån på säkerhet enligt kodexen ska vara ”lämplig i förhållande till risken”, och åtgärder ska vidtas för att förhindra och minimera incidenters inverkan på användare och på andra nät och tjänster.

[9] Det går att resonera kring om skrivningen utgör en exemplifiering som i och för sig omfattas av kodexens bestämmelser, trots att den inte anges där. Det saknar dock relevans för analysen.
[10] Se även prop. 2021/22:136 s. 313 f.

Motsvarande krav följer av NIS2-direktivets skrivningar, som även anger vilka faktorer som ska beaktas vid avvägningen mellan åtgärd och risk. Kodexen nämner att ”den senaste tekniska utvecklingen” ska beaktas, vilket inte framgår av NIS2. Enligt utredningen finns dock möjlighet att beakta sådana aspekter inom ramen NIS2 och det finns därför inte någon materiell skillnad på kraven i denna del.

Sammanfattningsvis anser utredningen att bestämmelsen i LEK korresponderar med det materiella innehåll som följer av artikel 40 i kodexen, och att NIS2-direktivets bestämmelser inte är begränsande i förhållande till kodexen i denna del. På motsvarande sätt ger utredningens föreslagna bestämmelser om riskhanteringsåtgärder (3 kap. i den föreslagna cybersäkerhetslagen) i denna del samma, eller större, utrymme för riskhanteringsåtgärder jämfört med vad som följer enligt LEK.

Artikel 108

Regeringen har bedömt att artikel 108 i kodexen syftar till att ge ett särskilt skydd för slutanvändares tillgång till grundläggande möjligheter att ringa röstsamtal och ha tillgång till internet samt nödnumret 112.[11] Artikeln har genomförts delvis genom bestämmelsen om säkerhetsåtgärder i 8 kap. 1 § LEK.[12] Den föreslagna cybersäkerhetslagens bestämmelser har ovan bedömts ge motsvarande eller större utrymme för riskhanteringsåtgärder än 8 kap. 1 § LEK. Utredningen bedömer mot denna bakgrund att artikel 108 i kodexen på motsvarande sätt ska anses delvis genomförd genom 3 kap. 1 § cybersäkerhetslagen.

11.2.4 Ramen för vad riskhanteringsåtgärderna kan avse

Kodexen använder begreppet ”säkerhetsåtgärder”. Utredningen kommer dock i det följande att använda begreppet ”riskhanteringsåtgärder” för att beteckna motsvarande åtgärder enligt så väl kodexen som NIS2-direktivet.

[11] Prop. 2021/22:136 s. 316.
[12] Prop. 2021/22:136 s. 492 f.

Enligt kodexen kan riskhanteringsåtgärder avse åtgärder inom flera områden, exempelvis. kontinuitetsplanering och fysisk säkerhet.[13]

Enligt NIS2-direktivet ska de aktuella riskhanteringsåtgärderna avse cybersäkerhet (se avsnitt 7.1.2 ovan). Med begreppet cybersäkerhet avses all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.[14] Cyberhot definieras i sin tur som en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare dessa system och andra personer (dessa kategorier benämns nedan som ”skyddsföremålen”).[15] Vid en första anblick skulle cyberhot semantiskt kunna förstås som hot som finns i cyberrymden, dvs. logiska hot såsom dataintrång eller dataförluster. Begreppet är dock i NIS2-kontexten betydligt bredare än så, och omfattar alla omständigheter som kan påverka skyddsföremålen negativt (jfr artikel 21.1). Som följd inkluderas alla aspekter som kan få påverkan, dvs. även exempelvis fysiska angrepp eller händelser (se artikel 21.2). Riskhanteringsåtgärderna vidtas för att hantera risker som hotar säkerheten i nätverks- och informationssystem (artikel 21.1 första stycket och artikel 6.2). De ska skydda både skyddsföremålen och lagrade, överförda eller behandlade uppgifter. Dessa ska skyddas mot alla händelser som kan ge negativ påverkan, oavsett om detta är fysiska eller logiska (”digitala”) händelser. Det kan även röra sig om organisatorisk påverkan, till exempel genom personalbrist eller brister i en delegationsordning. Eftersom ett elektroniskt kommunikationsnät utgör ett nätverks- och informationssystem[16] ska även denna fysiska infrastruktur skyddas. Mot denna bakgrund bedömer utredningen att ramen för riskhanteringsåtgärder som följer av NIS2 åtminstone motsvarar vad som följer enligt kodexen.

11.2.5 Säkerhetsrevision

Av 8 kap. 2 § LEK följer skyldigheten för tillhandahållare att utföra säkerhetsgranskning (*säkerhetsrevision* enligt utredningens förslag, se kapitel 8).

[13] Jfr skäl 9 och prop. 2021/22:136 s. 316.
[14] Artikel 6.3 NIS2-direktivet, jfr artikel 2.1 i cybersäkerhetsakten.
[15] Artikel 6.10 NIS2-direktivet, jfr artikel 2.8 i cybersäkerhetsakten.
[16] Se artikel 6.1 a i NIS2-direktivet, jfr artikel 2.1 i kodexen.

> Om det finns särskilda skäl, får tillsynsmyndigheten ålägga den som [är tillhandahållare] att på egen bekostnad låta ett oberoende kvalificerat organ utföra en säkerhetsgranskning av hela eller delar av verksamheten och att redovisa resultatet av granskningen för myndigheten.

Bestämmelsen genomför artikel 41.2 b i kodexen[17] som har följande lydelse.

> [Tillhandahållare ska] underkasta sig en säkerhetsgranskning som utförs av ett kvalificerat oberoende organ eller en behörig myndighet och göra resultatet av granskningen tillgängligt för den behöriga myndigheten; kostnaderna för säkerhetsgranskningen ska betalas av tillhandahållaren.

Utredningen bedömer att LEK:s genomförande inte går utöver vad som följer av kodexen. Motsvarande krav i NIS2-direktivet återfinns i artikel 32.2 och 33.2 (se avsnitt 8.4.6). Dessa krav omfattar enligt utredningen samma möjligheter som följer av kodexen. Genom utredningens förslag på genomförande av NIS2-direktivet i denna del kommer tillsynsmyndigheternas möjligheter att besluta om säkerhetsrevision motsvara vad som i dag gäller enligt LEK.

11.2.6 Incidentbegreppet

Säkerhetsincidenter som har haft en betydande påverkan på nät och tjänster är rapporteringspliktiga enligt 8 kap. 3 § LEK och kodexen (artikel 40.2). En säkerhetsincident definieras i 1 kap. 7 § LEK som:

> En händelse med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på förmågan att motstå sådana händelser.

Denna definition motsvarar innehållet i artikel 2.42 jämförd med artikel 2.21 i kodexen.[18]

> *säkerhetsincident*: en händelse med en faktisk negativ inverkan på säkerheten i elektroniska kommunikationsnät eller kommunikationstjänster

[17] Se prop. 2021/22:136 s. 317 f. och 494 f.
[18] Jfr prop. 2021/22:136 s. 411.

> *säkerhet för nät och tjänster*: elektroniska kommunikationsnäts och kommunikationstjänsters förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos dessa nät och tjänster, hos lagrade eller överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller kommunikationstjänster

Motsvarande definition följer av artikel 6.6 jämförd med artikel 6.2 i NIS2-direktivet:

> *incident*: en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem

> *säkerhet i nätverks- och informationssystem*: nätverks- och informationssystems förmåga att med en viss tillförlitlighetsnivå motstå händelser som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem

Som synes ovan har incidentbegreppet i LEK kompletterats med ”eller på förmågan att motstå sådana händelser”, hämtat från definitionen av *säkerhet för nät och tjänster*. Tillägget till incidentdefinitionen synes ha tillförts till LEK-bestämmelsen efter PTS förslag och för att incidentbegreppet både skulle träffa händelser med faktisk påverkan på tillgänglighet, riktighet etcetera, samt sådana händelser som påverkar förmågan att motstå sådana händelser.[19] Motsvarande tillägg finns även i NIS2-definitionen av *säkerhet i nätverks- och informationssystem*. Utredningen har dock inte funnit skäl att föreslå att incidentbegreppet ska få samma utformning som i LEK. I NIS2 omfattar incidentbegreppet fysisk infrastruktur och fysisk påverkan, men kräver att den aktuella händelsen ska ha någon form av påverkan på uppgifter eller tjänster. Det bör i det fortsatta lagstiftningsarbetet övervägas om denna skillnad i omfattning medför ett behov av vidare åtgärder.

[19] Prop. 2021/22:136 s. 319.

11.2.7 Kravet på incidentrapportering

Av 8 kap. 3 § första stycket LEK följer skyldigheten att rapportera säkerhetsincidenter:

> [Tillhandahållare] ska utan onödigt dröjsmål till tillsynsmyndigheten rapportera säkerhetsincidenter som har haft en betydande påverkan på nät och tjänster.

Bestämmelsen genomför artikel 40.2 första och andra stycket i kodexen som har följande lydelse.

> [Tillhandahållare ska] utan onödigt dröjsmål meddela den behöriga myndigheten om säkerhetsincidenter som har haft en betydande påverkan på driften av nät och tjänster.
>
> För att fastställa hur betydande påverkan en säkerhetsincident har ska särskilt följande parametrar, när sådana finns tillgängliga, beaktas:
>
> a) Det antal användare som påverkas av säkerhetsincidenten.
> b) Hur länge säkerhetsincidenten varar.
> c) Hur stort det geografiska område som påverkas av säkerhetsincidenten är.
> d) Den utsträckning i vilken nätverkets eller tjänstens funktion påverkas.
> e) Den utsträckning i vilken ekonomisk och samhällelig verksamhet påverkas.

I LEK anges inte vad som avses med *betydande påverkan*, men förarbetena hänvisar i denna del till de parametrar som ska beaktas enligt kodexen.[20] Utredningen anser att kraven i 8 kap. 3 § LEK direkt motsvarar kodexens bestämmelser i denna del.

Motsvarande krav i NIS2-direktivet följer av artikel 23 (se kapitel 7). Verksamhetsutövaren är bland annat skyldig att utan onödigt dröjsmål rapportera betydande incidenter till den behöriga myndigheten (artikel 23.1). Avgörande för om en incident ska anses vara betydande (se artikel 23.3) är om den:

1. har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten, eller
2. har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

[20] Prop. 2021/22:136 s. 320 och 495.

Utredningen kan konstatera att kodexen innehåller mer detaljerade bestämmelser än NIS2-direktivet om vad som ska beaktas vid bedömningen av om en incident har haft betydande påverkan och därmed är rapporteringspliktig. Genom utredningens förslag om att regeringen, eller den myndighet regeringen bestämmer, ska få meddela föreskrifter om vad som utgör en betydande incident anser utredningen dock att denna diskrepans mellan direktiven sannolikt kommer att sakna betydelse i den svenska tillämpningen.

11.2.8 Informera allmänheten om incidenter

Av artikel 40.2 tredje stycket i kodexen följer en möjlighet för behöriga myndigheter – om det kan anses ligga i allmänhetens intresse – att informera allmänheten, eller kräva att tillhandahållare ska informera allmänheten, om en säkerhetsincident. Bestämmelsen har genomförts genom 8 kap. 3 § andra stycket LEK.

Bestämmelsen har sin direkta motsvarighet i artikel 23.7 i NIS2-direktivet. Utredningen har även föreslagit en motsvarande möjlighet för tillsynsmyndigheten som i dag följer av LEK (se avsnitt 7.3). Mot denna bakgrund anser utredningen att 8 kap. 3 § andra stycket LEK direkt motsvaras av utredningens föreslagna reglering.

11.2.9 Informera om betydande cyberhot

Enligt artikel 40.3 i kodexen ska tillhandahållare informera sina användare om de kan påverkas av ett betydande hot om en säkerhetsincident i näten eller tjänsterna. De ska även informeras om eventuella skydds- eller motåtgärder som kan vidtas, och om det är lämpligt även om själva hotet. Bestämmelsen har genomförts genom 8 kap. 4 § LEK. Om skyldigheten inte uppfyllts kan PTS besluta om sanktionsavgift (12 kap. 1 § första stycket 6 LEK).

Motsvarande krav att informera om betydande cyberhot följer av artiklarna 23.2, 32.4 e och 33.4 e i NIS2-direktivet. Begreppet cyberhot har redogjorts för i avsnitt 7.3 och 11.3.4 ovan. Enligt utredningens förslag införs en motsvarande skyldighet att informera om betydande cyberhot. Skyldigheten föreslås även kunna leda till samtliga föreslagna sanktioner, däribland sanktionsavgift. Utredningen

bedömer mot denna bakgrund att bestämmelsen i LEK fullt ut motsvaras av den av utredningen föreslagna regleringen.

11.2.10 Ingripanden, sanktioner och vissa tillsynsåtgärder

Av artikel 41 i kodexen följer att tillsynsmyndigheten ska ha vissa befogenheter för att kunna säkerställa efterlevnad av direktivet. Utredningen bedömer att NIS2-direktivets bestämmelser i dessa delar[21] uppenbart omfattar de befogenheter som följer av kodexen.

Utredningen noterar att LEK:s utformning av bestämmelserna om uppgiftsskyldighet (11 kap. 3 §) skiljer sig språkligt mot motsvarande skyldighet enligt den föreslagna cybersäkerhetslagen. Till att börja med omfattar skyldigheten enligt 11 kap. 3 § första stycket LEK ”upplysningar eller handlingar”, kontra det av utredningen föreslagna ”information”. Utredningen anser att begreppet information innefattar både upplysningar och handlingar, varför den av utredningen föreslagna upplysningsskyldigheten är minst lika omfattande som den som följer av LEK i denna del.

Av 11 kap. 3 § andra stycket LEK följer dock även en möjlighet för PTS att förelägga andra aktörer än den aktuella tillhandahållaren att lämna upplysningar eller handlingar. Skyldigheten träffar sådana aktörer som inte omfattas av LEK, men som bedriver verksamhet inom sektorn elektronisk kommunikation. Bestämmelsen gäller vid all form av tillsyn enligt lagen, och är således inte begränsad till tillsyn avseende 8 kap. 1–4 §§ LEK. Av utredningens förslag följer att viss tillsyn som i dag bedrivs enligt LEK i stället kommer att bedrivas enligt cybersäkerhetslagen, där någon motsvarande möjlighet inte föreslås. Det kan därför finnas skäl att överväga om en bestämmelse av sådan innebörd är av betydelse för PTS tillsyn enligt cybersäkerhetslagen.

LEK innehåller möjligheter för PTS att meddela förelägganden för att åtgärda överträdelser av lagens bestämmelser (11 kap. 6 § första stycket 2). Sådana förelägganden kan i vissa fall gälla omedelbart (11 kap. 11 § första stycket 1). Bestämmelserna i LEK genomför både delar av artikel 41 och andra artiklar i kodexen. Det saknas därför skäl att överväga upphävande av dem. Utredningen kan dock konstatera att bestämmelserna – i de delar de genomför artikel 41 – helt

[21] Jfr artiklarna 32–34 i NIS2-direktivet, se vidare kapitel 8–10.

motsvaras av regleringen i utredningens föreslagna cybersäkerhetslag (4 kap. 6 § samt 5 kap. 6 och 21 §§).

Överträdelser av 8 kap. 1–4 §§ LEK kan vara grund för sanktionsavgifter (12 kap. 4–6 §§). Som utredningen bedömt ovan motsvarar skyldigheterna i 8 kap. 1–4 §§ LEK av de som följer av NIS2-direktivet och utredningens föreslagna genomförande. Genom att skyldigheterna i 8 kap. 1–4 §§ LEK föreslås upphävas bör även de korresponderande bestämmelserna om sanktionsavgifter upphävas. Avseende sanktionsavgifternas storlek är maximibeloppet i LEK (12 kap. 2 §) betydligt lägre än enligt NIS2, varför NIS2 inte är begränsande heller i denna del. Utredningen anser mot denna bakgrund att sanktionsavgifterna enligt LEK helt täcks av det föreslagna genomförandet av NIS2-direktivet.

11.2.11 Föreskriftsrätt

PTS har i dag föreskriftsrätt avseende bestämmelserna i LEK om säkerhetsåtgärder (8 kap. 1 §), incidentrapportering (8 kap. 3 § första stycket) och information till användare om betydande hot om säkerhetsincidenter (8 kap. 4 §). Genom utredningens förslag föreslås PTS, i egenskap av tillsynsmyndighet, endast få föreskriftsrätt avseende riskhanteringsåtgärder. Det bör i den fortsatta lagstiftningsprocessen utredas vilka konsekvenser detta medför.

11.3 Slutsatser och följdförslag

Utredningen har ovan gjort bedömningen att artiklarna 40 och 41 i kodexen och hur de har genomförts i LEK motsvaras av NIS2-direktivet och dess föreslagna genomförande i svensk rätt. På motsvarande sätt har utredningen bedömt att den krets som i dag träffas av 8 kap. 1–4 §§ LEK även träffas av NIS2-regleringen. Vidare är det även utredningens bedömning att de ingripanden, sanktioner och tillsynsbefogenheter som i aktuella delar följer av LEK motsvaras av utredningens föreslagna reglering. Som följd är utredningens inriktande förslag att 8 kap. 1–4 §§ LEK ska upphävas och förslag om författningsändringar lämnas därför inklusive de följdändringar som föranleds av ett sådant upphävande. Detta gäller dock inte reservationslöst. Det finns utrymme för närmare överväganden om ett antal

frågor, bland annat att en motsvarighet till LEK:s portalbestämmelse saknas i den föreslagna cybersäkerhetslagen, omfattningen av incidentbegreppet i NIS2-direktivet och ett eventuellt behov av en möjlighet att utfärda förelägganden motsvarande den som finns i 11 kap. 3 § andra stycket LEK vid PTS tillsyn av riskhanteringsåtgärder enligt cybersäkerhetslagen. Det kan även övervägas om en upplysningsbestämmelse bör lyftas in i LEK som informerar om att krav på bland annat incidentrapportering och riskhanteringsåtgärder framgår av den föreslagna cybersäkerhetslagen.

12 Konsekvensanalys

12.1 Allmänt

En utredning ska beskriva konsekvenserna av sina förslag och kraven är angivna i kommittéförordningen (1998:1474). I förordningens 14 § föreskrivs att om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, regioner, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas i betänkandet.

Om förslagen innebär samhällsekonomiska konsekvenser i övrigt ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för det allmänna ska utredningen föreslå en finansiering.

Vidare ska enligt 15 § i förordningen eventuella konsekvenser för den kommunala självstyrelsen redovisas. Detsamma gäller eventuella konsekvenser för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen. Därutöver gäller enligt 15 a § i förordningen särskilda krav för förslag till nya eller ändrade regler. För dem ska konsekvenserna även anges på ett sätt som motsvarar kraven i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning. Av den förordningens 6 § följer att en konsekvensutredning för förslag till nya eller ändrade regler ska innehålla följande:

1. en beskrivning av problemet och vad man vill uppnå,
2. en beskrivning av alternativa lösningar samt effekterna av att en reglering inte föreslås,
3. uppgifter om vem som berörs av regleringen,

4. uppgifter om kostnadsmässiga samt andra konsekvenser regleringen skulle medföra och en jämförelse av konsekvenserna,
5. en bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen (EU), och
6. en bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser.

Av 7 § samma förordning följer att om regleringen kan få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt ska konsekvensutredningen, utöver vad som följer av 6 § och i den omfattning som är möjlig, innehålla en beskrivning av följande:

1. antalet företag som berörs, vilka branscher företagen är verksamma i samt storleken på företagen,
2. tidsåtgången regleringen kan föra med sig för företagen och vad regleringen innebär för företagens administrativa kostnader,
3. andra kostnader den föreslagna regleringen medför för företagen och vilka förändringar i verksamheten som företagen kan behöva vidta till följd av den,
4. i vilken utsträckning regleringen kan komma att påverka konkurrensförhållandena för företagen,
5. hur regleringen i andra avseenden kan komma att påverka företagen, och
6. om särskilda hänsyn behöver tas till små företag vid reglernas utformning.

Av regeringens direktiv följer också därutöver särskilt att utredarens förslag ska utformas så att reglerna blir tydliga och ger så låga administrativa och andra kostnader som möjligt för verksamhetsutövarna. I detta ingår enligt regeringen att bedöma de ekonomiska konsekvenserna av förslagen för de behöriga myndigheterna. Det följer också av direktivet att det i 14 kap. 3 § regeringsformen anges att en inskränkning av den kommunala självstyrelsen inte bör gå utöver vad

som är nödvändigt med hänsyn till ändamålen. Det innebär att en proportionalitetsprövning ska göras under lagstiftningsprocessen. Om något av förslagen i betänkandet påverkar den kommunala självstyrelsen ska utöver dess konsekvenser, också de särskilda avvägningar som lett fram till förslaget särskilt redovisas.

I detta kapitel ska konsekvenserna av utredningens förslag redovisas. Nedan kommer konsekvenserna för förslagen som hänför sig till NIS2 att redovisas.

12.2 Jämställdhet och de integrationspolitiska målen

Inledningsvis bedömer utredningen att förslagen inte berör jämställdheten mellan kvinnor och män eller möjligheterna att nå de integrationspolitiska målen.

12.3 Regleringsalternativ

Utredningens uppdrag har i huvudsak varit att lämna förslag om hur NIS2-direktivet kan införlivas i svensk rätt. Syftet med NIS2-direktivet är att fastställa åtgärder för att uppnå en hög gemensam nivå på cybersäkerhet i nätverks- och informationssystem inom unionen. Det är ett bindande minimidirektiv med innebörd att medlemsstaten får anta bestämmelser som säkerställer en högre cybersäkerhetsnivå. Utredningen har dock med något mindre undantag genomgående utarbetat förslag utifrån minimikraven. Det betyder att den föreslagna regleringen i princip uteslutande är en konsekvens av Sveriges medlemskap i EU och går inte utöver dessa skyldigheter. Förslagen innehåller med undantag av skyldigheten om systematiskt informationssäkerhetsarbete inga krav som syftar till att uppnå en högre nivå av säkerhet än de som följer av direktivet. Effekten av att någon reglering inte kommer till stånd skulle således vara att Sverige inte följer skyldigheterna enligt EU-rätten.

12.4 Vem berörs av förslagen?

NIS2-direktivet ersätter det tidigare NIS-direktivet som införlivades genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagen från 2018 föreslås upphävas genom cybersäkerhetslagen. Den gällande lagen omfattar leverantörer av samhällsviktiga tjänster inom sektorerna energi, transport, bankverksamhet, finansmarknadsstruktur, hälso- och sjukvård, leverans och distribution av dricksvatten och digital infrastruktur. Vidare omfattar lagen digitala tjänster. Sådan verksamhet drivs av statliga myndigheter, kommuner, regioner eller företag.[1]

Cybersäkerhetslagen omfattar såväl offentliga som enskilda verksamhetsutövare. De offentliga är majoriteten av alla myndigheter samt alla regioner och alla kommuner. Därutöver omfattas ett stort antal enskilda verksamhetsutövare. Huvudregeln är att samtliga enskilda verksamhetsutövare inom 18 olika sektorer som är listade i bilaga 1 och 2 till NIS2-direktivet omfattas av lagen under förutsättning att verksamheten är etablerad i Sverige och uppfyller kraven för medelstort företag. Med det avses att verksamheten sysselsätter minst 50 personer eller har en omsättning som överstiger 10 miljoner euro per år. Innebörden av det är att som huvudregel omfattas inte små företag. Definitionen för små företag är alltså att verksamheten sysselsätter mindre än 50 personer och vars omsättning är lägre än 10 miljoner euro.

Därutöver gäller dock att storlekskravet inte behöver vara uppfyllt för vissa utpekade verksamhetsutövare. Det är verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner eller DNS-tjänster. Detsamma gäller för verksamheter som MSB bedömer som är särskilt kritiska, se cybersäkerhetslagen 1 kap.8 §. Det betyder att det skulle kunna finnas små företag bland dessa verksamhetsutövare. Utredningens bedömning är dock att det endast bör vara ett fåtal små företag som återfinns inom denna grupp.

Skillnaden mellan lagen om informationssäkerhet för samhällsviktiga och digitala tjänster och förslaget till cybersäkerhetslag är att den senare omfattar betydligt fler aktörer. Inledningsvis omfattar cybersäkerhetslagen som framgått 18 sektorer i stället för åtta. Det

[1] SOU 2017:36 s. 267.

är också viktigt att notera att om verksamhetsutövaren omfattas så gäller det hela verksamheten. Offentlig verksamhet är en egen sektor, vilket får som följd att hela den offentliga verksamheten omfattas med vissa specifikt angivna undantag, se vidare kapitel 5.

Därutöver omfattas alltså alla enskilda verksamhetsutövare inom sektorerna enligt cybersäkerhetslagen som huvudregel om storlekskravet är uppfyllt. Motsvarande gäller inte för den gällande lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. En förutsättning för att omfattas av den lagen är att leverantören tillhandahåller en samhällsviktig tjänst inom en av sektorerna, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Därutöver omfattas juridiska personer som tillhandahåller en digital tjänst.

12.5 Skyldigheterna för dem som omfattas

Verksamhetsutövarna har vissa skyldigheter. Till att börja med finns det en anmälningsskyldighet om verksamheten till tillsynsmyndigheten, se kapitel 6. Därutöver ska verksamhetsutövaren vidta riskhanteringsåtgärder och, i tillämpliga fall genomföra incidentrapportering. I riskhanteringsåtgärder innefattas utbildning om riskhantering och systematiskt och riskbaserat informationsarbete, se kapitel 7.

Därutöver följer det av cybersäkerhetslagen att myndigheter har uppgifter. Det handlar om tillsynsmyndigheter och MSB. Enligt förslag till cybersäkerhetsreglering är tillsynen delad mellan olika tillsynsmyndigheter. Innebörden är att det finns olika tillsynsmyndigheter för de olika sektorerna. Såväl MSB som merparten av tillsynsmyndigheterna har redan uppgifter enligt nu gällande lag.

12.6 Ekonomiska konsekvenser för tillsynsmyndigheterna och Myndigheten för samhällsskydd och beredskap samt finansiering

I detta avsnitt ska de ekonomiska konsekvenserna för tillsynsmyndigheterna och MSB analyseras samt förslag till finansiering lämnas.

12.6.1 Tillsynsmyndigheternas uppgifter

Av nedanstående tabell följer vem som är tillsynsmyndighet enligt utredningens förslag och deras tillsynsområden.

Tabell 12.1 Tabell över tillsynsmyndigheter

Tillsynsmyndighet	Sektor
Statens energimyndighet	Energi
Transportstyrelsen	Transporter Tillverkning
Finansinspektionen	Bankverksamhet Finansmarknadsinfrastruktur
Inspektionen för vård och omsorg	Hälso- och sjukvårdssektorn, vårdgivare
Läkemedelsverket	Hälso- och sjukvårdssektorn Tillverkning
Livsmedelsverket	Avloppsvatten Dricksvatten Produktion, bearbetning och distribution av livsmedel
Post- och telestyrelsen	Digital infrastruktur Digitala leverantörer Förvaltning av IKT-tjänster Post- och budtjänster Rymden
Länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län	Avfallshantering Forskning Lärosäten med examenstillstånd Offentlig förvaltning
	Tillverkning, produktion och distribution av kemikalier Tillverkning av datorer, elektronikvaror och optik Tillverkning av elapparatur Tillverkning av övriga maskiner

Det handlar alltså om elva myndigheter. Tillsynsmyndigheternas uppgift är att utöva tillsyn över att verksamhetsutövarna uppfyller sina skyldigheter. Om skyldigheterna inte uppfylls ska sanktioner utgå på sätt som följer av kapitel 9.

I första hand ska myndigheterna se till att verksamhetsutövarna uppfyller sin anmälningsskyldighet att lämna uppgifter om verksamheten. Dessa uppgifter ska respektive myndighet registrera och vidarebefordra till MSB. I denna del har tillsynsmyndigheten ingen föreskriftsrätt, eftersom den åvilar MSB. Därutöver ska respektive tillsynsmyndighet bedriva tillsyn över att verksamhetsutövarna uppfyller sina skyldigheter och vidtar riskhanteringsåtgärder, bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete samt uppfyller utbildningskravet om det. Varje tillsynsmyndighet ska också meddela föreskrifter om riskhanteringsåtgärderna, det systematiska informationssäkerhetsarbetet och utbildning, se vidare kapitel 7. Därutöver har verksamhetsutövarna en skyldighet att genomföra incidentrapportering när så ska ske, se avsnitt 7.3 och tillsynsmyndigheterna ska förstås se till att detta efterlevs. MSB ansvarar för föreskriftsrätten för incidentrapportering.

Tillsynsmyndigheterna ska också efter ansökan meddela undantag från storlekskravet för enskilda verksamhetsutövare med följd att verksamhetsutövarna inte omfattas av lagen. Det kan bli aktuellt för partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet, se kapitel 5. Detta beräknas dock endast behöva ske i begränsad utsträckning. Slutligen ska tillsynsmyndigheten även se till att skyldigheten att utse en företrädare enligt 1 kap. 6 § cybersäkerhetslagen efterlevs. Även det bör förekomma endast undantagsvis.

Flera av de elva tillsynsmyndigheterna bedriver redan tillsyn enligt 17 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Tillsynsfördelningen är följande:

Tabell 12.2 Gällande tillsynsfördelning

Tillsynsmyndighet	Sektor
Statens energimyndighet	Energi
Transportstyrelsen	Transport
Finansinspektionen	Bankverksamhet
Finansinspektionen	Finansmarknadsinfrastruktur
Inspektionen för vård och omsorg	Hälso- och sjukvård
Livsmedelsverket	Leverans och distribution av dricksvatten
Post- och telestyrelsen	Digital infrastruktur

Tillsynsmyndigheterna får också meddela föreskrifter om säkerhetsåtgärder avseende riskanalyser, riskhanteringsåtgärder och incidenthantering enligt 12–14 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster för sina respektive tillsynsområden. Socialstyrelsen får dock meddela sådana föreskrifter för Inspektionen för vård och omsorgs tillsynsområde. Det anförda betyder att sex av tillsynsmyndigheterna redan bedriver tillsyn enligt gällande regelverk och fem får meddela föreskrifter, men att dessa skyldigheter komma att upphävas och ersättas av nya tillsynsbestämmelser och nya bestämmelser om föreskriftsrätt.

Därutöver följer av 19 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster att tillsynsmyndigheterna ska lämna uppgifter till MSB, ge allmän vägledning och samarbeta med IMY, samarbetsgruppen och tillsynsmyndigheter i andra medlemsstater.

Det finns dock fem nya tillsynsmyndigheter som inte tidigare bedrivit tillsyn. Dessa är Läkemedelsverket och länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län.

12.6.2 Uppgifter för Myndigheten för samhällsskydd och beredskap

Enligt utredningens förslag till cybersäkerhetslag ska MSB vara gemensam kontaktpunkt och CSIRT-enhet. Det betyder att MSB kommer att ha ett flertal olika uppgifter. Sammantaget ska MSB enligt utredningens förslag ha följande uppgifter:

1. Ta emot det register över verksamhetsutövare från tillsynsmyndigheter och vidarebefordra dem till kommissionen och samarbetsgruppen (avsnitt 6.2),
2. upprätta ett särskilt register över gränsöverskridande verksamhetsutövare och lämna det vidare till Enisa. Uppgifterna och registren ska uppdateras, vilket ger en löpande skyldighet för MSB att vidarebefordra uppgifterna (avsnitt 8.2),
3. meddela föreskrifter om verksamhetsutövarens uppgiftsskyldighet (avsnitt 6.2),

4. vara ett stöd till tillsynsmyndigheterna i deras arbete med att utforma en vägledning till stöd för de enskilde verksamhetsutövarna om vem som omfattas av de olika sektorerna (avsnitt 5.2.12),
5. i föreskrifter peka ut enskilda verksamheter som bedöms vara särskilt kritiska och därför ska omfattas av lagen trots att storlekskravet inte är uppfyllt (avsnitt 5.2.13),
6. utarbeta en vägledning om riskhanteringsåtgärder till stöd för tillsynsmyndigheter (avsnitt 7.1),
7. ansvara för incidentrapportering (avsnitt 7.3),
8. leda ett samarbetsforum där tillsynsmyndigheterna ingår (avsnitt 8.4.7),
9. utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater, kommissionen och Enisa samt ett sektorsövergripande samarbete med tillsynsmyndigheterna (avsnitt 10.1.3),
10. vidarebefordra incidentrapporter till de gemensamma kontaktpunkterna i andra berörda medlemsstater (avsnitt 10.1.3),
11. varje tredje månad lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud (avsnitt 10.1.3),
12. företräda Sverige i samarbetsgruppen (avsnitt 10.1.3),
13. övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå och tillhandahålla varningar (avsnitt 10.2.3),
14. erbjuda stöd avseende realtidsövervakning av nätverks- och informationssystem (avsnitt 10.2.3),
15. ta emot incidentrapporter och vidta åtgärder och erbjuda stöd. Om en incident kan antas ha sin grund i en brottslig gärning ska verksamhetsutövaren skyndsamt uppmanas att anmäla incidenten till Polismyndigheten (avsnitt 10.2.3).
16. samla in och analysera forensiska uppgifter (avsnitt 10.2.3),
17. tillhandahålla dynamiska risk- och incidentanalyser samt situationsmedvetenhet (avsnitt 10.2.3),

18. på begäran utföra en proaktiv skanning av den berörda verksamhetsutövarens nätverks- och informationssystem,
19. delta i det nätverk som inrättats enligt artikel 15 i NIS2-direktivet (CSIRT-nätverket) (avsnitt 10.2.3),
20. vara samordnare för samordnad delgivning av information om sårbarheter (avsnitt 10.2.3), och
21. upprätta samarbetsförbindelser med relevanta intressenter inom privat och offentlig sektor samt bidra till samverkan rörande cybersäkerhet (avsnitt 10.2.3).

MSB har dock redan i dag omfattande uppgifter till följd av regleringen om informationssäkerhet för samhällsviktiga och digitala tjänster. Dessa är likartade dem som föreslås och avser följande:

1. Meddela föreskrifter om vad som utgör samhällsviktiga tjänster och vad som utgör en betydande störning. Begreppen styr vem som omfattas av lagen enligt 3 §,
2. meddela föreskrifter om leverantörernas skyldighet att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster,
3. lämna råd och stöd till tillsynsmyndigheterna när de tar fram föreskrifter om riskanalys, riskåtgärder och incidentåtgärder enligt 12–14 §§ lagen om informationssäkerhet för samhällsviktiga och digitala tjänster,
4. meddela föreskrifter om vad som avses med en betydande inverkan på kontinuiteten i en samhällsviktig tjänst. Begreppet har betydelse, eftersom leverantörer av samhällsviktiga tjänster enligt 18 § i samma lag ska rapportera incidenter ska rapportera incidenter som har sådan betydande inverkan,
5. vara CSIRT-enhet,
6. ta emot incidentrapporter, tillgängliggöra informationen i incidentrapporter för tillsynsmyndigheterna och uppmana leverantörer att till Polismyndigheten anmäla incidenter som kan antas ha sin grund i en brottslig gärning. Vidare ska MSB övervaka incidenter på nationell nivå, tillhandahålla tidiga varningar till relevanta aktörer,

vidta åtgärder till följd av incidenter och tillhandahålla dynamisk risk- och incidentanalys och situationsmedvetenhet,

7. delta i CSIRT-nätverket, bygga upp samarbetsrelationer med den privata sektorn, främja antagandet och användningen av gemensam eller praxis för förfaranden för hantering av incidenter och klassificeringssystem,
8. i vissa fall informera leverantörer, andra medlemsstater och allmänheten om incidenter,
9. på begäran av PTS bistå myndigheten i frågor om hantering av säkerhetsincidenter enligt lagen (2022:482) om elektronisk kommunikation,
10. meddela föreskrifter om incidentrapportering,
11. meddela föreskrifter om anmälningsskyldighet,
12. leda ett samarbetsforum där tillsynsmyndigheterna ingår,
13. vara nationell kontaktpunkt,
14. utöva sambandsfunktion för att säkerställa gränsöverskridande samarbete mellan medlemsstaternas myndigheter och med de berörda myndigheterna i andra medlemsstater samt med samarbetsgruppen,
15. informera samarbetsgruppen,
16. informera andra berörda medlemsstaterna, om incidenter som har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i den medlemsstaten,
17. fullgöra Sveriges skyldighet att samråda med andra medlemsstater samt rapportera resultatet av samrådet till berörd tillsynsmyndighet,
18. vara Sveriges representant i samarbetsgruppen, och
19. fullgöra Sveriges skyldighet att tillhandahålla information om genomförandet av NIS2-direktivet till kommissionen.

12.6.3 Utgångspunkter och bedömning för Finansinspektionen

Utredningens bedömning: Förslagen medför inte ökade kostnader för Finansinspektionen.

Av artikel 8.5 och 11.2 i NIS2-direktivet följer att medlemsstaterna ska säkerställa att deras behöriga myndigheter har tillräckliga resurser för att på ett ändamålsenligt och effektivt sätt utföra de uppgifter de tilldelas och därigenom når målet för direktivet, men det saknas en bestämmelse om hur finansieringen ska ske. Motsvarande bestämmelse fanns i NIS-direktivet. Innebörden är att medlemsstaterna redan accepterat att de behöriga myndigheterna får tillräckliga resurser.

I kommittéförordningen anges som framgår ovan att utredningen ska föreslå en finansiering för kostnadsökningar och intäktsminskningar för det allmänna. Som framgår ovan är flera av de tillsynsmyndigheter som utredningen föreslår redan tillsynsmyndigheter enligt gällande lag. Det gäller Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket och PTS.

Finansinspektionen har samma tillsynsområden. Här ska dock beaktas att utredningen föreslår att finansiella verksamhetsutövare som omfattas av Dora-förordningen inte ska omfattas av riskhanterings- och rapporteringsskyldigheter enligt lagen, se vidare avsnitt 5.4. Som följd kommer då inte heller tillsyns- och efterlevnadskontroll enligt lagen gälla för dem. Innebörden blir att finansiella verksamhetsutövare endast kommer att omfattas av uppgiftsskyldigheten. För Finansinspektionen betyder det att deras uppgifter i vart fall inte bör öka. Det som kommer att återstå är att Finansinspektionen ska se till att de finansiella verksamhetsutövarna lämnar uppgifter och vidarebefordrar dem till MSB. Utredningen drar för Finansinspektionen slutsatsen att kostnaderna inte kommer att öka.

Tillsynsområden är också samma för Statens energimyndighet och Inspektionen för vård och omsorg (IVO). För Statens energimyndighet tillkommer dock verksamhetsutövare inom delsektorerna elektricitet, fjärrvärme eller fjärrkyla, och olja och vätgas.

För IVO skulle det betyda att det endast tillkommer att myndigheten ska meddela föreskrifter, eftersom det arbete tidigare utförts av Socialstyrelsen. Här skulle samtidigt Socialstyrelsens kostnader minska med ungefärligt samma belopp.

För samtliga fem tillsynsmyndigheter, Statens energimyndighet, Transportstyrelsen, IVO, Livsmedelsverket och PTS blir en övergripande skillnad att den gällande lagen är begränsad till samhällsviktiga och digitala tjänster medan förslaget till cybersäkerhetslagen omfattar enskilda verksamhetsutövarna inom sektorn som uppfyller storlekskravet. Vidare omfattas nästan hela den offentliga sektorn enligt utredningens förslag.

Vad skillnaden innebär är oklar och behöver analyseras. Därtill tillkommer att samtliga myndigheter utom IVO får utökade tillsynsområden genom att sektorerna eller som för Statens energimyndighet undersektorerna utökas. Enligt gällande NIS-lag omfattar Transportstyrelsens område endast transport. För Transportstyrelsen tillkommer tillverkning, se vidare kapitel 8. För Livsmedelsverket har tillsynsområdet förändrats från leverans och distribution av dricksvatten till avloppsvatten, dricksvatten och produktion, bearbetning och distribution av livsmedel, se kapitel 8. Slutligen har PTS fått ett utökat tillsynsområde. Tidigare omfattade området endast digital infrastruktur och digitala tjänster, nu tillkommer digitala leverantörer, förvaltning av IKT-tjänster, post- och budtjänster samt rymden, se kapitel 8. För Statens energimyndighet tillkommer alltså verksamhetsutövare inom delsektorerna elektricitet, fjärrvärme eller fjärrkyla, och olja och vätgas. Dessa fyra myndigheter kan till följd av det få ökade kostnader. I vilken utsträckning behöver analyseras vidare.

Vidare tillkommer alltså fem tillsynsmyndigheter, som inte tidigare haft några uppgifter inom ramen för NIS. Läkemedelsverkets tillsynsområde är hälso- och sjukvårdssektorn samt tillverkning. Vidare ska Länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län bedriva tillsyn över avfallshantering, forskning, offentlig förvaltning, tillverkning samt tillverkning, produktion och distribution av kemikalier. Utredningens slutsats för dessa fem myndigheter är förstås att det kommer att medföra ökade kostnader. Hur stora dessa kostnader är behöver analyseras vidare. Här ska dock för länsstyrelserna beaktas att de redan har en etablerad tillsynsorganisation och den kompetens som behövs.

Utredningen har gett Sweco Aktiebolag, Sweco, i uppdrag att analysera de oklarheter som finns i detta avsnitt. Rapporten finns i *bilaga 4.*

12.6.4 Ekonomiska konsekvenser för Bolagsverket och finansiering

Utredningens förslag: De utvecklingskostnader som uppstår för Bolagsverket till följd av utredningens förslag bör finansieras inom befintlig ram.

Utredningen har i kapitel 9 lämnat förslag om införande av förbud att utöva ledningsfunktion. Genom förslaget pekas Bolagsverket och i registreringsansvariga länsstyrelser ut som ansvariga för att avregistrera en förbudsdrabbad individ från sina respektive associationsrättsliga register,[2] samt tillse att denne inte kan registreras på nytt hos verksamhetsutövaren under förbudstiden. Bolagsverket bedömer att det kommer få ökade kostnader om 500 000 kronor till följd av utredningens förslag. Kostnaderna är hänförliga till utveckling av samtliga de IT-system som utgör de företagsregister som verket ansvarar för, och består i att utveckla en ny avregistreringsorsak samt en spärr mot återregistrering. Bolagsverket har angett att kostnaden utgör en engångskostnad och att förslaget i övrigt inte bedöms medföra några ökade löpande förvaltningskostnader. Eftersom dessa förbud inte ska registreras i ett särskilt offentligt register, som till exempel näringsförbudsregistret, behövs enligt verket en särskild teknisk utveckling för utredningens förslag.

Utredningen bedömer att utveckling av befintliga system är en uppgift som redan följer av myndighetens uppdrag. Med hänsyn härtill anser utredningen att den kostnad som föranleds av förslaget bör finansieras inom befintligt budgetutrymme.

12.6.5 Övriga tillsynsmyndigheter och Myndigheten för samhällsskydd och beredskap – bakgrund

Vid val av metod för beräkning av kostnaderna och finansiering för tillsynsmyndigheternas och MSB:s kostnader har utredningen tagit ledning av överväganden och beslut om kostnader och finansiering vid införandet av gällande NIS-lag. Det handlar såväl om NIS-utred-

[2] Avseende Bolagsverket framgår dessa register av 1 § 1–3 förordningen (2007:1100) med instruktion för Bolagsverket.

ningen som Statskontorets bedömning och regeringens beslut om anslag.

NIS-utredningen

Den utredning som föreslog genomförandet av NIS-direktivet (NIS-utredningen) bifogade i sitt betänkande förstås en konsekvensanalys.[3] Utredningen delade upp kostnaderna i initiala och löpande. De initiala kostnaderna skulle avse bland annat utarbetandet av nya föreskrifter, bygga upp system för tillsyn, rekrytera eller utveckla ny kompetens. Utredningen bedömde att samtliga sex tillsynsmyndigheter skulle behöva förstärkas med två årsarbetskrafter under 2018.[4] En årsarbetskraft motsvarar cirka en miljon kronor. Innebörden skulle alltså vara att varje tillsynsmyndighet skulle behöva tillföras två miljoner kronor avseende initiala kostnader. Därutöver menade dock utredningen att varje tillsynsmyndighetskulle ha löpande kostnader för tillsyn och administrativa sanktioner. Dessa skulle dock variera beroende på antal leverantörer som skulle komma att omfattas. Utredningen kunde inte bedöma denna kostnad, utan föreslog att Myndigheten för samhällsskydd och beredskap med stöd av tillsynsmyndigheterna gavs i uppdrag att göra en uppskattning av hur många leverantörer av samhällsviktiga tjänster som fanns inom varje sektor. Därefter föreslogs att Statskontoret skulle ges i uppdrag att lämna ett förslag på genomförande och finansiering.[5]

När det gällde finansiering övervägde utredningen en avgiftsfinansierad tillsyn. Utredningen anförde följande:

> När det gäller finansiering av kostnader för att utöva tillsyn har utredningen övervägt en avgiftsfinansierad tillsyn. Av regeringens skrivelse, En tydlig, rättssäker och effektiv tillsyn, framgår bland annat att tillsyn i normalfallet bör finansieras genom avgifter. Det kan dock inom vissa områden vara mer lämpligt att låta tillsynen finansieras via skattemedel. Det kan exempelvis vara fallet när kostnaderna för att administrera ett avgiftsuttag bedöms som höga i relation till avgiften i övrigt. Det kan också finnas fördelningspolitiska och effektivitetsmässiga eller andra bärande motiv att låta tillsynen finansieras med skattemedel, särskilt inom områden där tillsynen riktas mot statligt och kommunalt finansierad verksamhet. En tillsynsavgift bör motsvaras av en tydlig motprestation, uppfattas som rättvis samt inte vara konkurrenssnedvridande. Av-

[3] SOU 2017:36 s. 265 ff.
[4] Se s. 271.
[5] SOU 2017:36 s. 272.

gifterna bör vara lättbegripliga och förutsebara för de objektsansvariga och ge incitament till avsedda beteenden hos tillsynsorganen och de objektsansvariga.

Utredningen bedömde därefter att när det gällde sådan verksamhet som omfattades av den föreslagna lagen var det svårt att bedöma omfattningen av den tillsyn som skulle genomföras. Sektorernas verksamhet skiljde sig åt liksom komplexiteten i de olika nätverken och informationssystemen. Den snabba tekniska utvecklingen liksom samhällets digitalisering kunde också få stora effekter på tillsynsverksamhetens omfattning och innehåll. Därtill menade utredningen att den verksamhet som skulle omfattas delvis fanns inom stat, region eller kommun. Förutsättning för en avgiftsfinansierad tillsyn var enligt utredningen att det var känt vilka leverantörer som omfattades och att kontroller sker hos samtliga som betalar tillsynsavgift. Detta var dock inte fallet för utredningens förslag. Därutöver menade den utredningen också att det var svårt att bestämma avgifterna, eftersom såväl antalet leverantörer som kommer att omfattas och komplexiteten i den verksamheten var oklar. Förslaget var därför att tillsynen i vart fall inledningsvis skulle vara anslagsfinansierad och fördelas på de utgiftsområden som respektive sektor tillhör.

Utredningen menade också att kostnaderna till viss del, i vart fall på lång sikt, kunde finansieras genom samhällsekonomiska vinster som en hög gemensam nivå av säkerhet i nätverk och informationssystem medför för respektive sektor.[6]

Statskontorets rapport och regeringens anslag

Under den fortsatta beredningen av betänkandet gav regeringen Statskontoret i uppdrag att utreda de ekonomiska konsekvenserna för MSB och de myndigheter som fått ansvar för tillsynen. I uppdraget ingick också att utreda om tillsynsverksamheten borde finansieras med avgifter. Oavsett bedömning i den frågan skulle Statskontoret också utreda hur en avgiftsfinansiering kunde utformas för varje sektor. Statskontoret redovisade uppdraget i rapporten, *Tillsyn enligt NIS-direktivet – kostnader och finansiering*, 2018:7, som publicerades i mars 2018.[7]

[6] SOU 2017:35 s. 271–272.
[7] https://www.statskontoret.se/publicerat/publikationer/publikationer-2018/tillsyn-enligt-nis-direktivet--kostnader-och-finansiering/?publication=true, inhämtat 2024- 01-16.

I rapporten redovisas såväl initiala som löpande kostnader. Uppgifterna bygger i sin helhet på preliminära uppskattningar från de sex tillsynsmyndigheterna och MSB. Statskontoret bedömde att myndigheternas uppgifter vilade på någorlunda stabil grund, men noterade också att myndigheterna fann det svårt att uppskatta kostnaderna och att det fanns en stor spridning i bedömningarna hos myndigheterna. Statskontoret menade att det var möjligt att uppskatta de ekonomiska konsekvenserna mer exakt när tillsynsobjekten var kända.[8]

Sammanlagt uppskattade de sex tillsynsmyndigheterna de initiala kostnaderna till sammanlagt 17,2 miljoner kronor, men variationen mellan myndigheterna var stor.

De löpande kostnaderna för de sex tillsynsmyndigheterna bedömdes av dem till sammanlagt cirka 60 miljoner kronor per år.[9]

Avseende MSB anförs i rapporten följande:

> MSB:s uppgifter är bland annat att vara nationell kontaktpunkt, att leda ett samarbetsforum för tillsynsmyndigheterna samt att representera Sverige i EU. MSB ska utveckla ett system för att ta emot och analysera incidentrapporter. I uppgifterna ingår också att ta fram föreskrifter för arbetet med tillsyn, stödja myndigheterna med tillsynsmetodik samt att informera om regler och krav.
>
> Enligt MSB behöver myndigheten avsätta 10–11 årsarbetskrafter för sitt arbete med NIS-direktivet. MSB uppskattar sina totala kostnader för genomförandet till 14 miljoner kronor per år, inklusive overheadkostnader. Statskontoret ifrågasätter inte MSB:s uppskattning, men vi konstaterar att de ekonomiska konsekvenserna i hög grad beror på hur MSB väljer att genomföra de nya uppgifterna.[10]

När det särskilt gällde incidentrapportering uppgav MSB till Statskontoret att man uppskattade att antalet incidentrapporter skulle kunna bli flera tusen samt att antalet incidentrapporter som skulle omhändertas med stor sannolikhet skulle komma att mångdubblas (under 2017 tog CERT-SE emot drygt 300 incidentrapporter från statliga myndigheter).[11]

[8] Avsnitt 7.1.
[9] Avsnitt 4.8.
[10] Se sammanfattningen.
[11] Avsnitt 2.1.

Sammanlagt bedömde tillsynsmyndigheterna behovet av initiala kostnader och löpande kostnader på följande sätt i tusen kronor:

Tabell 12.3 Myndigheternas bedömning

Myndighet	Initiala kostnader	Löpande kostnader
Energimyndigheten	200	8 000
Transportstyrelsen	4 000	15 000
Finansinspektionen	3 000	3 000
IVO	3 500	19 200
Livsmedelsverket	10 000	9 000
PTS	Kan ej uppge	5 200
Totalt	**17 200**	**59 400**

Av vårändringsbudgeten för 2018 följer sedan att Energimyndigheten tillerkändes 2,5 miljoner kronor, Transportstyrelsen 4 miljoner, Finansinspektionen 3 miljoner kronor, IVO 3,5 miljoner, Livsmedelsverket 10 miljoner och PTS 4 miljoner kronor. Innebörden är alltså att regeringen när det gällde ersättning för de initiala kostnaderna följde myndigheternas bedömningar som redovisades i Statskontorets rapport.

När det gäller löpande kostnader har det varit svårare för denna utredning att få en klar bild, särskilt avseende Energimyndigheten, Transportstyrelsen och Finansinspektionen. Det följer dock av Budgetpropositionen för 2019[12] att PTS fick ökat anslag med 5,2 miljoner för varje år under tiden för 2019–2021 avseende NIS-lagen. IVO tillerkändes 10 miljoner per år i ökat anslag och för Livsmedelsverket ökades anslaget med 9 miljoner per år från 2019. Rimligen har även Energimyndigheten och Transportstyrelsen erhållit anslagsförstärkningar under dessa år. Det betyder att regeringen följt bedömningarna i rapporten från PTS och Livsmedelsverket, men halverat den summa som IVO angett och som redovisades i rapporten.

MSB bedömde alltså sina kostnader till 14 miljoner kronor per år. I vårändringsbudgeten för 2018 tillerkändes MSB 7 miljoner, dvs. även här valde regeringen att halvera beloppet. För senare år är det rimligt att även MSB erhållit ökade anslag, men omfattningen har inte kunnat klarläggas.

[12] 2018/19:1 utgiftsområde 22, s. 101.

När det gällde avgiftsfinansiering ansåg Statskontoret inte att tillsynen enligt NIS-direktivet borde finansieras med avgifter. Inledningsvis anförde Statskontoret att det generellt finns goda skäl för en avgiftsfinansiering. Det hänvisades till att avgiftsfinansiering bör vara huvudregeln för tillsyn, eftersom det tydliggör kostnaden och avlastar statsbudgeten. Samtidigt anfördes att avgiftsfinansiering alltid bör vara fallet för verksamhetsutövare utanför den offentliga sektorn. Huvudsakliga skälet mot avgiftsfinansiering i detta fall var dock enligt Statskontoret risken för konkurrenssnedvridande effekter och höga administrationskostnader. Därutöver fanns det svårigheter att utforma tillsynen över sektorerna på ett enhetligt sätt och en svårighet att påvisa en tydlig motprestation för avgiften. Statskontorets analys byggde på intervjuer med tillsynsmyndigheterna och den visade att nackdelarna med en sådan finansieringsform vägde tyngre än fördelarna för fem av de sex aktuella myndigheterna.

Statskontoret föreslog därför att tillsynen enligt NIS-direktivet skulle finansieras med anslag, se vidare avsnitt 5 i rapporten.

I rapporten för Statskontoret även fram att regeringen bör ställa krav på att myndigheterna åtminstone för de närliggande åren att redovisa tillsynsverksamhetens kostnader och prestationer, det vill säga framför allt antalet utförda tillsyner. Det skulle också bidra till att effektivisera tillsynen, eftersom myndigheternas kostnader och prestationer i viss mån skulle kunna jämföras med varandra. Därutöver skulle redovisningen minska riskerna för att verksamheten korssubventioneras genom andra anslag.[13]

12.6.6 Swecos uppdrag och rapport

Swecos uppdrag har berört tio tillsynsmyndigheter och MSB, som samordnande myndighet. De tio tillsynsmyndigheterna är Statens Energimyndighet, Transportstyrelsen, IVO, Läkemedelsverket, Livsmedelsverket, PTS, samt länsstyrelserna i Norrbotten, Skåne, Stockholm och Västra Götaland. Av dessa tio tillsynsmyndigheter har alltså fem redan uppdrag som tillsynsmyndigheter enligt gällande NIS-reglering. Dessa fem är alltså Statens Energimyndighet, Transportstyrelsen, IVO, Livsmedelsverket och PTS. För dem handlar det om att klarlägga om kostnaderna ökar. Övriga fem myndigheter,

[13] Avsnitt 7.3.

dvs. fyra länsstyrelser och Läkemedelsverket har inte haft några tillsynsuppdrag tidigare om NIS. För dem ska kostnaderna beräknas, men här behöver också – i vart fall i större omfattning – de initiala kostnaderna för att bygga upp tillsynsverksamheten beaktas.

MSB är redan samordnande myndighet enligt gällande NIS-reglering och för den myndigheten handlar det därför om uppgifterna och som en följd även kostnaderna kan förväntas öka. Enligt uppdraget skulle även möjlig EU-finansiering klarläggas. Utgångspunkt är den analys som Statskontoret genomförde och de beslut regeringen fattade om anslag för gällande NIS-regelverk 2018.

Sweco har kontaktat samtliga berörda myndigheter med önskemål om intervju. Länsstyrelserna i Norrbotten och Västra Götaland har dock inte önskat medverka. Länsstyrelsen i Norrbotten svarade inte på förfrågan om intervju och länsstyrelsen i Västra Götaland ville inte lämna uppgifter.

Övriga myndigheter intervjuades. Frågor skickades ut på förhand till myndigheten. Det som efterlystes var uppgifter om initiala och löpande kostnadsuppskattningar under en tre-årsperiod. Under intervjuerna uppstod för samtliga dessa myndigheter ett behov av komplettering av lämnade uppgifter. Efter intervjun sammanställde Sweco uppgifterna och skickade underlaget till myndigheterna för komplettering och verifiering. Endast fyra myndigheter återkom med svar. Från Sweco har påpekats att uppdraget förutsätter att berörda myndigheter bistår med kostnadsunderlag och annan relevant information.

Enligt Swecos rapport bedömer tillsynsmyndigheterna och MSB att de under en treårsperiod totalt skulle ha kostnader på grund av införlivningen av NIS2-direktivet på cirka 385 miljoner kronor. Kostnaderna avser delvis såväl initiala kostnader som löpande kostnader.

Statens Energimyndighet uppskattar sin kostnad till cirka 11–17 miljoner kronor för treårsperioden. Uppskattningen grundar sig på att antalet tillsynsobjekt förväntas fördubblas. Enligt Sweco ska siffran bedömas med stor försiktighet, särskilt som myndigheten inte återkommit och verifierat Swecos beräkning.

Transportstyrelsen uppskattar sin kostnad till 18 miljoner kronor per år, dvs. sammanlagt för treårsperioden skulle kostnaden vara 54 miljoner kronor. Därtill skulle komma en uppstartskostnad på 770 000 kronor. Antalet tillsynsobjekt skulle öka från 130 till 750. Det skulle innebära att antalet årsarbetskrafter skulle behöva öka

från 5 till 15. Antalet tillsyner år 2022 var tre och det fanns då två årsarbetskrafter till en kostnad av 2 miljoner kronor. År 2025 skulle antalet tillsyner kunna vara 150, antalet årsarbetskrafter 15 och kostnaden 18 miljoner kronor. För tre år blir summan 54 miljoner kronor. Swecos bedömning är att Transportstyrelsen har inkommit med det mest kompletta underlaget, men den kostnadspost som saknas är kostnaderna för teknisk utveckling och systemstöd.

IVO uppskattar sin kostnad preliminärt till 38 miljoner kronor. Bedömningen vilar på att antal tillsynsobjekt skulle öka från 240 till 819. Under 2022 genomförde myndigheten tillsyn i 13 fall till en kostnad av cirka 8 miljoner kronor.

Livsmedelsverket uppskattar sin kostnad för treårsperioden till cirka 26 miljoner kronor. Myndigheten bedömer att antalet tillsynsobjekt kommer att öka från cirka 100 till cirka 525–675. Det skulle leda till ett behov av ytterligare åtta årsarbetskrafter till totalt 16. Enligt Sweco är beräkningarna osäkra, eftersom de inte verifierats av myndigheten.

PTS har till utredningen anfört att de angivna kostnaderna i rapporten är felaktiga. Myndigheten bedömer sina löpande kostnader till 18 miljoner kronor för treårsperioden, men här saknas uppskattning om initiala kostnader. Bedömningen grundar sig på att antalet tillsynsobjekt kommer att öka från 60 till 1 100, men det finns en del osäkerhet i ökningen. En komplikation är att 700 aktörer av de 1 100 i dag omfattas av LEK-regelverket, men framöver kommer att hänföras till NIS2-regleringen. För närvarande arbetar 5,5 årsarbetskrafter med tillsyn för gällande NIS-lag och åtta med tillsyn över LEK, som framöver kommer att höra till NIS-regleringen. Myndigheten bedömer att det finns ett behov av ytterligare sammanlagt 15 årsarbetskrafter. Av dessa arbetar dock åtta alltså redan med tillsyn enligt LEK-regleringen. Det betyder att det skulle behöva tillföras totalt sju helt nya årsarbetskrafter och den kostnaden beräknas till 21 miljoner för treårsperioden. Skulle dock även kostnaden för de åtta årsarbetskrafter som i dag arbetar med tillsyn enligt LEK ingå uppskattas de löpande kostnaderna till 45 miljoner kronor. Utredningen noterar att det bör finnas möjliga kostnadsminskningar för PTS till följd av att myndigheten inte längre kommer vara första mottagare av NIS2-verksamhetsutövarnas incidentrapporter, som i stället ska skickas till CSIRT-enheten först och därefter lämnas till PTS. PTS synes inte ha bedömt någon sådan kostnadsminskning.

När det gäller myndigheter som inte tidigare haft tillsynsuppdrag uppskattar Läkemedelsverket preliminärt kostnaden till 70 miljoner kronor, men med det tillägget att hänsyn inte tagits till vad tillsynen de facto kommer att innebära. Verket betonar att kostnadsuppskattningarna är preliminära och kommer att behöva kompletteras.

De fyra länsstyrelserna ansvarar redan för tillsyn enligt säkerhetsskyddslagen, varför länsstyrelsen i Skåne utgått från kostnaderna för breddning av tillsynsverksamheten. Det uppskattas att det behövs ytterligare fyra årsarbetskrafter för det löpande arbetet, samt en årsarbetskraft under ett år för att starta upp verksamheten, sammanlagt till en kostnad av 13 miljoner kronor för tre år. I beräkningen ingår alltså enbart årsarbetskraft. Länsstyrelsen i Stockholm har uppskattat kostnaden till 23 miljoner för årsarbetskraft, varav en årsarbetskraft avseende information under ett år och fem årsarbetskrafter under treårsperioden. Länsstyrelserna i Norrbotten och Västra Götaland har alltså inte inkommit med uppgifter.

MSB har uppskattat sina kostnader för tre år till totalt cirka 131 miljoner kronor. Det är kostnadsuppskattningar för att stärka organisatoriska och tekniska förmågor samt teknisk utveckling. Utredningen förstår då detta som att det är tillkommande belopp utöver den budgetfinansiering MSB uppbär på grund av gällande NIS-reglering. Som grund för bedömningen har myndigheten uppgett att beloppet avser organisatoriska förmågor och teknisk utveckling. För att stärka organisatoriska och tekniska förmågor skulle det krävas 15,7 årsarbetskrafter till en total kostnad av 47,1 miljoner kronor för tre år. Därutöver anges tillkommande kostnader till 65,5 miljoner kronor utan närmre precisering. Vidare skulle kostnaden för teknisk utveckling kräva 6,4 årsarbetskrafter till en kostnad av 6,4 miljoner kronor och tillkommande kostnader vara 12 miljoner kronor. Av Swecos rapport framgår inga uppgifter om EU-finansiering för MSB. Myndigheten har dock till utredningen anfört att MSB fått ett preliminärt besked om att den beviljats EU-medel för arbetet med att utveckla CSIRT-enheten och den nationella kontaktpunkten så att de svarar upp mot NIS2. Ett villkor är att halva beloppet finansieras nationellt.

12.6.7 Utredningens förslag – ekonomiska konsekvenser för tillsynsmyndigheterna och för Myndigheten för samhällsskydd och beredskap

Utredningens förslag:

1. Regeringen bör ge Statskontoret i uppdrag att klarlägga de löpande kostnaderna för tillsynsmyndigheterna och Myndigheten för samhällsskydd och beredskap för tiden från 1 januari 2026.
2. Regeringen bör för år 2025 ge Statens energimyndighet, Transportstyrelsen, Inspektionen för vård och omsorg, Livsmedelsverket och Post- och telestyrelsen ett förstärkt anslag för löpande kostnader med två miljoner kronor vardera.
3. Regeringen bör för år 2025 ge Myndigheten för samhällsskydd och beredskap ett förstärkt anslag med två miljoner kronor för löpande kostnader.
4. Läkemedelsverket och länsstyrelserna i Skåne, Stockholms, Västra Götalands och Norrbottens län bör som initialkostnad få ett anslag om fem miljoner vardera.
5. Kostnaderna för myndigheternas tillsyn ska inte avgiftsfinansieras utan anslagsfinansieras.
6. Regeringen bör under de första åren efter det att cybersäkerhetsregleringen trätt i kraft ställa ett återrapporteringskrav för tillsynsmyndigheterna och MSB.

Tillsynsmyndigheternas kostnader och kostnader för MSB

Det är utredningens uppgift att klarlägga de ekonomiska konsekvenserna för tillsynsmyndigheterna och MSB. Samtidigt kan utredningen bara fullgöra denna uppgift om myndigheterna lämnar uppgifter för utredningen att analysera och bedöma.

Som framgått har utredningen valt samma arbetsmetod som användes av Statskontoret vid implementeringen av NIS-direktivet.

Att uppskatta kostnaderna är självfallet oerhört komplicerat. Som framkommit ovan hade tillsynsmyndigheterna när NIS-direktivet införlivades svårigheter att uppskatta dem. Samtidigt var de kompletta och Statskontoret bedömde att de vilade på stabil grund.

Så är inte förhållandet för utredningen. Uppgifterna är i nuläget många gånger ofullständiga och två myndigheter har valt att inte lämna uppgifter. Den arbetsmetod som Sweco använde sig av var också att genomföra intervjuer och sen sammanställa ett skriftligt underlag, som skickades till myndigheten för komplettering och verifiering. Endast fyra myndigheter har återkommit med komplettering och verifiering. Sweco gör också den övergripande bedömningen att det inte nog går att understryka att kostnadsberäkningarna från myndigheterna bör kompletteras för att få en tillförlitlig bild av vad införandet av NIS2-direktivet kommer att innebära.

Sammantaget gör utredningen den bedömningen att det för närvarande inte är möjligt att dra tillförlitliga slutsatser om de löpande kostnaderna för tillsynsmyndigheterna under en treårsperiod utan delar Swecos bedömning om att det krävs kompletteringar. Utredningen förslår därför att regeringen på samma sätt som vid beredningen av NIS-direktivet ger ett uppdrag till Statskontoret att komplettera Swecos underlag. Samtidigt föreslås dock cybersäkerhetsregleringen träda i kraft redan 1 januari 2025. Det betyder att hänsyn behöver tas till myndigheternas ökade kostnader redan vid den budgetberedning som inleds i Regeringskansliet i maj 2024. En lösning är att utredningen skönsmässigt uppskattar den budgetförstärkning som de angivna tillsynsmyndigheterna kan behöva för 2025, men att Statskontoret fortsatt utreder de löpande kostnaderna för tiden därefter. Skälet för att tillsynsmyndigheterna bör ha utökade resurser för 2025 är att myndigheterna ska kunna identifiera vilka verksamhetsutövare som omfattas av den nya lagen, utfärda nya föreskrifter och nya vägledningar utan att samtidigt behöva minska ambitionen med tillsyn.

När det gäller initialkostnader för att bygga upp tillsynsverksamheten menar dock utredningen att de fem myndigheter som bedriver tillsyn redan har byggt upp en organisation. För dessa myndigheter menar utredningen att det inte behövs särskilda anslag för initiala kostnader. När det gäller de fem nya tillsynsmyndigheterna bedömer utredningen att dessa fem myndigheter precis som vid införlivandet av NIS-direktivet behöver få medel för att kunna starta upp verksamheten. Utifrån vad länsstyrelsen i Skåne i denna del anfört

och med hänsyn till de belopp som anslogs för detta ändamål vid införlivandet av NIS-direktivet föreslår utredningen att detta belopp bestäms till fem miljoner kronor per myndighet.

Som framgått har MSB bedömt att myndigheterna utifrån sitt uppdrag kommer att behöva tillkommande resurser under en treårsperiod på 131 miljoner kronor, vilket skulle motsvara cirka 44 miljoner kronor om året.

Utredningen noterar att kostnaden är hög, särskilt med hänsyn till de bedömningar som gjordes vid införlivningen av NIS-direktivet som av MSB bedömdes till 14 miljoner kronor per år och av regeringen till 7 miljoner. Av den jämförelse utredningen genomfört i 12.6.2 av myndighetens uppgifter enligt gällande lag och framöver följer också att uppgifterna är snarlika. Däremot är det förstås så att betydligt fler verksamheter kommer att omfattas av cybersäkerhetslagen än den gällande NIS-lagen. Enligt utredningens uppfattning behöver det närmare analyseras i vilken utsträckning det kommer att påverka myndighetens uppdrag. Flera kostnader är i nuläget inte heller specificerade eller förklarade av myndigheten.

MSB har bland annat anfört att den främsta kostnaden avseende teknisk utveckling avser utveckling av WIS (webbaserat informationssystem). Systemet används för att dela, samla in och sammanställa information samt omvärldsbevakning. Systemet har i dag över 10 000 användare från myndigheter, kommuner, regioner, frivilligorganisationer och privata aktörer som har en roll i Sveriges krisberedskap eller civila försvar.[14] Utredningen anser att det är oklart på vilket sätt de angivna kostnaderna är motiverade utifrån NIS2, och i vilken mån de överstiger MSB:s befintliga medel för förvaltning och vidareutveckling av WIS.

Som framgår ovan av avsnitt 12.6.5 uppgav MSB 2018 att antalet incidentrapporter enligt gällande NIS-lag skulle kunna bli flera tusen och att antalet incidentrapporter som skulle behöva omhändertas med stor sannolikhet skulle mångdubblas. Enligt MSB:s årsrapport *It-incidentrapportering 2022*[15] har detta visat sig vara en felaktig uppskattning. Totalt har antalet rapporterade it-incidenter sedan 2019 legat på drygt 300.

[14] https://www.msb.se/sv/verktyg--tjanster/wis/om-wis/, hämtat januari 2024.
[15] s. 17.

Sweco har anfört att kostnaderna är preliminära och kan komma att revideras av MSB och att det inom myndigheten pågår ett analysarbete om framtida kostnader. Därtill kommer att MSB upplyst om att EU-bidrag kan komma att utgå.

Sammantaget gör utredningen för dessa kostnader samma bedömning som för tillsynsmyndigheternas uppskattningar. Det går i nuläget inte att dra någon slutsats av uppgifterna, varför underlaget behöver kompletteras på samma sätt som för tillsynsmyndigheterna i ett senare skede. För 2025 bör MSB på motsvarande sätt som tillsynsmyndigheterna få ett förstärkt anslag med två miljoner kronor. När det särskilt gäller kostnaden för WIS, menar utredningen att den kostnaden bör rymmas inom befintlig budgetram. Vidare behöver det beaktas att bedömningarna som låg till grund avseende incidentrapportering 2018 var överskattade.

Avgifts- eller anslagsfinansiering?

Från Finansdepartementet har anförts att utredningen bör överväga en avgiftsfinansiering. Som framgår ovan har dock denna fråga utretts i närtid av såväl Utredningen om genomförande av NIS-direktivet som Statskontoret. Utredningen drog slutsatsen att förutsättningen för en avgiftsfinansierad tillsyn var att det var känt vilka leverantörer som omfattades och att kontroller sker hos samtliga som betalar tillsynsavgift. Detta var dock inte fallet för den utredningens förslag. Därutöver menade den utredningen också att det var svårt att bestämma avgifterna, eftersom såväl antalet leverantörer som skulle omfattas och komplexiteten i verksamheten var oklar. Verksamheten som skulle omfattas fanns också delvis fanns inom stat, region eller kommun. Förslaget var därför att tillsynen i vart fall inledningsvis skulle vara anslagsfinansierad.

För NIS2-direktivet gäller detta i än högre grad. Det är delvis oklart vilka enskilda verksamhetsutövare som kommer att omfattas och utredningen har också därför i kapitel 5 föreslagit att regeringen ger tillsynsmyndigheterna i uppdrag att med stöd av MSB skyndsamt utarbeta en vägledning. En stor andel utgörs också av offentliga verksamhetsutövare, eftersom alla myndigheter med några undantag, samt samtliga regioner och kommuner kommer att omfattas. Antalet verksamhetsutövare som kommer att omfattas är alltså betydligt fler än

tidigare, vilket innebär också innebär att endast en begränsad andel kan komma att tillsynas.

Statskontoret drog slutsatsen att tillsynen enligt NIS-direktivet inte borde finansieras med avgifter. Huvudsakliga skälet mot avgiftsfinansiering var enligt Statskontoret risken för konkurrenssnedvridande effekter och höga administrationskostnader. Därutöver fanns det svårigheter att utforma tillsynen över sektorerna på ett enhetligt sätt och en svårighet att påvisa en tydlig motprestation för avgiften, se vidare Statskontorets rapport.[16]

Sammantaget ansluter sig utredningen till tidigare bedömningar och menar att argumenten i hög grad har bäring även för NIS2-tillsynen.

Återrapportering

Som framgått av detta kapitel kommer ett stort antal verksamhetsutövare att omfattas av NIS2-regleringen, vilket i sin tur utifrån förslaget om en anslagsfinansiering skulle medföra stora kostnader för staten. Statskontoret förde i sin rapport 2018 fram att regeringen avseende NIS-regleringen borde ställa krav på att myndigheterna åtminstone under några år redovisar tillsynsverksamhetens kostnader och prestationer, det vill säga framför allt antalet utförda tillsyner. En sådan redovisning skulle enligt Statskontoret ge regeringen möjlighet att justera resurserna om den väljer att finansiera tillsynen med anslag. Det skulle också bidra till att effektivisera tillsynen, eftersom myndigheternas kostnader och prestationer i viss mån skulle kunna jämföras med varandra. Därutöver skulle redovisningen minska riskerna för att verksamheten korssubventioneras genom andra anslag.[17]

Utredningen ansluter sig till detta förslag för NIS2-regleringen och menar att återrapporteringen även bör omfatta MSB som samordnande myndighet.

[16] https://www.statskontoret.se/publicerat/publikationer/publikationer-2018/tillsyn-enligt-nis-direktivet--kostnader-och-finansiering/?publication=true#_Toc508707866, inhämtat januari 2024.
[17] Se avsnitt 7.3.

12.7 Ekonomiska konsekvenser för offentliga verksamhetsutövare

Utredningens bedömning: Kostnaderna för offentliga verksamhetsutövare ska finansieras inom befintlig budgetram.

Som framgått tidigare omfattas i princip hela den offentliga sektorn av cybersäkerhetsregleringens krav. Det betyder alla myndigheter med några få undantag samt samtliga regioner och kommuner med undantag av region- och kommunstyrelse. Det är en stor förändring jämfört med dagens krav, eftersom offentliga verksamhetsutövare bara i enstaka fall omfattas av gällande NIS-lag.

Det handlar om en anmälningsskyldighet om verksamheten till tillsynsmyndigheten, se kapitel 6. Därutöver ska verksamhetsutövaren vidta riskhanteringsåtgärder och i tillämpliga fall genomföra incidentrapportering. I riskhanteringsåtgärder innefattas utbildning om riskhantering och ett systematiskt och riskbaserat informationsarbete, se kapitel 7.

Utredningen bedömer att kraven inte kan beskrivas som omfattande, men samtidigt är de tillräckligt ingripande för att verksamhetsutövaren behöver avsätta resurser. Här bör det särskilt handla om skyldigheten att vidta riskhanteringsåtgärder, eftersom anmälningsskyldigheten bör kräva ett försumbart arbete och incidenthanteringen bara aktualiseras vid problem. Tidsåtgången kommer att vara beroende av verksamhetens storlek.

SKR har hänvisat till finansieringsprincipen. Den principen innebär att kommuner och regioner inte ska behöva höja skatten eller prioritera om sin verksamhet för att finansiera nya statliga uppgifter. Den innebär enligt SKR att inga nya obligatoriska uppgifter från staten får införas utan medföljande finansiering till kommuner och regioner.[18]

Samtidigt menar utredningen att det är rimligt att offentliga verksamhetsutövare vidtar grundläggande säkerhetsåtgärder. Åtgärderna för att förebygga incidenter kan också förhindra eller begränsa incidenter och genom incidenthantering erhåller verksamhetsutövaren stöd.

[18] https://skr.se/skr/ekonomijuridik/ekonomi/finansieringsprincipen.1709.html, inhämtat 2024-01-30.

På samma sätt som anfördes redan i betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster*[19] kommer enhetliga regler, tillsyn och möjligheten att få upplysningar av tillsynsmyndigheten att bidra till minskade kostnader för verksamhetsutövaren.

Sammantaget bedömer utredningen att förslagen medför kostnader för offentliga verksamhetsutövare, men övergripande för hela offentliga sektorn även besparingar. De ekonomiska konsekvenserna föreslås därför finansieras inom verksamhetsutövarens befintliga budgetram.

12.8 Ekonomiska konsekvenser för enskilda verksamhetsutövare

De enskilda verksamhetsutövare som omfattas av utredningens förslag är verksamhetsutövare som innefattas i de sektorsbeskrivningarna som finns i bilaga 1 eller 2 i NIS2-direktivet. Därtill kommer enskilda lärosäten med examenstillstånd. För de flesta sektorerna är det tydligt vem som omfattas, men för några krävs en analys. Utredningen har därför som tidigare nämnts föreslagit att regeringen ger tillsynsmyndigheterna i uppdrag att med stöd av MSB skyndsamt utarbeta en vägledning. Här finns det alltså fortfarande en oklarhet. Däremot är det klart att utredningens förslag innebär att betydligt fler enskilda verksamhetsutövare kommer att omfattas av krav än vad som gäller enligt gällande NIS-lag. En vidare förutsättning är dock som anges ovan under avsnitt 12.4 att huvudregeln är att verksamheten sysselsätter minst 50 personer eller har en omsättning som överstiger 10 miljoner euro per år. Innebörden av det är att utredningens förslag som huvudregel inte omfattar små företag. Definitionen för små företag är alltså att verksamheten sysselsätter mindre än 50 personer och vars omsättning är lägre än 10 miljoner euro.

De krav som kommer att gälla för dessa enskilda verksamhetsutövare är samma som utredningens förslag riktar mot offentliga verksamhetsutövare. På samma sätt som för offentliga verksamhetsutövare kommer förslagen att medföra kostnader, men samtidigt även stöd och övergripande besparingar.

Det ska vidare beaktas att kraven kommer att gälla samtliga enskilda verksamhetsutövare inom sektorn, inte bara i Sverige utan även inom hela EES. Utredningen bedömer därför att regleringen

[19] SOU 2017:36 s. 276.

inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

12.9 Förslagens konsekvenser för det kommunala självstyret

Utredningens bedömning: Förslagen innebär en viss inskränkning i självstyrelsen. Med hänsyn till det stora intresset av att öka cybersäkerheten i nätverks- och informationssystem är inskränkningen nödvändig.

När det gäller förslagens konsekvenser för det kommunala självstyret ansluter sig utredningen till den bedömning som gjordes av regeringen i propositionen med förslag till NIS-lag.
I betänkandet om införlivning av NIS-direktivet anförs att det finns ett antal värden som kan tillgodoses genom kommunal självstyrelse, som demokrativärden och effektivitetsvärden.

Vid analysen av konsekvenser för kommunalt självstyre kunde enligt den utredningen följande frågor användas:

1. Har förslaget betydelse för den lokala demokratin – återverkar det på kommunalpolitikernas handlingsutrymme eller medborgarnas möjlighet att utöva inflytande i systemet?
2. Påverkar förslaget uppgiftsfördelningen mellan staten och kommunerna?
3. Innebär förslaget statlig regelstyrning eller tillsyn över kommunal verksamhet?
4. Innebär förslaget att man inom någon del av den kommunala verksamheten inför nya rättigheter för medborgarna? Föreslås domstolskontroll av den kommunala verksamheten?

Utredningen anför dock vidare att det finns även lagstiftning som inte påverkar den kommunala självstyrelsen på det sätt som avses. Det anges att kommuner och regioner ska kunna omfattas av säkerhetsföreskrifter med mera av produktionsmässig karaktär. I de situationer blir det enligt den utredningen inte aktuellt att göra en prövning av den föreslagna lagstiftningen utifrån de värden som den kommunala självstyrelsen är satt att värna.

I betänkandet gjordes därför bedömningen att de förslagen inte påverkade den kommunala självstyrelsen på sätt som avses i 15 § kommittéförordningen (1998:1474). Det hänvisades till att förslagen avsåg krav på säkerhetsåtgärder och incidentrapportering som omfattar kommuner och regioner i deras egenskap av tillhandahållare av en samhällsviktig tjänst på samma sätt som andra leverantörer av samhällsviktiga tjänster.

I propositionen om förslag till NIS-lag anförde regeringen att förslagen innebar att kommuner och landsting kan bli skyldiga att vidta säkerhetsåtgärder och att rapportera incidenter. Dessa nya åliggganden för kommuner och landsting innebar enligt regeringens bedömning en viss inskränkning i självstyrelsen. Regeringen bedömde dock med hänsyn till det stora intresset av att öka säkerheten i nätverks- och informationssystem att inskränkningen var nödvändig. Utredningen ansluter sig detta synsätt.

13 Ikraftträdande med mera

I detta kapitel ska utredningen ta ställning till när cybersäkerhetsregleringen och toppdomänlagen ska träda i kraft och behovet av övergångsregler samt behovet av följdändringar i annan lagstiftning.

13.1 Cybersäkerhetsregleringen

Utredningens förslag: Cybersäkerhetslagen och cybersäkerhetsförordningen ska träda i kraft den 1 januari 2025.

Genom cybersäkerhetslagen upphävs lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och genom cybersäkerhetsförordningen upphävs förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Ändringarna i lag (2006:24) om nationella toppdomäner för Sverige på internet ska också träda i kraft den 1 januari 2025. Dessa förändringar kräver inte övergångsbestämmelser.

Av artikel 41 följer att medlemsländerna senast den 17 oktober 2024 ska anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet. Bestämmelserna ska tillämpas från den 18 oktober 2024.

Utredningen föreslår med hänsyn till det och svensk lagstiftningstradition att den lag och förordning som ska innehålla direktivets krav träder i kraft den 1 januari 2025. Genom lagen upphävs också den tidigare NIS- lagen och genom den nya förordningen den tidigare NIS-förordningen.

Även ändringarna i toppdomänlagen ska träda i kraft den 1 januari 2025, eftersom de också följer av NIS2-direktivet.

Direktivet innehåller inga övergångsbestämmelser.

Genom cybersäkerhetslagen och cybersäkerhetsförordningen upphävs alltså tidigare lag och förordning och det införs bland annat nya och strängare sanktioner. Dessa ska inte ha retroaktiv verkan. I stället ska den tidigare lagen och förordningen gälla för överträdelser som skett före ikraftträdandet, dvs. före den 1 januari 2025.

PTS har anfört att utredningen bör överväga om det krävs övergångsbestämmelser avseende tillsynsbestämmelserna. I gällande NIS-lag finns det bestämmelser om tillsyn i 21–27 §§ och i NIS-förordningen i 17–21 §§. Enligt den regleringen är det så att Statens energimyndighet är tillsynsmyndighet för sektorn energi, Transportstyrelsen för transport, Finansinspektionen för bankverksamhet och finansmarknadsinfrastruktur, IVO för Hälso- och sjukvård, Livsmedelsverket för leverans och distribution av dricksvatten och PTS för digital infrastruktur. Det betyder att tillsynsområden som redan omfattades av NIS-lagen kommer att ha oförändrade tillsynsmyndigheter. Däremot kommer tillsynen ske enligt ny lagstiftning. De formella tillsynsbestämmelserna i cybersäkerhetslagen är i hög grad utformade på samma sätt som motsvarande bestämmelser i NIS-lagen. Den skillnad som därmed finns är de bakomliggande materiella bestämmelser som är mer långtgående i cybersäkerhetslagen. Sammantaget betyder detta enligt utredningens att det saknas behov av ytterligare övergångsbestämmelser i cybersäkerhetsregleringen.

Förändringarna i toppdomänlagen är tre. Det handlar dels om att lagens tillämpningsområde vidgas, dels om att uppgifter ska lämnas ut även på annat sätt än genom internet. Dessa två förändringar kräver inga övergångsbestämmelser. Slutligen är en ändring i toppdomänlagen att registret över domännamn även ska innehålla registreringsdatum. Det betyder att domänadministratören för tidigare registrerade domännamn behöver komplettera registret med registreringsdatum. Denna förändring kräver inte en övergångsbestämmelse.

13.2 Följdändringar i annan författning

13.2.1 Hänvisningar i författning

Utredningens förslag: Till följd av införandet av cybersäkerhetslagen behöver hänvisningar till den nya lagen göras i punkten 153 i bilagan till offentlighets- och sekretessförordningen (2009:641) samt i 4 § 21 i förordningen 2007:951) om instruktion till Post- och telestyrelsen.

Ändringarna ska träda i kraft den 1 januari 2025.

Genom upphävandet av lagen NIS-lagen och ikraftträdandet av den nya cybersäkerhetslagen behöver hänvisningar till NIS-lagen i annan författning ersättas. Två sådana hänvisningar finns:

1. Punkten 153 i bilagan till offentlighets- och sekretessförordningen (2009:641), och
2. 4 § 21 i förordningen (2007:951) om instruktion till Post- och telestyrelsen.

Som följd ska dessa hänvisningar ersättas.

13.2.2 Bestämmelser som upphävs eller ändras

Utredningens bedömning: Genomförandet av NIS2-direktivet i svensk rätt innebär att 8 kap. 1–4 §§ (2022:482) lagen om elektronisk kommunikation ska upphävas. De följdändringar som följer av det ska genomföras. Bestämmelserna ska dock fortfarande gälla för överträdelser som har skett före ikraftträdandet. Ändringarna ska träda i kraft samtidigt som den föreslagna cybersäkerhetsregleringen, dvs. den 1 januari 2025.

Utredningens förslag:

1. Lagen (2022:482) om elektronisk kommunikation ska ändras på så sätt att:

– 8 kap. 1–4 §§ ska upphävas,

– 12 kap. 1 § ska ändras, och

– rubriken närmast före 8 kap. 1 § ska utgå.

2. Förordningen (2022:511) om elektronisk kommunikation ska ändras på så sätt att:

– 1 kap. 2 § fjortonde strecksatsen ska upphöra att gälla,

– 8 kap. 1 och 5 §§ ska upphöra att gälla,

– 1 kap. 2 § femtonde strecksatsen ska ändras, och

– 8 kap. 4 § ska ändras.

Ändringarna ska träda i kraft 1 januari 2025.

Utredningen har i 11 kap. bedömt att LEK, till följd av genomförandet av NIS2-direktivet, ska ändras. Den huvudsakliga ändringen består i att 8 kap. 1–4 §§ LEK ska upphävas, och det innebär även behov av följdändringar i LEK och den anslutande förordningen om elektronisk kommunikation. De närmare övervägandena framgår av kapitel 11 och förslagen framgår i detalj av avsnitt 1.3 och 1.7. Författningsändringarna föreslås träda i kraft vid samma tidpunkt som den föreslagna cybersäkerhetslagen och förordningen träder i kraft.

14 Författningskommentar

14.1 Förslaget till lag om cybersäkerhet

1 kap. Inledande bestämmelser

Lagens syfte

1 § Syftet med denna lag är att uppnå en hög cybersäkerhetsnivå.

Paragrafen genomför artikel 1.1 i NIS2-direktivet och behandlas i avsnitt 5.1.2. Den anger syftet med lagen.

Uttryck i lagen

2 § Se författningsförslaget.

Paragrafen genomför artikel 6 i NIS2-direktivet och bakgrunden är analyserad i avsnitt 5.2.2.

Definitionen i punkt 33 har anpassats till etablerad svensk terminologi och där begreppet entitet ersätts av verksamhetsutövare. Verksamhetsutövarens verksamhet i dess helhet omfattas.

Lagens tillämpningsområde

Offentliga verksamhetsutövare

3 § Denna lag gäller för

1. statliga myndigheter i Sverige med undantag för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och Sveriges domstolar,
2. regioner i Sverige med undantag för regionfullmäktige, och
3. kommuner i Sverige med undantag för kommunfullmäktige.

Paragrafen genomför del av artikel 2.1 samt 2.2 f och 2.5 a. Vidare genomför paragrafen artikel 26.1 c om jurisdiktion. Bakgrunden till paragrafen behandlas i avsnitt 5.2.9. och 5.3.1.

I begreppet Sveriges domstolar ingår samtliga domstolar och nämnder, även exempelvis Domarnämnden och Rättshjälpsmyndigheten, men inte Domstolsverket, som är en statlig myndighet som har till uppgift att stödja och serva domstolar, nämnder och myndigheter inom Sveriges Domstolar.

Att även Regeringskansliet, utlandsmyndigheter och kommittéväsendet är undantagna från lagen utvecklas i avsnitt 5.5.4.

Enskilda verksamhetsutövare

4 § Denna lag gäller för enskilda verksamhetsutövare om

1. verksamheten omfattas av bilaga 1 eller 2 i NIS2-direktivet eller är ett lärosäte med examenstillstånd,
2. inte annat följer av 5 och 6 §§, verksamheten är etablerad i Sverige, och
3. inte annat följer av 7 och 8 §§, verksamheten uppfyller kraven för medelstort företag enligt artikel 2 och 3.1–3.3 i bilagan till kommissionens rekommendation 2003/361/EG.

Regeringen eller den myndighet regeringen bestämmer får i föreskrifter meddela undantag för 3 avseende partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet.

Paragrafen genomför resterande del av artikel 2.1 samt 2.5 b och 26.1. Bakgrunden till paragrafen behandlas i avsnitt 5.2.12. och 5.3.2.

Den reglerar vad som gäller för alla andra verksamhetsutövare än offentliga, dvs. enskilda verksamhetsutövare. Det kan vara juridiska eller fysiska personer, se § 2 punkt 33. Utgångspunkten för att omfattas är att verksamheten omfattas av bilaga 1 eller 2. Detta är utvecklat i 5.2.12. Som anges där föreslår utredningen att regeringen bör ge tillsynsmyndigheterna i uppdrag att med stöd av MSB utforma en vägledning om vem som omfattas av sektorsbeskrivningarna.

Därutöver omfattas lärosäten med examenstillstånd som inte är statliga myndigheter av denna paragraf. Som framgår av avsnitt 5.2.14 inryms statliga lärosäten som är egna myndigheter i 3 §. Lärosäten med examenstillstånd omfattas inte av bilaga 1 eller 2 till direktivet och behöver därför anges specifikt i paragrafen. Begreppet innefattar universitet, högskolor och enskilda utbildningsanordnare. Bakgrunden till att lärosäten omfattas framgår alltså av avsnitt 5.2.14.

Paragrafen anger i punkt 2 huvudregeln om jurisdiktion för enskilda verksamhetsutövare. Det krävs som huvudregel, om inte verksamhetsutövaren erbjuder allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, att verksamhetsutövaren är etablerad i Sverige. Vad som gäller för den som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster följer av 5 §. Därutöver finns det en särskild jurisdiktionsregel för gränsöverskridande verksamhetsutövare i 6 §.

I paragrafen hänvisas under punkt 3 till kommissionens rekommendation 2003/361/EG artikel 2 och artikel 3.1–3.3. Som framgår av avsnitt 5.2.8 följer av artikel 2 i rekommendationen att ett medelstort företag är ett företag som sysselsätter minst 50 personer eller vars omsättning eller balansomslutning överstiger 10 miljoner euro per år. Skälet för hänvisningen även till artikel 3.1–3.3 i rekommendationen är att det i dessa artiklar finns bestämmelser som har betydelse för beräkning av storlekskraven. Här definieras nämligen vad som anges med begreppen partnerföretag och anknutna företag.

5 § Verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster behöver inte vara etablerade i Sverige för att omfattas av lagen utan det är tillräckligt att verksamhetsutövaren erbjuder tjänster i Sverige.

6 § Gränsöverskridande verksamhetsutövare är verksamhetsutövare som erbjuder:

1. DNS-tjänster,
2. registreringsenheter för toppdomäner,
3. domännamnsregistrering,
4. molntjänster,
5. datacentraltjänster,
6. nätverk för leverans av innehåll,
7. hanterade tjänster,
8. hanterade säkerhetstjänster, eller
9. marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster.

Gränsöverskridande verksamhetsutövare som erbjuder tjänster inom EES, men saknar etablering där ska utse en företrädare med etablering i något av de länder där tjänster erbjuds.

För gränsöverskridande verksamhetsutövare krävs det i stället för etablering att Sverige är huvudsakligt etableringsställe eller att företrädaren är etablerad i Sverige för att verksamhetsutövaren ska omfattas av lagen.

För gränsöverskridande verksamhetsutövare som erbjuder tjänster i Sverige, men inte utser en företrädare gäller kap. 5.

Regeringen får meddela föreskrifter om vad som utgör huvudsakligt etableringsställe.

Paragraferna genomför artiklarna 26.1 a och 26.1 b. samt 26.2 och 26.3 och bakgrunden till paragrafen behandlas i avsnitt 5.3.2.

Paragraf fem avser jurisdiktion för verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster. Paragrafen är ett undantag från huvudregeln i 4 § punkt 2.

Bakgrunden till paragrafen är redovisad i avsnitt 5.3.2.

Paragraf sex anger jurisdiktion för gränsöverskridande verksamhetsutövare och är också ett undantag från huvudregeln i 4 § punkt 2.

Av paragrafen följer också krav på att en företrädare utses för sådana verksamhetsutövare i vissa fall. Om verksamhetsutövaren helt saknar etablering inom EES föreligger det en skyldighet för verksamhetsutövaren att utse en företrädare som är etablerad inom EES om utövaren erbjuder tjänster inom EES. Det är dock tillräckligt att en företrädare utses i ett av dessa länder och då i ett av länderna där tjänster erbjuds.

7 § Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 och som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner, DNS-tjänster eller domännamnsregistrering omfattas av lagen.

8 § Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 omfattas också av lagen om,

1. verksamheten är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner,
2. en störning kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet, folkhälsa eller medföra betydande systemrisker särskilt om det får gränsöverskridande konsekvenser, eller
3. verksamheten är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av denna verksamhet.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter.

Paragraferna genomför artiklarna 2.2 a–e, 2.3 och 2.4 och bakgrunden till paragraferna behandlas i avsnitt 5.2.13.

Innebörden av paragrafen är att verksamheter som anges i paragrafen omfattas av lagen även om storlekskravet i 4 § 3 inte uppnås, dvs. det är ingen medelstor verksamhet enligt definitionen i 2 § punkt 20.

Undantag från lagens tillämpningsområde

Krav i andra författningar

9 § Om annan författning innehåller bestämmelser om krav på riskhanteringsåtgärder eller incidentrapportering för en verksamhetsutövare med motsvarande verkan gäller inte kraven i 3 kap. för verksamhetsutövaren.

Vid jämförelsen av verkan mellan författningarna ska hänsyn tas till bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till bestämmelserna.

Regeringen får i föreskrifter ange vilka andra bestämmelser om riskhanteringsåtgärder och incidentrapportering som har motsvarande verkan.

Paragrafen genomför artikel 4 och bakgrunden till paragrafen följer av avsnitt 5.4.

Som framgår där föreslår utredningen att det av förordningen ska följa att finansiella verksamhetsutövare som omfattas av Dora-förordningen inte ska omfattas av krav om riskhanterings- och rapporteringsskyldigheter. Som en följd gäller då inte sanktionsbestämmelserna avseende underlåtenhet att uppfylla riskhanterings- och rapporteringsskyldigheter. I riskhanteringsåtgärder ingår systematiskt informationssäkerhetsarbete och utbildning.

10 § Lagen ska inte tillämpas på verksamheter som undantagits enligt artikel 2.4 i Dora-förordningen.

Paragrafen genomför artikel 2.10 och bakgrunden är redovisad i avsnitt 5.4. Som framgår där rör det sig om Svenska Skeppshypotekskassan.

Sveriges säkerhet eller brottsbekämpning

11 § Lagen gäller inte statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) eller brottsbekämpning.

Regeringen får i föreskrifter ange vilka statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning.

Paragrafen genomför artikel 2.7 och bakgrunden till paragrafen är redovisad i 5.5.1, 5.5.2 och 5.5.4.

Innebörden är att enligt paragrafen undantas hela verksamheter från lagen. Vilka dessa är ska följa av förordningen.

12 § För andra statliga myndigheter som utövar säkerhetskänslig verksamhet eller brottsbekämpning än de som avses i 11 § gäller inte kraven i 6 § andra och fjärde stycket samt kap. 3 för den del av verksamheten som är säkerhetskänslig eller utgör brottsbekämpning. För den övriga delen av verksamheten gäller lagen i dess helhet.

Vad som anförs i första stycket gäller även regioner och kommuner.

13 § Lagen gäller inte för enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet, brottsbekämpning eller som enbart erbjuder tjänster till statliga myndigheter som avses i 11 §.

Om en enskild verksamhetsutövare bedriver även annan verksamhet gäller för den säkerhetskänsliga verksamheten, brottsbekämpningen och verksamheten som avser tjänster till statliga myndigheter enligt 11 § inte kraven i 6 § andra och fjärde stycket samt kap. 3.

För den övriga delen av verksamheten gäller lagen i dess helhet.

Vad som anförs ovan i andra stycket gäller inte om verksamhetsutövaren är en tillhandahållare av betrodda tjänster. För dessa verksamhetsutövare gäller lagen i dess helhet.

Paragraferna genomför artikel 2.7 och bakgrunden till paragraferna är redovisad i avsnitt 5.5.1, 5.5.2, 5.5.,4 och 5.5.5.

I 12 § anges vad som gäller för statliga myndigheter. Det som undantas är den säkerhetskänsliga verksamheten och verksamhet som bedriver brottsbekämpning. Säkerhetskänslig verksamhet definieras i säkerhetsskyddslagen (2018:585) och i begreppet brottsbekämpning ingår förebyggande, utredning, upptäckt och lagföring av brott. Verksamhetsutövare med tillsynsbefogenheter anses inte bedriva verksamhet på brottsbekämpningsområdet och den delen är därför inte undantagen. De verksamhetsutövare som innefattas här är de offentliga utövare som omfattas av lagen, dvs. statliga myndigheter, regioner och kommuner. Regionfullmäktige och kommunfullmäktige omfattas inte av lagen. I begreppet statlig myndighet ingår statliga affärsverk.

I 13 § finns bestämmelser för enskilda verksamhetsutövare som motsvarar vad som anges i paragraferna 11 och 12 för offentliga verksamhetsutövare.

14 § Skyldighet att lämna uppgifter enligt denna lag gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585).

Paragrafen genomför artikel 2.11 och bakgrunden till paragrafen är redovisad i 5.5.3.

Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet enligt 1 kap. 2 § andra stycket säkerhetsskyddslagen (2018:585).

Skyldigheten ska tolkas brett och omfatta såväl rapporteringskrav som andra skyldigheter att lämna uppgifter. Säkerhetsskyddsklassificerade uppgifter kan avse såväl uppgifter som härrör från verksamhetsutövarens egen verksamhet som uppgifter från myndigheter och andra.

2 kap. Klassificering och registrering

1 § Följande verksamhetsutövare är väsentliga:

1. Statliga myndigheter,
2. verksamhetsutövare som bedriver verksamhet enligt bilaga 1 till NIS2-direktivet, är en kommun eller ett lärosäte med examenstillstånd och vars verksamhet överstiger trösklarna för medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,
3. verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och vars verksamhet är medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,
4. kvalificerade tillhandahållare av betrodda tjänster,
5. registreringsenheter för toppdomäner,
6. verksamhetsutövare som erbjuder DNS-tjänster och
7. verksamhetsutövare som anges i 1 kap. 8 § och identifierats som väsentliga enligt 33 § förordning om cybersäkerhet.

Verksamhetsutövare som inte är väsentliga är viktiga verksamhetsutövare.

Paragrafen genomför artikel 3.1 och 3.2 och bakgrunden till paragrafen redovisas i avsnitt 6.1.

I paragrafen anges vilka verksamheter som är väsentliga. Begreppen definieras i 1 kap. 2 §.

Av *punkten 2* följer att verksamheter som anges i bilaga 1 till direktivet och överstiger trösklarna för medelstora företag enligt kommissionens rekommendation 2003/361/EG är väsentliga. Innebörden är att det gäller för såväl offentliga som enskilda verksamhetsutövare. Det finns visserligen i den rekommendationen i artikel 3.4 ett undan-

tag för offentliga verksamhetsutövare, men det undantaget är i sin tur satt ur spel genom artikel 2.1 andra stycket i NIS2-direktivet, se även avsnitt 5.2.8.

Utredningen menar att det när det gäller kommissionens rekommendation krävs det inte bara en hänvisning till artikel 2 utan även till artikel 3.1–3. Skälet är att det där finns bestämmelser som har betydelse för beräkning av storlekskraven. Här definieras nämligen vad som anges med begreppen partnerföretag och anknutna företag.

2 § Verksamhetsutövare ska i en anmälan till tillsynsmyndigheten lämna uppgift om identitet, kontaktuppgift, IP-adressintervall, verksamhet och uppgift om i vilka länder verksamheten bedrivs. Gränsöverskridande verksamhetsutövare ska även lämna uppgift om huvudsakligt etableringsställe och i förekommande fall kontaktuppgift till företrädaren.

Ändras uppgifterna ska verksamhetsutövaren anmäla förändringen inom 14 dagar.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om uppgifterna.

Paragrafen genomför artikel 3.4 och bakgrunden till paragrafen redovisas i avsnitt 6.2.

Den innehåller en skyldighet för verksamhetsutövare som omfattas av lagen att lämna uppgifter. Dessa ska ligga till grund för det register som tillsynsmyndigheter ska upprätta enligt 10 § cybersäkerhetsförordningen och som till slut kommissionen ska ta del av. Med identitet avses namn och kontaktuppgift är en samlingsterm för adress och e-postadress.

Paragrafen innehåller ett bemyndigande i andra stycket.

3 kap. Riskhanteringsåtgärder och incidentrapportering

1 § Verksamhetsutövaren ska vidta tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken. De ska utvärderas och särskilt innefatta följande:

1. Incidenthantering,
2. kontinuitetshantering,
3. säkerhet i leveranskedjan,
4. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation,
5. strategier och förfaranden för användning av kryptografi och kryptering,

6. personalsäkerhet,
7. strategier för åtkomstkontroll och tillgångsförvaltning,
8. säkrade lösningar för kommunikation, och
9. lösningar för autentisering.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om riskhanteringsåtgärder.

Paragrafen genomför artikel 21.1–21.3 och bakgrunden till paragrafen finns i avsnitt 7.1.2. Bestämmelsen genomför även delvis artikel 108 i kodexen om elektronisk kommunikation[1] och beskrivs i kapitel 11.

I första stycket regleras syftet med riskhanteringsåtgärder. Det är nätverks- och informationssystem som ska skyddas mot incidenter, inbegripet systemens fysiska miljö. I formuleringen ”skydda nätverks- och informationssystem” innefattas att riskhanteringsåtgärderna även ska minimera konsekvenserna av incidenter.

I andra stycket finns det en uppräkning av vilka åtgärder som särskilt ska vidtas. Innebörden är att även andra åtgärder eller strategier kan krävas.

Åtgärderna ska vara proportionella. Här ska hänsyn tas till verksamhetsutövarens riskexponering, verksamhetens storlek samt sannolikheten för att incidenter inträffar. Det ska även beaktas hur allvarliga dessa incidenter i så fall är och hänsyn ska då bland annat tas till konsekvenser för samhället och de ekonomiska konsekvenserna.

Som framgår av de allmänna övervägandena föreslår utredningen att begreppet driftskontinuitet ersätts av begreppet *kontinuitetshantering*. Med detta avses exempelvis säkerhetskopiering, katastrofhantering och krishantering.

Med *säkerhet i leveranskedjan*, inbegrips säkerhetsaspekter som rör förbindelserna mellan varje verksamhetsutövare och dess direkta leverantörer eller tjänsteleverantörer. Det betyder enligt utredningens uppfattning att varje verksamhetsutövare endast behöver vidta riskhanteringsåtgärder i förhållande till sin leverantör. Innebörden skulle vara att varje verksamhetsutövare ansvarar för ett led i kedjan. De närmare bestämmelserna om detta bör följa av föreskrifter.

Begreppet *åtkomstkontroll* inbegriper sådana funktioner som syftar till att reglera och kontrollera en användares åtkomst till information och resurser. Detta avser således både behörighetsstyrning (tilldel-

[1] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning).

ning, återkallande och hantering av behörigheter och motsv.) samt uppföljning av åtkomst till information och resurser, till exempel genom loggar och andra hjälpmedel.

Kommunikation avser röst-, video- och textkommunikation. *Autentisering* syftar till användning av multifaktorautentisering eller kontinuerlig autentisering.

2 § Verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete.

Bestämmelsen är överförd från lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Överväganden finns i avsnitt 7.1.3.

3 § Ledningen i enskilda och offentliga verksamheter ska genomgå utbildning om riskhanteringsåtgärder och anställda ska erbjudas sådan utbildning.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om utbildning.

Paragrafen genomför artikel 20.2 och bakgrunden finns i avsnitt 7.2. Utbildningskravet gäller såväl för offentliga som enskilda verksamhetsutövare. I artikeln anges att utbildningen ska avse ledningsorganet. Det betyder för ett aktiebolag styrelsen, men även den verkställande direktören ska självfallet omfattas. Utredningen använder med hänsyn till det och att även offentliga verksamhetsutövare omfattas begreppet ledningen. För offentliga verksamhetsutövare betyder det för myndigheter generaldirektören och de anställda som utövar ledningsfunktioner och för regioner och kommuner region- eller kommunstyrelse. Den närmare omfattningen ska följa av föreskrifter.

4 § Med betydande incident avses

1. En incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller

2. en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande incident.

Paragrafen genomför artikel 23.3. Övervägandena finns i avsnitt 7.3.

Den anger övergripande innebörden av en betydande incident. Den preciserade betydelsen ska följa av föreskrifter. Till grund för definitionen ligger definitionen av incident, se 1 kap. 2 § 19. En incident avseende den fysiska infrastrukturen och som har en betydande påverkan ska som utgångspunkt innebära en rapporteringspliktig incident.

5 § Verksamhetsutövaren ska som en varning underrätta CSIRT-enheten om betydande incidenter inom 24 timmar efter det att verksamhetsutövaren fått kännedom om den. Det ska anges om det finns misstanke om att incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter.

Paragrafen genomför artikel 23.4 a. Övervägandena finns i avsnitt 7.3. I paragrafen regleras kravet på verksamhetsutövarens första åtgärd som benämns varning.

6 § Verksamhetsutövaren ska också inom 72 timmar från tidpunkten från kännedom göra en incidentanmälan till CSIRT-enheten om betydande incidenter. Den ska innehålla en inledande bedömning av hur allvarlig den betydande incidenten är, konsekvenserna av den och förekomsten av angreppsindikatorer. Vidare ska tidigare varning enligt 5 § uppdateras.

För verksamhetsutövare som erbjuder betrodda tjänster ska en incidentanmälan göras inom 24 timmar.

CSIRT-enheten får begära ytterligare information av verksamhetsutövaren.

Verksamhetsutövaren ska samtidigt även informera kunder som kan antas påverkas av den betydande incidenten. Kunderna ska vid behov informeras om avhjälpande åtgärder. Detsamma gäller betydande cyberhot.

Paragrafen genomför artikel 23.2 och 23.4 b och c. Övervägandena finns i avsnitt 7.3. Den reglerar den andra åtgärden som benämns incidentanmälan.

7 § Verksamhetsutövaren ska inom en månad från incidentanmälan i 5 § lämna en slutrapport till CSIRT-enheten. Om incidenten fortfarande är pågående ska i stället en lägesrapport lämnas som ska kompletteras med en slutrapport en månad efter det att incidenten har hanterats. Slutrapporten eller lägesrapporten ska innehålla en beskrivning av

1. Incidenten och dess konsekvenser,
2. hur allvarlig incidenten bedöms vara,
3. vad som sannolikt utlöst incidenten,
4. åtgärderna för att begränsa incidenten, och
5. incidentens möjliga gränsöverskridande effekter.

Paragrafen genomför artikel 23.4 d och e. Överväganden finns i avsnitt 7.3.

8 § Regeringen eller den myndigheten regeringen bestämmer får meddela föreskrifter om incidentrapporteringen enligt 5–7 §§.

4 kap. Tillsyn

Tillsynsmyndighet

1 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Paragrafen genomför artikel 8.1 och behandlas i avsnitt 8.4.1 och 8.4.2.

Det ska finnas en eller flera tillsynsmyndigheter för varje sektor. I 8 § förordningen anges vilka myndigheter som är tillsynsmyndighet för vilken sektor.

Tillsynsmyndighetens uppdrag

2 § Tillsynsmyndigheten ska utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

Paragrafen genomför artikel 31.1 och behandlas i avsnitt 8.4.3.

Syftet med tillsyn är att kunna bedöma hur verksamhetsutövare uppfyller kraven på riskhanteringsåtgärder, incidentrapportering och anmälan. Resultatet av en tillsyn kan ligga till grund för ingripanden och sanktioner.

3 § Tillsynsåtgärder för viktiga verksamhetsutövare får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att denna lag eller föreskrifter som meddelats i anslutning till lagen inte följs.

Paragrafen genomför artikel 33.1 och behandlas i avsnitt 8.4.4.

Tillsynsåtgärder när det gäller viktiga verksamhetsutövare ska vidtas bara när det finns bevis, indikationer eller information om att verksamhetsutövaren inte uppfyller lagens krav. Informationen kan till exempel komma från andra tillsynsmyndigheter eller via incidentrapporteringen.

Tillsynsmyndighetens undersökningsbefogenheter

4 § Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten den information som behövs för tillsyn.

Paragrafen genomför artikel 32.2 a, e–g och 33.2 a samt d–f och behandlas i avsnitt 8.4.6.

Tillsynsmyndigheten kan ålägga en verksamhetsutövare att tillhandahålla sådan information som behövs för att bedöma om verksamhetsutövaren uppfyller lagens krav. Detta inkluderar bland annat information som behövs för att bedöma de riskhanteringsåtgärder som verksamhetsutövaren vidtagit, dokumenterade cybersäkerhetsstrategier samt resultaten av säkerhetsrevisioner eller annan dokumentation.

5 § Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamheten.

Paragrafen genomför artikel 32.2 a och 33.2 a och behandlas i avsnitt 8.4.6.

Paragrafen ger tillsynsmyndigheten tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, i den utsträckning det behövs för att kunna utöva tillsyn.

6 § Tillsynsmyndigheten får förelägga den som står under tillsyn att tillhandahålla information och ge tillträde enligt 4 och 5 §§.

Ett sådant föreläggande får förenas med vite.

Bakgrunden till paragrafen behandlas i avsnitt 8.4.6.

Paragrafen ger tillsynsmyndigheten möjlighet att förelägga en verksamhetsutövare att tillhandahålla information enligt 4 § och ge tillträde enligt 5 §. Ett beslut om föreläggande får enligt andra stycket förenas med vite.

7 § Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att genomföra de åtgärder som avses i 4 och 5 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Bakgrunden till paragrafen behandlas i avsnitt 8.4.6.

Om en verksamhetsutövare vägrar att ge tillsynsmyndigheten information eller tillträde till en lokal kan tvångsåtgärder behöva användas. Tillsynsmyndigheten ska därför vid behov kunna begära biträde av Kronofogdemyndigheten.

Säkerhetsrevision

8 § Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten.

Tillsynsmyndigheten får även anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare.

Regeringen får meddela föreskrifter om säkerhetsrevisioner.

Paragrafen genomför artikel 32.2 b–c och 33.2 b–c och behandlas i avsnitt 8.4.6. Den ger tillsynsmyndigheten möjlighet att ålägga verksamhetsutövare på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision. Paragrafen ger också tillsynsmyndigheten möjlighet att anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare. Att tillsynsmyndigheten har möjlighet att utföra egna säkerhetsrevisioner ingår i uppgiften att bedriva tillsyn.

Med oberoende organ avses exempelvis ett företag som genomför säkerhetsrevisioner. Organet ska vara oberoende i förhållande till tillsynsmyndigheten och den verksamhetsutövare vars verksamhet ska granskas. Organet ska ha den sakkunskap som krävs för säkerhetsrevisionen. Det är upp till tillsynsmyndigheten att bedöma om lämpliga organ som ska utföra säkerhetsrevisionen bör pekas ut i samband med åläggandet eller om det kan överlåtas till verksamhetsutövaren.

Säkerhetsskanning

9 § Tillsynsmyndigheten får låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av denna lag.

En säkerhetsskanning ska ske i samarbete med verksamhetsutövaren.

Paragrafen genomför artikel 32.2 d och 33.2 d och behandlas i avsnitt 8.4.6. Den ger tillsynsmyndigheten möjlighet att låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av

lagen. En säkerhetsskanning får inte ha någon negativ inverkan på hur nätverks- och informationssystem fungerar och ska ske i samarbete verksamhetsutövaren.

5 kap. Ingripanden och sanktioner

Inledande bestämmelser

1 § Tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter enligt denna lag, eller föreskrifter som har meddelats med stöd av bestämmelserna om

1. skyldighet att utse företrädare enligt 1 kap. 6 §,
2. anmälningsskyldighet enligt 2 kap. 2 §,
3. riskhanteringsåtgärder enligt 3 kap. 1 §,
4. utbildning enligt 3 kap. 3 §, eller
5. incidentrapportering enligt 3 kap. 5–7 §§.

Paragrafen fastställer att tillsynsmyndigheten är skyldig att ingripa vid en verksamhetsutövares överträdelser mot de skyldigheter som anges i lagen eller föreskrifter som har meddelats med stöd av den. Skyldigheterna redogörs för i avsnitt 5.3.2, kapitel 6 och 7.

2 § Ingripanden sker genom att tillsynsmyndigheten

1. meddelar föreläggande enligt 6 §,
2. ansöker om förbud att utöva ledningsfunktion enligt 7 §, eller
3. meddelar sanktionsavgift enligt 11 §.

Om tillsynsmyndigheten inte finner skäl att ingripa enligt första stycket ska den i stället meddela verksamhetsutövaren en anmärkning.

Tillsynsmyndigheten får avstå från att ingripa enligt första och andra stycket om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren eller den fysiska personen med anledning av överträdelsen, och tillsynsmyndigheten bedömer att dessa åtgärder är tillräckliga.

Paragrafen genomför artikel 32.4 a, 33.4 a och 34.2 och beskrivs i avsnitt 9.3.

Första och andra stycket anger på vilka sätt tillsynsmyndigheten kan ingripa genom att använda olika sanktioner. Tillsynsmyndigheten kan använda sig av en eller flera sanktioner för att ingripa mot samma överträdelse. Möjligheten att meddela anmärkning är subsidiär till övriga ingripanden, och ska användas om tillsynsmyndigheten inte använder sig av något av de andra ingripandena.

Tredje stycket medför en ventil för tillsynsmyndigheten att avstå från ingripanden i vissa särskilda fall och utvecklas i avsnitt 9.3.1. Den ska tillgripas restriktivt och tar sikte på situationer där ett ingripande exempelvis skulle anses strida mot dubbelprövningsförbudet enligt Europakonventionens sjunde tilläggsprotokoll (*ne bis in idem*) eller anses oproportionerligt på grund av en annan myndighets ingripande mot samma överträdelse eller händelse. Det behöver i sådana lägen inte avse en svensk tillsynsmyndighet, utan skulle till exempel kunna avse en utländsk NIS2-tillsynsmyndighet. Att tillsynsmyndigheten avstår från att ingripa innebär att den inte använder något av verktygen föreläggande, förbud, sanktionsavgift eller anmärkning. Tillsynsmyndigheten behöver inte fatta ett beslut om att avstå från att ingripa.

Omständigheter som ska beaktas vid ett ingripande

3 § Vid val och utformning av ingripandeåtgärder enligt 2 § ska hänsyn tas till hur allvarlig överträdelsen är, hur länge den har pågått, samt den skada eller risk för skada som uppstått till följd av överträdelsen.

Vid bedömningen ska särskilt beaktas

1. de åtgärder verksamhetsutövaren vidtagit för att förhindra eller minska skadan,
2. verksamhetsutövarens samarbete med tillsynsmyndigheten,
3. om överträdelsen begåtts med uppsåt eller oaktsamhet, och
4. den ekonomiska fördel som verksamhetsutövaren fått till följd av överträdelsen.

Paragrafen genomför artiklarna 32.7 delvis, 33.5 delvis och 34.3 delvis, och behandlas i avsnitt 9.4.2. Att tillsynsmyndigheten ska beakta alla relevanta omständigheter följer bland annat av förvaltningslagen (2017:900). I bestämmelsen anges dock ett antal omständigheter som ska beaktas särskilt vid val av ingripandeåtgärder och utformningen av dessa.

I *första stycket* anges att tillsynsmyndigheten ska ta hänsyn till hur allvarlig överträdelsen är och hur länge den pågått. Det bör redan här noteras att alla former av överträdelser kan vara att betrakta som allvarliga, det krävs alltså inte att någon av de omständigheter som tas upp i 5 § föreligger. Exempelvis kan en verksamhetsutövare som förvisso aldrig begått någon tidigare överträdelse, men som vid tillsyn visar sig ha underlåtit att vidta lämpliga och effektiva riskhan-

teringsåtgärder anses ha begått en allvarlig överträdelse. Vidare anges att den (risk för) skada som uppstått genom överträdelsen ska beaktas. Detta kan avse både materiell och immateriell skada. Skadan behöver vara förutsebar på något sätt för verksamhetsutövaren, och bedömningen bör utgå ifrån vad denne insett eller borde ha insett om adekvata analyser hade gjorts. Att även risk för skada beaktas medför att även sårbarheter som funnits under lång tid men som inte lett till någon inträffad incident kan beaktas. Att en överträdelse inneburit (risk för) stor skada bör generellt tala i försvårande riktning.

I *andra stycket* anges ett omständigheter som ska beaktas särskilt vid bedömningen enligt första stycket.

Av *punkten ett* följer att de åtgärder som verksamhetsutövaren har vidtagit för att förhindra eller minska skadan som uppstått till följd av överträdelsen ska beaktas. Detta bedömningskriterium kan även beaktas motsatsvis om en verksamhetsutövare trots kännedom om en sårbarhet inte vidtagit några åtgärder för att minska skadan.

Enligt *punkten två* ska verksamhetsutövarens samarbete med tillsynsmyndigheten beaktas. Om verksamhetsutövaren försökt åtgärda en inträffad incident och aktivt bistått tillsynsmyndigheten med information bör detta tala i mildrande riktning. Detsamma bör gälla om verksamhetsutövaren hörsammat den information som tillsynsmyndigheten förmedlat på andra sätt än genom förelägganden.

Av *punkten tre* följer att skälet till överträdelsen ska beaktas. Om en överträdelse skett uppsåtligen bör detta vara att betrakta som en kraftigt försvårande omständighet, medan en omedveten och oavsiktlig överträdelse kan betraktas som en neutral eller i vissa fall förmildrande omständighet.

I *punkten fyra* anges att den ekonomiska fördelen av överträdelsen ska beaktas. Detta tar sikte både på vilka vinster som kan ha gjorts, eller vilka kostnader som undvikits, exempelvis genom att vidta en billig och otillräcklig riskhanteringsåtgärd. Det kan även avse att någon sådan riskhanteringsåtgärd inte vidtagits över huvud taget.

4 § Utöver vad som anges i 3 § ska det beaktas som försvårande om verksamhetsutövaren tidigare har begått en överträdelse.

I förmildrande riktning ska beaktas om verksamhetsutövaren har följt godkända uppförandekoder eller godkända certifieringsmekanismer.

I paragrafen anges att vissa omständigheter ska beaktas som försvårande och andra som förmildrande. Bestämmelsen genomför artikel 32.7 delvis, 33.5 delvis och 34.3 delvis, samt kompletterar 3 §. Innehållet beskrivs i avsnitt 9.4.2.

Av *första stycket* följer att tidigare överträdelser ska beaktas som försvårande för verksamhetsutövaren. Vid denna bedömning bör särskild vikt fästas vid om överträdelserna är likartade och den tid som har gått mellan överträdelserna. De tidigare överträdelserna bör bedömas vara relevanta, men de behöver inte vara identiska med den nu aktuella. Upprepade överträdelser bör betraktas som försvårande omständigheter, där upprepade överträdelser av likartad typ bör göra att överträdelsen ska betraktas som allvarlig (se 5 § 1).

Enligt *andra stycket* ska det kunna beaktas i mildrande riktning om verksamhetsutövaren följer godkända uppförandekoder eller godkända certifieringsmekanismer som tagits fram baserat på EU:s arbete. I vissa fall skulle det kunna inträffa att en skada eller sårbarhet uppstår trots att en tillämplig uppförandekod följts i just denna del. Detta bör då beaktas i mildrande riktning.

5 § En överträdelse ska betraktas som allvarlig om verksamhetsutövaren
1. har begått upprepade överträdelser,
2. inte har rapporterat eller avhjälpt en betydande incident,
3. inte har följt ett tidigare föreläggande från en tillsynsmyndighet,
4. har hindrat säkerhetsrevisioner eller tillsynsåtgärder som tillsynsmyndigheten beslutat om, eller
5. har lämnat oriktiga uppgifter avseende riskhanteringsåtgärder eller rapporteringsskyldigheter enligt 3 kap. 1 eller 5–7 §§.

Bestämmelsen genomför artikel 32.7 delvis, 33.5 delvis och 34.3 delvis, samt kompletterar 3 §. Innehållet beskrivs i avsnitt 9.4.2. Paragrafen anger vissa omständigheter som gör att en överträdelse är att betrakta som allvarlig.

I *punkten ett* anges att upprepade överträdelser utgör ett sådant exempel. För att kunna avgöra om en överträdelse är upprepad bör både överträdelsens art och tiden mellan den föregående och nu aktuella överträdelsen beaktas. Även likartade överträdelser som begåtts med förhållandevis lång tid emellan bör kunna bedömas som *upprepade* om det finns indikationer på att verksamhetsutövaren har begått dem på ett systematiskt sätt.

Av *punkten två* följer att underlåtelse att rapportera eller avhjälpa en betydande incident (se artikel 23.3 NIS2-direktivet) ska innebära en allvarlig överträdelse. En sådan överträdelse ska enligt utredningen anses föreligga både om verksamhetsutövaren inte rapporterar eller avhjälper över huvud taget, eller om det avseende rapporteringen sker men efter de tidsramar som anges i artikel 23.4 NIS2-direktivet.

Enligt *punkten tre* ska även bristande efterföljande av tidigare föreläggande betraktas som en allvarlig överträdelse. Detta hänger samman med att om tillsynsmyndighetens föreläggande följts hade överträdelsen kunnat lösas tidigare, och därmed hade eventuella (risker för) skada kunnat minimeras. Vid denna bedömning bör tillsynsmyndigheten kunna nyansera bedömningen utifrån verksamhetsutövares agerande. Det bör till exempel kunna medföra skillnader om verksamhetsutövaren lojalt försökt att följa föreläggandet men inte lyckats fullt ut, kontra att den obstruerat och över huvud taget inte försökt följa föreläggandet.

I *punkten fyra* anges att även hindrande av verkställighet av tillsynsmyndighetens tillsynsåtgärder med mera ska betraktas som en allvarlig överträdelse. Detta kräver någon form av passiv eller aktiv obstruktion av den åtgärd som tillsynsmyndigheten försökt genomföra, till exempel genom att den vägrats tillträde till lokaler eller att genomföra säkerhetsrevisioner. Som följd har detta kunnat leda till ökad riskexponering, till exempel genom att en sårbarhet inte har kunnat upptäckas eller åtgärdas i tid. Det bör poängteras att verksamhetsutövarens utnyttjande av sin rätt att överklaga tillsynsmyndighetens beslut inte utgör exempel på sådant beteende som bestämmelsen tar sikte på.

Av *punkten fem* följer att även oriktiga uppgifter ska utgöra en allvarlig överträdelse. Med ”oriktig uppgift” avses felaktiga eller missvisande uppgifter, men även utelämnade uppgifter som borde ha lämnats, jfr 49 kap. 5 § skatteförfarandelagen (2011:1244). Bestämmelsen tar inte sikte på oriktiga uppgifter i alla skeden, utan är begränsad till sådana som lämnas avseende riskhanteringsåtgärder eller rapporteringsskyldigheter.

Förelägganden

6 § Tillsynsmyndigheten får meddela de förelägganden som behövs för att verksamhetsutövare ska uppfylla skyldigheterna som följer av 1 §.

Förelägganden enligt denna paragraf får förenas med vite.

Paragrafen genomför artiklarna 32.4 b–d och f, 33.4 b–d och f, 34.6 samt 36 (delvis). Innehållet behandlas i avsnitt 9.5.1.

Första stycket fastställer tillsynsmyndighetens rätt att använda förelägganden i syfte att få en verksamhetsutövare att upphöra med en överträdelse.

Andra stycket anger att förelägganden får förenas med vite. Viten regleras i lagen (1985:206) om viten.

7 § Tillsynsmyndigheten får förelägga en verksamhetsutövare att offentliggöra information på det sätt som tillsynsmyndigheten beslutar rörande överträdelser av denna lag och föreskrifter som har meddelats med stöd av lagen.

Tillsynsmyndigheten får förelägga en verksamhetsutövare att informera de användare som kan påverkas av ett betydande cyberhot om hotet och vilka skydds- eller motåtgärder de kan vidta.

Förelägganden enligt denna paragraf får förenas med vite.

Paragrafen genomför artiklarna 32.4 e och h, 33.4 e och g samt 36 (delvis). Innehållet behandlas i avsnitt 9.5.2–3.

Första stycket ger möjligheten för tillsynsmyndigheten att tvinga en verksamhetsutövare att offentliggöra en överträdelse av lagens bestämmelser. Tillsynsmyndigheten får besluta hur och var ett sådant offentliggörande ska ske, samt vad det ska innehålla.

Andra stycket anger tillsynsmyndighetens rätt att förelägga en verksamhetsutövare att informera berörda användare om ett betydande cyberhot. Informationen ska ange vilka skydds- eller motåtgärder som användarna kan vidta för att undvika eller minska effekterna av hotet. Det kan till exempel röra sig om användning av kryptering, byte av lösenord eller uppgradering av programvaruversioner.

Tredje stycket ger tillsynsmyndigheten möjlighet att förena förelägganden enligt ovan med vite.

Förbud att utöva ledningsfunktion

8 § Om ett föreläggande enligt 6 § inte följts får tillsynsmyndigheten ingripa mot en person som ingår i verksamhetsutövarens ledning. Ingripande sker genom att tillsynsmyndigheten ansöker hos allmän förvaltningsdomstol om att en person inte ska få vara befattningshavare hos en viss verksamhetsutövare (förbud).

Ett sådant ingripande får riktas mot den som är befattningshavare enligt 3 § andra stycket lagen (2014:836) om näringsförbud.

Ett ingripande får endast göras om överträdelsen som ligger till grund för föreläggandet är allvarlig och om personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Paragrafen genomför artikel 32.5 b (delvis) samt 36 (delvis) och behandlas i avsnitt 9.5.6.

Första stycket anger det grundläggande villkoret för att sanktionen ska få användas, nämligen att det utfärdats ett åtgärdsföreläggande mot en verksamhetsutövare och att detta inte följts inom utsatt tid. I sådana lägen kan tillsynsmyndigheten – om övriga förutsättningar bedöms uppfyllda – ansöka hos förvaltningsdomstol om att en person i verksamhetsutövarens ledning ska förbjudas att utöva ledningsfunktion hos verksamhetsutövaren.

Andra stycket anger vilken personkrets som kan komma i fråga för sanktionen. Av 3 § andra stycket lagen (2014:836) om näringsförbud följer att det rör sig om:

1. i kommanditbolag: komplementär,
2. i andra handelsbolag: bolagsman,
3. i aktiebolag, ömsesidiga försäkringsbolag och ömsesidiga tjänstepensionsbolag: ledamot och suppleant i styrelsen samt verkställande direktör och vice verkställande direktör,
4. i sparbanker, ekonomiska föreningar, försäkringsföreningar och tjänstepensionsföreningar: ledamot och suppleant i styrelsen samt verkställande direktör och vice verkställande direktör,
5. i europeiska ekonomiska intressegrupperingar med säte i Sverige: företagsledare,
6. i europabolag och europakooperativ med säte i Sverige: ledamot och suppleant i förvaltnings-, lednings- eller tillsynsorgan samt verkställande direktör och vice verkställande direktör,

7. i utländska filialer som omfattas av lagen (1992:160) om utländska filialer m.m.: verkställande direktör och vice verkställande direktör, och
8. i stiftelser som omfattas av 2 kap. 3 § bokföringslagen (1999:1078): ledamot och suppleant i styrelsen samt, när en stiftelse har anknuten förvaltning, sådana befattningshavare hos förvaltaren som anges i detta stycke.

Av *tredje stycket* följer att sanktionen endast kan komma i fråga vid allvarliga överträdelser (se avsnitt 9.4.2). Det kan till exempel röra sig om att samma individ vid flera tillfällen hindrat att en viss riskhanteringsåtgärd vidtagits eller vägrat följa tillsynsmyndighetens förelägganden. Därtill krävs att den person förbudet riktar sig mot kan hållas ansvarig för överträdelsen, genom att denne uppsåtligen eller av grov oaktsamhet har orsakat den aktuella överträdelsen. Detta medför att sanktionen inte kan tillämpas på en individ som förvisso har orsakat en överträdelse, men där det skett till följd av oaktsamhet (som inte varit att beteckna som grov).

9 § Ett beslut om förbud enligt 8 § fattas av förvaltningsrätten på ansökan från tillsynsmyndigheten. En ansökan ska innehålla uppgifter om

1. den person som ansökan avser,
2. verksamhetsutövaren,
3. överträdelsen och de omständigheter som behövs för att kännetecknа den, och
4. de bestämmelser som är tillämpliga på överträdelsen.

Ett förbud ska tidsbegränsas till lägst ett år och högst tre år och ska upphävas omedelbart när föreläggandet har följts.

Förbud får inte riktas mot offentliga verksamhetsutövare.

Ansökan ska prövas skyndsamt av domstolen.

Paragrafen genomför artikel 32.5 b (delvis) och 36 (delvis) och behandlas i avsnitt 9.5.6.

I *första stycket* anges att det är förvaltningsrätten som beslutar om sanktionen efter ansökan från en tillsynsmyndighet och anger vidare vilka uppgifter som måste finnas i ansökan för att domstolen ska kunna pröva den. Bestämmelserna kompletterar allmänna bestämmelserna en ansökans innehåll som följer av 3 och 4 §§ förvaltningsprocesslagen (1971:291). Uppgifter om verksamhetsutövaren behövs för att denne ska kunna underrättas vid ett beslutat förbud, samt att ett sådant förbud ska kunna registreras hos registerförande myndighet.

Enligt *andra stycket* ska ett förbud tidsbegränsas till lägst ett och högst tre år. Vidare anges att förbudet ska upphävas omedelbart när föreläggandet har följts. I direktivet betonas att sanktionen är en tillfällig åtgärd för att framtvinga att verksamhetsutövaren avhjälper de aktuella bristerna eller uppfyller de krav som tillsynsmyndigheten ställt. När så har skett ska förbudet alltså omedelbart hävas och detta kan således inträffa långt innan tidsbegränsningen löpt ut.

I *tredje stycket* anges en ytterligare begränsning i sanktionens tillämpningsområde, nämligen att den inte får tillämpas på offentliga verksamhetsutövare. En sådan begränsning följer även av artikel 32.5 i NIS2-direktivet.

Av *fjärde stycket* följer att domstolens handläggning av målet ska ske med förtur. Detta gäller både vid förvaltningsrätten prövning av ansökan och eventuella överklaganden i överinstans.

10 § Ett beslut om förbud ska upphävas om det inte längre finns förutsättningar för förbudet.

Bestämmelsen behandlas i avsnitt 9.5.6. Bestämmelsen ger uttryck för att ett beslut om förbud ska upphävas när det saknas förutsättningar för det. Det kan exempelvis röra sig om att verksamhetsutövaren nu har följt det föreläggande som tillsynsmyndigheten meddelat (och som tidigare inte följts), jfr 9 § andra stycket.

11 § Förvaltningsrätten ska pröva om ett beslutat förbud ska upphävas om tillsynsmyndigheten eller den enskilde begär det, eller om det annars finns skäl för det. Den enskilde ska upplysas om sin rätt att begära att ett förbud ska upphävas.

Om tillsynsmyndigheten bedömer att det inte längre finns förutsättningar för förbudet ska den omedelbart begära att förvaltningsrätten ska upphäva förbudet.

Bestämmelsen behandlas i avsnitt 9.5.6 och anger vad som kan föranleda ett beslut enligt 10 §.

Enligt *första stycket* ska en sådan prövning göras om tillsynsmyndigheten eller den enskilde begär det, eller om det annars finns skäl för det. Exempel på om det annars finns skäl för det kan vara att den enskilde har avlidit, och detta upptäcks av domstolen. Domstolen har då möjlighet att på eget initiativ (*ex officio*) besluta om att förbudet ska upphävas.

Av *andra stycket* följer att tillsynsmyndigheten är skyldig att omedelbart begära att förbudet ska upphävas om förutsättningarna för förbudet har upphört (jfr 9 § andra stycket).

Sanktionsavgift

12 § Tillsynsmyndigheten får besluta att en verksamhetsutövare ska betala en sanktionsavgift till följd av en överträdelse enligt 1 §.

Bestämmelsen genomför artikel 32.4 i, 33.4 h, 34.2, 34.7 samt 36 (delvis) och behandlas i avsnitt 9.6.1. Den ger tillsynsmyndigheten behörighet att besluta om sanktionsavgifter enligt de efterföljande bestämmelserna. Tillsynsmyndigheten får ta ut sanktionsavgift vid överträdelser och det ska ske med tillämpning av strikt ansvar där det saknar betydelse om överträdelsen skett av misstag eller uppsåtligen. Sådana aspekter ska i stället kunna vägas in vid bestämmande av sanktionsavgiftens storlek.

Sanktionsavgiftens storlek

13 § Sanktionsavgiften ska för väsentliga verksamhetsutövare bestämmas till lägst 5 000 kr och högst till det högsta av:

1. Två procent av den väsentliga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 10 000 000 euro.

Bestämmelsen genomför artikel 34.4–5 och 7 (delvis) samt 36 (delvis) och behandlas i avsnitt 9.6.2. Gemensamt för bestämmelserna i 13–15 §§ är miniminivån på 5 000 kronor. Maximinivån beror på vilken typ av verksamhetsutövare det rör sig om. Det stora spannet mellan minimi- och maximibelopp ger tillsynsmyndigheten stor handlingsfrihet kring utformningen av sanktionen. Detta gör att tillsynsmyndighetens kan anpassa sanktionen för att vara effektiv, proportionerlig och avskräckande i varje enskilt fall med beaktande av samtliga omständigheter.

14 § Sanktionsavgiften ska för viktiga verksamhetsutövare bestämmas till lägst 5 000 kr och högst till det högsta av:

1. 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 7 000 000 euro.

Bestämmelsen genomför artikel 34.4–5 och 7 (delvis) samt 36 (delvis), behandlas i avsnitt 9.6.2 och kompletterar 13 §.

15 § Sanktionsavgiften ska för offentliga verksamhetsutövare bestämmas till lägst 5 000 kr och högst 10 000 000 kr.

Bestämmelsen genomför artikel 34.4–5 och 7 (delvis) samt 36 (delvis), behandlas i avsnitt 9.6.2 och kompletterar 13 och 14 §§.

Hur sanktionsavgiften ska bestämmas

16 § När sanktionsavgiftens storlek bestäms ska tillsynsmyndigheten särskilt beakta de omständigheter som följer av 3–5 §§.

Paragrafen genomför artikel 34.1 och är ett förtydligande om att omständigheterna i 3–5 §§ ska beaktas även vid bestämmande av en sanktionsavgift.

Hinder mot att ta ut sanktionsavgift

17 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

En sanktionsavgift får inte heller beslutas för samma överträdelse som lett till att verksamhetsutövaren har påförts en sanktionsavgift enligt Allmänna dataskyddsförordningen.

Paragrafen genomför artikel 35.2 och behandlas i avsnitt 9.6.3.

Bestämmelsen utgör ett uttryck för det så kallade dubbelprövningsförbudet enligt Europakonventionen och kompletterar den allmänna ventilen mot ingripande i 2 § tredje stycket. Bestämmelsen medför inte någon begränsning för tillsynsmyndigheten att besluta om någon annan sanktion än just sanktionsavgift för den aktuella överträdelsen.

Betalning, verkställighet och preskription

18 § En sanktionsavgift får endast tas ut om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Beslut om sanktionsavgift ska delges.

Paragrafen behandlas i avsnitt 9.6.4 och innehåller förfarandebestämmelser för sanktionsavgifter.

18 § första stycket innebär en preskriptionsregel för sådana sanktionsavgifter där den verksamhetsutövaren inte har fått tillfälle att yttra sig inom två år från överträdelsen.

18 § andra stycket anger ett beslut om sanktionsavgift ska delges. Vid delgivning är delgivningslagen (2010:1932) tillämplig.

19 § Sanktionsavgiften ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning ska verkställighet få ske enligt utsökningsbalken.

Sanktionsavgift tillfaller staten.

Paragrafen behandlas i avsnitt 9.6.4 och innehåller förfarandebestämmelse för sanktionsavgifter.

19 § första stycket fastställer när betalning ska ske, och att tillsynsmyndigheten har möjlighet att förlänga den tid som betalning ska ske inom.

19 § andra stycket anger att obetalda avgifter ska få lämnas för indrivning och att sådan verkställighet får ske enligt utsökningsbalkens regler.

Av *19 § tredje stycket* framgår att sanktionsavgift tillfaller staten.

20 § En beslutad sanktionsavgift ska falla bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Paragrafen behandlas i avsnitt 9.6.4 och innebär att en sanktionsavgift preskriberas om inte verkställighet av den har skett inom fem år från det att beslutet fick laga kraft.

Förordnande om att beslut ska gälla omedelbart

21 § Tillsynsmyndigheten får bestämma att ett beslut om föreläggande enligt denna lag ska gälla omedelbart.

Bakgrunden till paragrafen behandlas i avsnitt 9.7.

Bestämmelsen medför en möjlighet för tillsynsmyndigheten att låta förelägganden gälla omedelbart i vissa fall. Det kan exempelvis avse sådana tillsynsåtgärder som måste vidtas omedelbart för att vara verksamma, till exempel att få tillträde till en verksamhetsutövares lokaler eller dokumentation. Det kan även exempelvis gälla skyldigheten att offentliggöra information om ett cyberhot enligt 7 § andra stycket.

6 kap. Överklagande

1 § Tillsynsmyndighetens beslut enligt denna lag eller anslutande föreskrifter får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen behandlas i avsnitt 9.8 och fastställer den ordning som ska gälla för överklagande av beslut enligt lagen. Bestämmelsen innebär att beslut som överklagas ska prövas av den förvaltningsrätt inom vars domkrets ärendet först prövats. Förvaltningsrättens avgörande kan överklagas till behörig kammarrätt, men det krävs prövningstillstånd för att målet ska tas upp till prövning.

14.2 Förslaget till lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet

Genom toppdomänlagen är artikel 28 i NIS2-direktivet delvis redan genomförd. Det finns dock särskilda bestämmelser i 28.1, 28.2 och 28.5 som kräver en ändring av lagen.

Rubriken och 1 §

Denna lag gäller teknisk drift av toppdomäner *med huvudsakligt etableringsställe i* Sverige på *i*nternet. *Vidare omfattar lagen* tilldelning och registrering av domännamn under dessa toppdomäner.

Ändringar av paragrafen genomför artikel 28.1. Övervägandena finns i avsnitt 6.3.

Som framgår av avsnitt 6.3 är syftet med ändringen att toppdomänlagen inte bara ska omfatta nationella toppdomäner för Sverige utan även toppdomänen .nu. Vidare är det tillräckligt att toppdomänen har huvudsakligt etableringsställe i Sverige. Vad som utgör huvudsakligt etableringsställe följer av förslaget till cybersäkerhetsförordning 3 §.

Skälet till dessa förändringar är att artikel 28.1 har en bredare ansats genom att den använder begreppet registreringsenhet för toppdomäner som definieras som en verksamhet som har delegerats en specifik toppdomän och som ansvarar för att administrera, förvalta, sköta teknisk drift samt registrering av domännamn under en specifik toppdomän, dock inte om toppdomänen endast avses för eget bruk.

Förslaget till cybersäkerhetslag omfattar registreringsenheter för toppdomäner om det huvudsakliga etableringsstället finns i Sverige.

Som en följd av ändringarna i 1 § behöver även författningsrubriken anpassas.

2 §

I denna lag avses med

domännamnssystemet: det internationella hierarkiska system som för befordringsändamål på Internet används för att tilldela domännamn,

domän: nivå i domännamnssystemet och del av domännamn,

domännamn: unikt namn sammansatt av domäner, där en i domännamnssystemet lägre placerad domän står före en domän som är högre placerad i systemet,

toppdomän: den domän som återfinns sist i ett domännamn,

administration: teknisk drift av en toppdomän samt tilldelning och registrering av domännamn under denna,

domänadministratör: den som ansvarar för administration av en toppdomän,

namnserver: dator i ett elektroniskt kommunikationsnät som programmerats så att den lagrar och distribuerar information om domännamn samt tar emot och svarar på frågor om domännamn.

Paragrafen innehåller definitioner. Förändringarna är en följd av att lagens tillämpningsområde utökats enligt 1 §. Innebörden är att definitionen av nationell toppdomän utgår och att begreppet nationell toppdomän för Sverige ersätts med toppdomän.

6 §

En domänadministratör *ska* föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna

Registret *ska* innehålla

1. domännamnet,
2. namnet på domännamnsinnehavaren och dennes postadress, telefonnummer och adress för elektronisk post,
3. namnet på den som tekniskt administrerar domännamnet och dennes postadress, telefonnummer och adress för elektronisk post,
4. uppgifter om de namnservrar som är knutna till domännamnet,
5. övrig teknisk information som behövs för att administrera domännamnet, *och*
6. *registreringsdatum.*

Uppgifterna i registret *ska* kunna hämtas utan avgift via *i*nternet. *Därutöver ska uppgifter även på begäran lämnas ut skyndsamt till myndigheter och andra med offentligrättsliga uppgifter inom EES.*

Personuppgifter får *endast* göras tillgängliga på *internet* om den registrerade har samtyckt till det.

Domänadministratören är personuppgiftsansvarig för behandling av personuppgifter i registret.

En ändring i paragrafen genomför artikel 28.2.b som innehåller krav om att registreringsuppgifterna även innehåller registreringsdatum. En annan ändring genomför artikel 28.5. Överväganden finns i avsnitt 6.3.

Utredningen har i den delen gjort en ändamålsmässig tolkning av ”legitima åtkomstsökanden av lagliga och vederbörligen motiverade begäran” till att det är myndigheter och andra med offentligrättsliga uppgifter inom EES som begär ut uppgiften. Dessa ska även kunna begära ut uppgifter på annat sätt än genom internet. En följdändring är att det av paragrafen uttryckligen behöver följa att begränsningen om att personuppgifter bara får göras tillgängliga om den registrerade har samtyckt till det, endast avser uppgifter som lämnas genom internet,

alltså inte om de lämnas ut till myndigheter och andra med offentligrättsliga uppgifter på annat sätt. Däremot gäller den allmänna dataskyddsförordningens bestämmelser även för dessa uppgifter.

14.3 Förslaget till lag om ändring i lagen (2022:482) om elektronisk kommunikation

Genom NIS2-direktivet upphävs artikel 40 och 41 i kodexen om elektronisk kommunikation[2] och ersätts med bestämmelserna som följer av NIS2-direktivet.[3] 8 kap. 1–4 §§ lagen (2022:482) om elektronisk kommunikation genomför artiklarna 40, 41 och delvis 108 i kodexen. Utredningen föreslår som följd att dessa paragrafer ska upphävas. Genom att dessa bestämmelser upphävs ska även tre punkter i 12 kap. 1 § lagen om elektronisk kommunikation upphävas. Detta leder till att bestämmelsen ändras på så sätt att punkterna 4–6 upphävs, och att punkterna 7–15 numreras om till 4–12. Avseende artikel 108 i kodexen ska den fortsättningsvis anses genomförd genom 3 kap. 1 § i den föreslagna cybersäkerhetslagen, se avsnitt 14.1.

Övervägandena redogörs för i kapitel 11.

[2] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning).
[3] Se skäl 92 och artikel 43 i NIS2-direktivet.

Kommittédirektiv 2023:30

Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft

Beslut vid regeringssammanträde den 23 februari 2023

Sammanfattning

Europaparlamentet och rådet har nyligen antagit två nya EU-direktiv: direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) och direktivet om kritiska entiteters motståndskraft (CER-direktivet). En särskild utredare ska föreslå de anpassningar av svensk rätt som är nödvändiga för att NIS2-direktivet och CER-direktivet ska kunna genomföras.

Utredaren ska bl.a.

- föreslå hur identifieringen av och krav på entiteter som omfattas av NIS2-direktivet respektive CER-direktivet ska regleras,
- föreslå hur rollfördelningen mellan svenska myndigheter ska se ut med avseende på de olika uppgifter och ansvarsområden som föreskrivs i NIS2-direktivet och CER-direktivet,
- analysera hur den nya regleringen ska fungera vid sidan av säkerhetsskyddsregleringen och föreslå de ändringar som behövs för att uppnå en mer sammanhållen systematik mellan regelverken,

- ta ställning till om det behövs ett starkare och mer omfattande sekretesskydd för uppgifter som kan komma att behandlas enligt direktiven, och
- lämna förslag till nödvändiga författningsändringar.

Uppdraget ska redovisas senast den 23 februari 2024.

Uppdraget att föreslå hur NIS2-direktivet ska genomföras

NIS-direktivet ställer krav på säkerhet i nätverk och informationssystem

Digitaliseringen innebär att en allt större andel av samhällets aktiviteter i olika grad är beroende av nätverk och informationssystem. Den digitala utvecklingen medför stora möjligheter som bl.a. bättre tjänster och ökad effektivitet, men också risker. Därför är informations- och cybersäkerhet i dag en fråga som angår hela samhället. Särskilt höga säkerhetskrav ska ställas när det gäller samhällsviktig verksamhet som, för att upprätthålla nödvändiga samhällsfunktioner, måste fungera under alla förhållanden.

Utmaningarna inom informations- och cybersäkerhetsområdet delas med andra länder. De strategiska lösningarna måste därför utvecklas genom internationell samverkan. De senaste årens utveckling har till stor del drivits av EU-rätten, i synnerhet genom Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet), som antogs den 6 juli 2016.

Syftet med NIS-direktivet var att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen. Direktivet gäller för leverantörer av samhällsviktiga tjänster inom sju särskilt utpekade sektorer: energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Vidare omfattas leverantörer av vissa digitala tjänster.

Enligt direktivet ställs krav på att leverantörerna ska vidta säkerhetsåtgärder för att hantera risker och incidenter i nätverk och informationssystem som de är beroende av för att kunna tillhandahålla

tjänsterna. Leverantörerna ska också rapportera incidenter som har en betydande eller avsevärd påverkan på kontinuiteten i tjänsterna. Medlemsstaterna ska utse behöriga myndigheter med ansvar för att övervaka tillämpningen av direktivet på nationell nivå. I direktivet fastställs även en ram för samarbete både på nationell nivå och mellan medlemsstaterna, vilket ska ske bl.a. genom en särskilt inrättad samarbetsgrupp.

Direktivet har genomförts i svensk rätt genom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174), även kallad NIS-lagen, och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Därutöver har främst Myndigheten för samhällsskydd och beredskap (MSB) meddelat föreskrifter.

Kraven skärps genom det nya NIS2-direktivet

EU har nyligen antagit det så kallade NIS2-direktivet, som ersätter det tidigare NIS-direktivet. Syftet med det nya direktivet är att minska fragmenteringen av den inre marknaden genom att föreskriva minimiregler för ett samordnat regelverk. Tillämpningsområdet för regleringen utvidgas till att omfatta aktörer inom fler sektorer än det tidigare NIS-direktivet. De tillkommande sektorerna är avloppsvatten, förvaltning av IKT-tjänster (mellan företag), offentlig förvaltning, rymden, post- och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, tillverkning, digitala leverantörer och forskning.

Vidare skärps kraven på aktörer genom minimikrav för åtgärder som ska tillämpas för att hantera risker kopplade till säkerheten i respektive aktörs nätverk och informationssystem. Dessutom införs mer precisa rapporteringskrav. I syfte att harmonisera sanktionssystemen i medlemsstaterna innehåller NIS2-direktivet även detaljerade bestämmelser om ingripanden och sanktioner.

En annan nyhet i NIS2-direktivet är införandet av ett system för sakkunnigbedömningar (peer reviews) som ska kunna utföras av cybersäkerhetsexperter utsedda av andra medlemsstater. Deltagandet i sakkunnigbedömningarna är emellertid frivilligt för medlemsstaterna och metodiken för dessa, liksom organisatoriska aspekter, ska etable-

ras av samarbetsgruppen efter det att direktivet har trätt i kraft. Det finns därmed inte skäl att inom ramen för detta uppdrag analysera hur ett eventuellt svenskt deltagande vid sakkunnigbedömningar bör utformas.

Medlemsstaterna ska ha genomfört direktivet senast 21 månader efter dess ikraftträdande.

Vilka aktörer ska omfattas av regleringen?

Enligt NIS-direktivet har medlemsstaterna ansvaret för att fastställa vilka aktörer som uppfyller kriterierna för att klassificeras som leverantörer av samhällsviktiga tjänster. I NIS2-direktivet fastslås i stället ett enhetligt kriterium för vilka aktörer (i direktivet benämnda entiteter) som enligt huvudregeln ska omfattas av direktivets tillämpningsområde. Kriteriet innebär att alla entiteter som är av en viss storlek och av en typ som pekas ut i direktivet omfattas. Även mindre entiteter omfattas av direktivet om de uppfyller vissa specifika kriterier som tar sikte på om entiteten har en nyckelroll för samhället, ekonomin eller en viss sektor som omfattas av direktivet.

En av de nya sektorerna i NIS2-direktivet är offentlig förvaltning. Offentliga aktörer som bedriver verksamhet inom någon av de befintliga sektorerna berörs redan av det nuvarande NIS-regelverket. Inkluderingen av en särskild sektor för offentlig förvaltning innebär dock att offentliga aktörer kommer att omfattas i betydligt högre utsträckning än tidigare. Inom denna sektor är det bara aktörer, som i direktivet benämns offentliga förvaltningsentiteter, på statlig och regional nivå som omfattas. Översatt till svenska förhållanden kan direktivet tolkas så att statliga myndigheter och regioner omfattas, men inte kommuner. Medlemsstaterna är dock fria att bestämma att även de senare ska omfattas. Eftersom direktivets bestämmelser gäller för regioner finns det skäl för att regelverket ska gälla även för kommuner. I samma riktning talar den omständigheten att viss kommunal verksamhet under alla förhållanden kommer att omfattas, när verksamheten bedrivs inom någon av de övriga sektorerna. Det är dock viktigt att också belysa skäl som kan tala mot en full inkludering av kommunerna. Vid denna bedömning ska utredaren beakta bl.a. de eventuellt ökade kostnaderna för staten som en inkludering kan med-

föra. Utredaren ska mot denna bakgrund överväga om kommuner bör omfattas av den nya regleringen.

Forskning är en annan ny sektor i NIS2-direktivet. I sektorn innefattas forskningsorganisationer, vilka i NIS2-direktivet definieras som en entitet vars främsta mål är att bedriva tillämpad forskning eller experimentell utveckling i syfte att utnyttja resultaten av denna forskning i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner. Det är emellertid frivilligt för medlemsstaterna att föreskriva att NIS2-direktivet ska tillämpas på utbildningsinstitutioner, särskilt om de utför kritisk forskningsverksamhet. Utredaren ska mot denna bakgrund överväga om universitet och högskolor, eller ett urval av dessa, bör omfattas av den nya regleringen. Utredaren ska i sina överväganden rörande universitet och högskolor ta hänsyn till principer som säkerställer akademisk frihet, institutionell autonomi och forskningsintegritet samt excellens och öppenhet inom högre utbildning och forskning.

Entiteter som omfattas av direktivets tillämpningsområde ska klassificeras antingen som väsentliga eller som viktiga entiteter, utifrån deras betydelse för den sektor de verkar inom eller den tjänst de tillhandahåller, liksom utifrån deras storlek. Medlemsstaterna ska upprätta en förteckning över väsentliga och viktiga entiteter och regelbundet uppdatera den. För att möjliggöra upprättandet av förteckningen ska entiteterna vara skyldiga att lämna vissa uppgifter till de behöriga myndigheterna. Medlemsstaterna får även inrätta ett system som bygger på att entiteterna själva registrerar sig. De behöriga myndigheterna ska därefter med viss regelbundenhet underrätta kommissionen om bl.a. antalet registrerade entiteter inom olika kategorier.

Mot denna bakgrund behöver det analyseras hur direktivets bestämmelser om registrering av väsentliga och viktiga entiteter ska genomföras i svensk rätt. Dagens reglering bygger på att det är verksamhetsutövaren som är ansvarig för att avgöra om denne omfattas av regelverket och i så fall anmäla sig till tillsynsmyndigheten. Det bör vara utgångspunkten även för genomförandet av det nya direktivet.

Utredaren ska därför

- ta ställning till om kommuner ska omfattas av regleringen,
- överväga om universitet och högskolor, eller ett urval av dessa, ska omfattas av den nya regleringen,

- föreslå ett system för hur entiteter som omfattas av regleringen ska identifieras och registreras, och
- lämna förslag till nödvändiga författningsändringar.

Hur ska rollfördelningen mellan svenska myndigheter se ut?

I likhet med vad som gäller enligt NIS-direktivet ska medlemsstaterna enligt NIS2-direktivet utse en eller flera behöriga myndigheter och en nationell gemensam kontaktpunkt. De behöriga myndigheterna ska utöva tillsyn och övervaka tillämpningen av direktivet på nationell nivå. Den nationella gemensamma kontaktpunkten ska utgöra en sambandsfunktion som säkerställer gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater och ett sektorsövergripande samarbete med andra nationella behöriga myndigheter i medlemsstaten. Liksom NIS-direktivet föreskriver NIS2-direktivet att det ska finnas en eller flera enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) som bl.a. ska ansvara för hanteringen av incidenter. I NIS2-direktivet åläggs dessa ytterligare uppgifter.

NIS2-direktivet innehåller dessutom nya regler om ramverk för storskaliga cybersäkerhetsincidenter och cyberkriser. Varje medlemsstat ska enligt direktivet utse en eller flera behöriga myndigheter med ansvar för hanteringen av sådana incidenter och kriser (cyberkrishanteringsmyndighet).

Vidare ställer NIS2-direktivet större krav på såväl strategiskt som operativt samarbete mellan medlemsstaterna. Det befintliga samarbetet inom samarbetsgruppen förstärks. Det gör även det operativa samarbetet, bl.a. genom att det så kallade CSIRT-nätverket – där företrädare för de nationella CSIRT-enheterna deltar – tilldelas fler arbetsuppgifter.

I NIS2-direktivet regleras även nya forum för samarbete mellan medlemsstaterna. Ett sådant forum är det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), som ska verka stödjande vid samordning och hantering av storskaliga incidenter och cyberkriser. Nätverket ska bestå av företrädare för medlemsstaternas cyberkrishanteringsmyndigheter. Det finns redan i dag på frivillig basis, med MSB som svensk representant, men får i NIS2 en tydlig rättslig grund.

Vid genomförandet av NIS2-direktivet bör systemet för tillsyn utgå från den struktur som finns enligt dagens regelverk. Utöver de ändringar som är nödvändiga med anledning av NIS2-direktivets utökade krav kan det emellertid finnas skäl till ändringar för att åstadkomma en mer effektiv tillsyn. Utredaren ska därför göra en utvärdering av den tillsyn som har bedrivits enligt den nuvarande NIS-regleringen sedan dess införande. Enligt den nu gällande NIS-lagen finns det för varje sektor och för de digitala tjänster som omfattas av lagen en utpekad tillsynsmyndighet som ska ansvara för att övervaka att regelverket följs. De nuvarande tillsynsmyndigheterna är Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket och Post- och telestyrelsen.

Som konstaterats innebär NIS2-direktivet att fler sektorer kommer att omfattas av regelverket än vad som är fallet i dag. Det behöver därför utses tillsynsmyndigheter för de tillkommande sektorerna. Inom vissa av dessa finns redan myndigheter med tillsynsuppgifter inom informationssäkerhet. Exempelvis utövar Post- och telestyrelsen tillsyn enligt säkerhetsskyddslagen (2018:585) över enskilda verksamhetsutövare inom området posttjänster. I dessa fall är det naturligt att myndigheten utses till tillsynsmyndighet för den aktuella sektorn även enligt NIS2-regelverket. I andra fall behöver utredaren överväga vilken myndighet som ska anförtros tillsynsansvaret för sektorn. I enlighet med vad som anges nedan bör tillsynsmyndigheterna enligt CER-direktivet som utgångspunkt vara desamma som tillsynsmyndigheterna enligt NIS2-direktivet. Även detta behöver beaktas av utredaren.

MSB har i dag en bred roll kopplat till NIS-regleringen som bl.a. innefattar ett samordningsansvar för tillsynen. Myndigheten leder bl.a. ett samarbetsforum där samtliga tillsynsmyndigheter och Socialstyrelsen ingår. Därutöver är MSB nationell gemensam kontaktpunkt och företräder Sverige i den strategiska samarbetsgruppen. MSB har även rollen som Sveriges CSIRT-enhet och deltar därmed också i CSIRT-nätverket. Denna ansvarsfördelning är ändamålsenlig och utgångspunkten för utredarens uppdrag bör därför vara att MSB ska fullgöra motsvarande uppgifter enligt det nya NIS2-regelverket. Mot bakgrund av de närliggande uppgifter som MSB har i dag och den kompetens som finns inom myndigheten bör MSB även utses till cyberkrishanteringsmyndighet. Det innebär att MSB även fortsättningsvis bör företräda Sverige i det nya europeiska kontaktnätverket för cyberkriser. Det behöver analyseras om och i vilken utsträckning som

MSB:s nuvarande mandat behöver förändras för att myndigheten ska kunna fullgöra dessa uppgifter.

NIS2-direktivet anger vidare att medlemsstaterna är skyldiga att anta en nationell strategi för cybersäkerhet. Som en del av strategin ska medlemsstaterna särskilt anta riktlinjer på en rad områden. Dessutom ska medlemsstaterna anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser där mål och villkor för hanteringen av storskaliga cybersäkerhetsincidenter och kriser fastställs. Utformningen av den nationella strategin och den nationella planen bör emellertid inte omfattas av utredarens uppdrag utan bör i stället hanteras i särskild ordning.

Utredaren ska därför

- utvärdera den tillsyn som har bedrivits enligt NIS-lagen sedan dess införande,
- föreslå vilka myndigheter som ska utöva tillsyn över de tillkommande sektorerna i NIS2-direktivet,
- analysera vilka ändringar av den befintliga tillsynsstrukturen som i övrigt behövs,
- analysera vilka ändringar som behövs för att MSB i enlighet med NIS2-direktivets krav ska kunna utöva uppdraget som nationell gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet samt deltagare i de samarbetsnätverk som direktivet lägger grund för, och
- lämna förslag till nödvändiga författningsändringar.

Vilka krav ska ställas på aktörerna?

NIS2-direktivet skärper kraven på väsentliga och viktiga entiteter vad gäller riskhanteringsåtgärder, i nuvarande lagstiftning benämnda som säkerhetsåtgärder, och rapporteringsskyldigheter. Medlemsstaterna ska säkerställa att entiteterna vidtar tekniska, operationella och organisatoriska åtgärder för att hantera risker för säkerheten i nätverks- och informationssystem. Åtgärderna ska vara proportionella, med beaktande av bl.a. entitetens storlek, sannolikheten för att incidenter inträffar och den påverkan de skulle ha. Direktivet fastställer vissa minimikrav på åtgärder som entiteterna ska vidta. Kraven

omfattar bl.a. rutiner för riskanalys och säkerhet i informationssystem, incidenthantering samt rutiner för kryptografi och, om det är lämpligt, kryptering. Åtgärderna ska även innefatta säkerhet i leveranskedjor.

Direktivet ålägger även medlemsstaterna att säkerställa att entiteterna rapporterar incidenter som har en betydande inverkan på tillhandahållandet av deras tjänster till CSIRT-enheten eller nationella behöriga myndigheter. Rapportering ska ske vid olika tillfällen efter att en incident har inträffat och en slutlig rapport med mer detaljerad information ska avges inom en månad från det att den första incidentrapporten lämnades.

Enligt nuvarande ordning ska incidenter rapporteras till CSIRT-enheten, det vill säga MSB. Mot bakgrund av den roll som MSB i egenskap av CSIRT-enhet har när det gäller hantering av incidenter bör detta vara utgångspunkten även vid genomförandet av NIS2-direktivet.

Medlemsstaterna får enligt direktivet bestämma att entiteter som ett led i riskhanteringen ska använda särskilda certifierade produkter i nätverks- och informationssystem. Utredaren ska analysera hur ändamålsenlighet och proportionalitet i sådana föreskrifter kan beaktas samt hur de ska meddelas. I det sammanhanget behöver det beaktas att kommissionen har getts befogenhet att genom delegerade akter föreskriva att vissa kategorier av entiteter ska vara skyldiga att använda vissa certifierade produkter.

Utredaren ska därför

- analysera hur direktivets krav på riskhanteringsåtgärder och incidentrapportering ska genomföras i svensk rätt, och
- lämna förslag till nödvändiga författningsändringar.

Vilka befogenheter ska tillsynsmyndigheterna ha?

I likhet med det tidigare direktivet förutsätts det att tillsynsmyndigheterna har tillräckliga verktyg för att se till att regelverket följs. NIS2-direktivet uppställer även detaljerade krav på vissa befogenheter som tillsynsmyndigheterna ska ha och på sanktioner som ska kunna tillgripas. Kraven skiljer sig åt mellan väsentliga respektive viktiga entiteter. Vid tillsynen av väsentliga entiteter ska tillsynsmyndigheterna ha större befogenheter och tillsynen ska vara såväl proaktiv

som reaktiv. För viktiga entiteter ska tillsynen vara reaktiv och mindre omfattande.

Direktivet föreskriver flera åtgärder som saknar direkt motsvarighet i svensk rätt. När det gäller väsentliga entiteter kräver direktivet bl.a. att det ska finnas möjlighet – om andra åtgärder visar sig vara ineffektiva – att tillfälligt upphäva en certifiering eller auktorisation för entitetens verksamhet och att tillfälligt förbjuda personer i entitetens ledning från att utöva ledningsfunktioner. Utredaren behöver analysera hur den nationella regleringen av sådana åtgärder ska förhålla sig till relevant reglering på andra områden, t.ex. associationsrättsliga regler eller sektorsspecifika regler som innehåller krav på certifiering eller auktorisation för viss verksamhet.

Det är enligt direktivet upp till medlemsstaterna att avgöra om bestämmelser om straffansvar ska införas för överträdelser av den nationella regleringen.

Vid genomförandet av NIS-direktivet gjordes bedömningen att överträdelser inte skulle vara straffsanktionerade (prop. 2017/18:205 s. 64 f.). Det saknas skäl att frångå den bedömningen. Inriktningen ska alltså vara att sanktioner för överträdelser av den nya regleringen ska vara av administrativt slag.

Utredaren ska därför

- analysera vilka befogenheter i fråga om tillsyn och sanktioner som tillsynsmyndigheterna enligt NIS2-direktivet bör ha, och
- lämna förslag till nödvändiga författningsändringar.

Uppdraget att föreslå hur CER-direktivet ska genomföras

CER-direktivet ställer krav på motståndskraft i samhällsviktig verksamhet

Säkerheten för samhällsviktig verksamhet, inbegripet kritisk infrastruktur, är en i högsta grad aktuell fråga. Motståndskraften hos sådan verksamhet är central för att förebygga, motstå och hantera situationer som riskerar att innebära allvarliga störningar av viktiga samhällsfunktioner. Arbetet med att stärka motståndskraften behöver ske på alla nivåer i samhället, och även på unionsnivå.

Inom EU har det under en längre tid pågått arbete med frågor kopplade till skydd av kritisk infrastruktur. Den unionsrättsliga regleringen har dock främst skett sektorsvis och endast tagit sikte på vissa aspekter av motståndskraft hos aktörer inom de sektorerna. Bland annat finns det regler som tar sikte på skyddet för europeisk kritisk infrastruktur inom energi- respektive transportsektorn i rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna. Vid utvärderingen av detta direktiv har det konstaterats att skyddsåtgärder som tar sikte på enskilda tillgångar inte är tillräckliga för att förhindra alla störningar från att uppstå. I stället har det bedömts att ansatsen bör ändras i riktning mot att säkerställa motståndskraften hos de aktörer som bedriver samhällsviktig verksamhet.

EU har nyligen antagit det så kallade CER-direktivet, vilket ersätter rådets direktiv 2008/114/EG. Enligt CER-direktivet ska medlemsstaterna identifiera aktörer (så kallade kritiska entiteter) som tillhandahåller samhällsviktiga tjänster inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymden samt produktion, bearbetning och distribution av livsmedel.

Direktivet ålägger de kritiska entiteterna skyldigheter att bl.a. vidta åtgärder för att stärka sin motståndskraft och att rapportera incidenter. Det innehåller också bestämmelser om tillsyn och sanktioner. Vidare fastställs i direktivet en ram för samarbete mellan medlemsstaterna.

Medlemsstaterna ska ha genomfört direktivet senast 21 månader efter dess ikraftträdande.

Hur ska rollfördelningen mellan svenska myndigheter se ut?

Direktivet ålägger medlemsstaterna att utse en nationell gemensam kontaktpunkt för samarbetet med andra medlemsstater och en eller flera behöriga myndigheter som ska ansvara för direktivets tillämpning på nationell nivå. Frågan vilka befogenheter de behöriga myndigheterna ska ha för att kunna utöva en effektiv tillsyn och beivra överträdelser behandlas i ett särskilt avsnitt nedan.

För att säkerställa samstämmighet mellan de två direktiven föreskrivs det i dessa att entiteter som har identifieras som kritiska entiteter enligt CER även ska anses vara väsentliga entiteter enligt NIS2. I direktiven anges vidare att de behöriga myndigheterna enligt respektive direktiv ska utbyta information med varandra om hot och incidenter samt om åtgärder som myndigheterna vidtar. Mot denna bakgrund är en naturlig utgångspunkt att samma myndighet som utövar tillsyn över en viss entitet enligt NIS2-direktivet även utövar tillsyn över entiteten enligt CER-direktivet. På så vis kan det säkerställas att tillsynen enligt de två direktiven utövas på ett effektivt och samordnat sätt.

MSB har en bred kompetens kopplad till skyddet för samhällsviktig verksamhet och kritisk infrastruktur. Myndigheten fullgör också rollen som nationell gemensam kontaktpunkt för det arbete som i dag bedrivs inom ramen för direktiv 2008/114/EG. Av dessa skäl, och för att säkerställa samstämmighet med NIS2-regleringen, bör MSB utses till nationell gemensam kontaktpunkt även enligt CER-direktivet.

MSB har i dag en samordnande roll mellan tillsynsmyndigheterna enligt NIS-regelverket. För att säkerställa att NIS2-direktivet och CER-direktivet genomförs och tillämpas på ett effektivt och koordinerat sätt bör MSB ha en motsvarade roll enligt båda regelverken. För att få en samlad bild av genomförandet och tillämpningen behöver MSB få del av relevant information från de övriga behöriga myndigheterna. MSB bör även ha en samordnande roll i fråga om den riskbedömning som de behöriga myndigheterna är skyldiga att göra.

Medlemsstaterna ska enligt CER-direktivet även anta en nationell strategi för kritiska entiteters motståndskraft. Frågan om hur en sådan strategi ska utformas bör emellertid inte omfattas av utredarens uppdrag utan i stället hanteras i särskild ordning, i likhet med den nationella strategin för cybersäkerhet som medlemsstaterna ska anta enligt NIS2-direktivet.

Utredaren ska därför

- föreslå ett system för tillsyn som uppfyller CER-direktivets krav och som är samordnat med det system som föreslås för NIS2,
- föreslå vilka myndigheter som ska utses till tillsynsmyndigheter,
- ta ställning till hur MSB:s roll som nationell gemensam kontaktpunkt ska utformas och regleras, och

- lämna förslag till nödvändiga författningsändringar.

Hur ska identifieringen av de kritiska entiteterna gå till?

Medlemsstaterna är skyldiga att identifiera kritiska entiteter inom de sektorer och undersektorer som omfattas av direktivet och upprätta en förteckning över dessa. För att en aktör ska anses vara en kritisk entitet ska tre kriterier vara uppfyllda: för det första att aktören tillhandahåller en eller flera samhällsviktiga tjänster, för det andra att aktören verkar på medlemsstatens territorium och har sin kritiska infrastruktur belägen där, för det tredje att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten eller tjänsterna. För det fall en kritisk entitet tillhandahåller samma eller liknande samhällsviktiga tjänster i sex eller fler medlemsstater ska kommissionen ha möjlighet att fastställa att denna ska betraktas som en så kallad kritisk entitet av särskild europeisk betydelse. För sådana entiteter gäller särskilda bestämmelser enligt direktivet.

En icke uttömmande förteckning över tjänster som ska anses samhällsviktiga kommer att fastställas av kommissionen genom en delegerad akt. Det kan inte uteslutas att det kan finnas behov av att låta den nationella regleringen omfatta aktörer som tillhandahåller även andra samhällsviktiga tjänster än de som kommissionen pekar ut. Utredaren behöver därför ta ställning till hur regler för att peka ut samhällsviktiga tjänster ska utformas. Det måste även analyseras hur direktivets kriterier för vad som utgör en betydande störning ska tillämpas i en svensk kontext och hur eventuella tröskelvärden ska fastställas. Enligt den nuvarande nationella NIS-regleringen får MSB, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela föreskrifter dels om vilka tjänster som är samhällsviktiga tjänster, dels om vad som avses med en betydande störning. En motsvarande ordning skulle kunna vara lämplig för genomförandet av CER-direktivet. Det behöver även övervägas vem som ska ansvara för identifieringen av de kritiska entiteterna, hur identifieringsförfarandet ska gå till och hur förteckningen över de kritiska entiteterna ska upprättas och uppdateras.

Vidare måste utredaren analysera om särskilda nationella bestämmelser behövs i fråga om identifieringen och anmälan till kommissionen av kritiska entiteter av särskild europeisk betydelse.

Utredaren ska därför

- föreslå hur kritiska entiteter ska identifieras samt hur en förteckning över dessa kan upprättas och uppdateras i enlighet med direktivets krav, och
- lämna förslag till nödvändiga författningsändringar.

Vilka krav ska ställas på de kritiska entiteterna?

Medlemsstaterna ska enligt CER-direktivet säkerställa att kritiska entiteter utför en riskbedömning som omfattar alla relevanta risker som skulle kunna leda till incidenter. Vidare ska medlemsstaterna se till att de kritiska entiteterna vidtar lämpliga och proportionella åtgärder för att säkerställa sin motståndskraft. Åtgärderna ska grundas på den riskbedömning som den kritiska entiteten själv har utfört men även på relevant information från medlemsstaternas riskbedömning som har delats med entiteten. Direktivet uppställer även vissa minimikrav på åtgärder som ska vidtas. Kommissionen kommer vid en senare tidpunkt att komplettera dessa minimikrav med icke bindande riktlinjer och med tekniska specifikationer. Utredaren ska mot denna bakgrund analysera hur reglerna om de kritiska entiteternas riskbedömning ska utformas och vid behov kunna kompletteras. Vid den analysen ska utredaren även överväga hur CER-direktivets krav på riskbedömningar förhåller sig till liknande krav i annan reglering.

Vidare innehåller direktivet krav på att kritiska entiteter ska rapportera incidenter som medför eller skulle kunna medföra en betydande störning vid tillhandahållandet av samhällsviktiga tjänster. Parametrar som ska beaktas vid bedömningen av en störnings betydelse är antalet användare som påverkas av störningen, störningens varaktighet och det geografiska område som påverkas av störningen. Hur den närmare bedömningen ska gå till regleras emellertid inte i direktivet och är därför en fråga som utredaren behöver analysera.

Incidenter ska enligt CER-direktivet rapporteras till den behöriga myndigheten. För det fall en medlemsstat har utsett flera behöriga myndigheter måste det anses vara upp till medlemsstaten att avgöra till vilken eller vilka av dessa som rapporteringen ska ske. Vid genomförandet av NIS-direktivet gjordes, som framgått ovan, bedömningen att incidenter skulle rapporteras till MSB i myndighetens egenskap av CSIRT-enhet. Motsvarande fråga behöver analyseras i fråga om

CER-direktivet. Utredaren behöver således ta ställning till vilken eller vilka myndigheter som incidenter ska rapporteras till.

Utredaren ska därför

- analysera hur direktivets krav på riskbedömning, åtgärder för motståndskraft och incidentrapportering för kritiska entiteter ska genomföras i svensk rätt,
- lämna förslag till nödvändiga författningsändringar.

Hur ska systemet för bakgrundskontroller utformas?

Medlemsstaterna ska enligt CER-direktivet anta regler som ger kritiska entiteter rätt att i vissa fall begära bakgrundskontroller. Bakgrundskontroller ska kunna begäras avseende bl.a. personer som innehar en känslig roll i den kritiska entiteten, som har tillträde till entitetens lokaler eller tillgång till dess informationssystem eller som är aktuella för en anställning som innefattar en sådan roll, sådant tillträde eller sådan tillgång. En bakgrundskontroll ska bekräfta personens identitet och ska även innefatta uppgifter från belastningsregistret. Utredaren behöver analysera hur direktivets krav på bakgrundskontroller ska genomföras i svensk rätt. Det behöver särskilt övervägas hur ett system för belastningsregisterkontroll ska utformas.

Utgångspunkten för utredarens överväganden ska vara att de kritiska entiteterna på ett effektivt sätt ska kunna få kännedom om eventuella uppgifter om brott som kan vara av betydelse för deltagande i verksamheten. Samtidigt måste det beaktas att de uppgifter som finns i belastningsregistret är av integritetskänsligt slag. Systemet för belastningsregisterkontroll bör utformas på ett sätt som innebär att integritetsintrånget för den enskilde inte blir större än nödvändigt.

Utredaren behöver bl.a. ta ställning till vem som ska ha rätt att begära ut uppgifterna från Polismyndigheten. Systemet ska emellertid inte bygga på att den kritiska entiteten själv begär ut uppgifterna. Även om det i belastningsregisterregleringen finns exempel på situationer där enskilda har getts rätt att begära uppgifter om andra enskilda kan en sådan lösning inte anses vara lämplig i detta fall.

Utredaren ska därför

- föreslå hur ett system med bakgrundskontroller ska utformas, och
- lämna förslag till nödvändiga författningsändringar.

Vilka befogenheter ska tillsynsmyndigheterna ha?

I likhet med NIS2-direktivet förutsätter CER-direktivet att tillsynsmyndigheterna har tillräckliga verktyg för att se till att regelverket följs. Myndigheterna ska enligt direktivet ha rätt att utföra inspektioner av såväl kritisk infrastruktur som de kritiska entiteternas riskhanteringsåtgärder. Tillsynsmyndigheterna ska också ha befogenhet att utföra säkerhetsrevision eller att begära att de kritiska entiteterna genomgår sådan. Vidare ska myndigheterna kunna begära att de kritiska entiteterna lämnar information som är nödvändig för att utvärdera entiteternas riskhanteringsåtgärder och dokumentation gällande genomförandet av dessa åtgärder.

Tillsynsmyndigheterna ska även ha befogenhet att kräva att kritiska entiteter som inte fullgör sina skyldigheter vidtar rättelse. Dessutom ska medlemsstaterna anta regler om effektiva, proportionella och avskräckande sanktioner för överträdelser av direktivets bestämmelser.

I jämförelse med NIS2-direktivet lämnar CER-direktivet förhållandevis stort bedömningsutrymme för medlemsstaterna vad gäller den närmare utformningen av tillsynsmyndigheternas verktyg. Som konstaterats ovan kommer emellertid samtliga entiteter som omfattas av CER-direktivet även att omfattas av NIS2-direktivet. Vidare bör tillsynsmyndigheterna vara desamma för båda direktiven. Det behöver inte nödvändigtvis betyda att det är lämpligt att samtliga verktyg för tillsynsmyndigheterna som föreskrivs i NIS2-direktivet ska kunna tillämpas även i fråga om kritiska entiteter enligt CER-direktivet eller att sanktionsavgifterna måste ha samma storlek. Utgångspunkten för utredarens överväganden ska dock vara att tillsynen enligt båda direktiven ska kunna utövas på ett samordnat och effektivt sätt. Det ska också eftersträvas att de ingripanden och sanktioner som kan bli aktuella enligt respektive direktiv framstår som proportionerliga i förhållande till varandra och lever upp till enskildas behov av förutsebarhet.

Utredaren ska därför

- analysera vilka befogenheter i fråga om tillsyn och sanktioner som tillsynsmyndigheterna enligt CER-direktivet bör ha, och
- lämna förslag till nödvändiga författningsändringar.

Gemensamma frågor för NIS2-direktivet och CER-direktivet

Förhållandet till säkerhetsskyddsregleringen

Säkerhetsskyddslagen är den lag som reglerar skyddsåtgärder för de mest skyddsvärda verksamheterna i samhället. Lagen gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Säkerhetsskyddslagstiftningens huvudsyfte är alltså att skydda verksamheter som har betydelse för Sveriges säkerhet ur ett nationellt perspektiv mot i första hand antagonistiska angrepp.

Av artikel 4.2 i fördraget om Europeiska unionen följer att den nationella säkerheten ska vara varje medlemsstats eget ansvar. I NIS2-direktivet och CER-direktivet betonas också att direktiven inte påverkar medlemsstaternas ansvar för att skydda nationell säkerhet. Offentliga förvaltningsentiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning är i sin helhet undantagna från direktivens tillämpningsområde. När det gäller andra aktörer har medlemsstaterna möjlighet att besluta att särskilda entiteter med verksamhet på de aktuella områdena ska vara undantagna från skyldigheter enligt direktivet.

Reglerna om undantag för särskilda entiteter i NIS2-direktivet innebär sammanfattningsvis följande. Om entiteten endast delvis bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning får medlemsstaten besluta att entiteten ska undantas från direktivets krav på riskhanteringsåtgärder och incidentrapportering, när det gäller den delen av verksamheten. Motsvarande gäller med avseende på sådana tjänster som en entitet tillhandahåller uteslutande till offentliga förvaltningsentiteter på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning. Om en entitet bedriver verksamhet eller tillhandahåller tjänster uteslutande på dessa områden, får entiteten undantas även från reglerna om registrering. På motsvarande sätt får medlemsstaterna enligt CER-direktivet besluta att flertalet av det direktivets bestämmelser inte ska vara tillämpliga på särskilda kritiska entiteter som bedriver verksamhet inom de aktuella områdena.

Direktivens bestämmelser om undantag för särskilda entiteter saknar motsvarighet i svensk rätt. Undantaget för säkerhetskänslig verksamhet i NIS-lagen är i stället konstruerat på det sättet att lagen inte gäller för verksamhet som omfattas av säkerhetsskyddslagen. Regleringen bygger på att en leverantör av samhällsviktiga eller digitala tjänster som bedriver säkerhetskänslig verksamhet själv ska bedöma vilka delar av verksamheten som omfattas av säkerhetsskyddslagen respektive NIS-lagen. En sådan lösning framstår emellertid inte som förenlig med hur möjligheten till undantag för verksamhet som rör nationell säkerhet har formulerats i NIS2-direktivet och CER-direktivet. Det behöver därför analyseras hur direktivens möjlighet att undanta specifika aktörer ska genomföras i svensk rätt.

I detta sammanhang framstår det som naturligt att utgå från den befintliga tillsynsstrukturen inom säkerhetsskyddsregleringen. Denna innebär att tillsynsansvaret är fördelat på Försvarsmakten, Säkerhetspolisen och vissa andra utpekade myndigheter som ansvarar för tillsynen av verksamhetsutövare inom olika sektorer. Tillsynsmyndigheterna ska genom systematisk kartläggning identifiera vilka verksamhetsutövare och andra tillsynsobjekt som finns inom myndigheternas respektive tillsynsområden. Myndigheterna ska ha en aktuell förteckning över sina tillsynsobjekt. Det framstår därför som en effektiv ordning att dessa myndigheter ges rätt att besluta om undantag från skyldigheter enligt direktiven för sådana aktörer som står under deras tillsyn enligt säkerhetsskyddslagen. Utredaren får emellertid föreslå även andra lösningar om det finns skäl för det. Inriktningen för förslagen ska vara att säkerhetskänslig verksamhet undantas från den nya regleringen i den utsträckning som är möjlig.

Vidare framgår det av både NIS2-direktivet och CER-direktivet att det inte finns någon skyldighet att tillhandahålla information vars utlämnande strider mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar. I skälen i direktivens ingresser anges det att nationella regler till skydd för säkerhetsskyddsklassificerade uppgifter bör beaktas i detta sammanhang.

För att säkerställa att säkerhetsskyddsklassificerade uppgifter inte lämnas ut är det inte tillräckligt att särskilda entiteter som bedriver säkerhetskänslig verksamhet helt eller delvis kan undantas från direktivens krav på bl.a. incidentrapportering. Exempelvis behöver det även säkerställas att uppgifter som rör säkerhetskänslig verksamhet inte

registreras i den europeiska sårbarhetsdatabas som enligt NIS2-direktivet ska upprättas av Enisa eller lämnas ut i samband med sådana rådgivande uppdrag för kritiska entiteter av särskild europeisk betydelse som regleras i CER-direktivet. Det behöver därför införas regler som direkt undantar säkerhetsskyddsklassificerade uppgifter från såväl rapporteringskraven som från annan uppgiftslämning som regleras i direktiven.

Det anförda innebär att delar av en entitets verksamhet kan komma att omfattas av NIS2-direktivets eller CER-direktivets tillämpningsområde samtidigt som andra delar av verksamheten undantas och i stället omfattas av säkerhetsskyddslagen. Det behöver mot denna bakgrund analyseras hur säkerhetsskyddslagens systematik och terminologi i praktiken ska fungera vid sidan om den nya regleringen. Utredaren får föreslå ändringar i säkerhetsskyddsregleringen som behövs för att uppnå en sammanhållen systematik mellan regelverken.

I detta sammanhang finns det särskilt anledning att uppmärksamma tillsynsmyndigheternas befogenheter och bestämmelserna om sanktioner. Tillsynsmyndigheternas befogenheter enligt säkerhetsskyddsregleringen är i flera avseenden mindre långtgående än motsvarande befogenheter som regleras i NIS2-direktivet. Detta skulle i vissa fall kunna få till följd att brister i en aktörs säkerhetsskydd leder till mindre ingripande åtgärder än brister i andra delar av aktörens verksamhet som inte rör säkerhetskänslig verksamhet och som därför omfattas av NIS2-direktivet eller CER-direktivet. Eftersom säkerhetsskyddsregleringen gäller för de mest skyddsvärda verksamheterna i samhället är en sådan ordning inte önskvärd. Utredaren ska därför särskilt analysera vilka ändringar i säkerhetsskyddsregleringen som behövs i detta avseende.

Utredaren ska därför

- föreslå ett system för hur aktörer som bedriver säkerhetskänslig verksamhet ska undantas, med avseende på den verksamheten, från NIS2-direktivets och CER-direktivets krav på bl.a. incidentrapportering,
- föreslå hur säkerhetsskyddsklassificerade uppgifter ska undantas från rapporteringsplikten och andra former av uppgiftslämning som regleras i direktiven,

- analysera hur den nya regleringen ska fungera vid sidan av säkerhetsskyddsregleringen och föreslå ändringar som behövs för att uppnå en mer sammanhållen systematik mellan regelverken, särskilt vad gäller tillsynsmyndigheternas befogenheter och sanktionsavgifternas storlek, och
- lämna förslag till nödvändiga författningsändringar.

Förhållandet till annan unionsrättslig och nationell reglering

Både NIS2-direktivet och CER-direktivet innehåller bestämmelser om förhållandet till sektorsspecifika unionsrättsakter. Exempelvis följer det av CER-direktivet att berörda bestämmelser i det direktivet inte ska vara tillämpliga om det i en sektorsspecifik unionsrättsakt ställs åtminstone likvärdiga krav på att kritiska entiteter ska vidta åtgärder för att stärka sin motståndskraft. Ett liknande undantag finns i NIS2-direktivet. En sektorsspecifik unionsrättsakt som pekas ut särskilt i båda direktiven är Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (Dora-förordningen). I CER-direktivet framhålls även att behörig myndighet för sektorerna bankverksamhet och finansmarknadsinfrastruktur i princip ska vara den behöriga myndigheten enligt Dora-förordningen. Utredaren behöver beakta dessa bestämmelser och relevanta sektorsspecifika unionsrättsakter när det gäller vilka krav som ska ställas på entiteterna, hur rollfördelningen mellan svenska myndigheter ska se ut och vilka befogenheter tillsynsmyndigheterna ska ha.

Av föregående avsnitt följer att utredaren ska analysera hur den nya regleringen ska fungera vid sidan av säkerhetsskyddsregleringen, i syfte att uppnå en mer sammanhållen systematik mellan regelverken. Utredaren behöver i sitt arbete beakta även annan relevant reglering. Utredaren ska särskilt överväga hur förslagen kan utformas på ett sätt som innebär att samordningsvinster i entiteternas säkerhetsarbete kan uppnås. Vidare ska utredaren analysera hur den terminologi som används i direktiven vid genomförandet kan anpassas till vedertagna begrepp i nationell reglering, såsom den nuvarande NIS-lagen och förordningen (2022:524) om statliga myndigheters beredskap.

Såväl NIS2-direktivet som CER-direktivet är så kallade minimidirektiv. Medlemsstaterna är oförhindrade att anta bestämmelser som säkerställer en högre cybersäkerhetsnivå eller en högre nivå av motståndskraft än vad som krävs enligt direktiven. Utredaren har därmed möjlighet att lämna förslag som exempelvis omfattar även andra sektorer och typer av entiteter än de som pekas ut i EU-direktiven, om det bedöms lämpligt för att uppnå en bättre sammanhållen reglering för samhällsviktig verksamhet. Utgångspunkten för utredarens arbete ska dock vara att förslagen utformas så att regelbördan och administrationen för berörda entiteter minimeras. Om förslag lämnas som går utöver EU-direktivens krav, ska utredaren särskilt motivera varför dessa är nödvändiga för att uppnå nationella svenska mål och göra en analys av om förslagen är samhällsekonomiskt effektiva och hur förslagen påverkar svenska företags konkurrenskraft. Vid utformningen av förslagen ska utredaren genomgående beakta vikten av kostnadseffektivitet.

Utredaren får även ta upp andra närliggande frågor i samband med de frågeställningar som ska utredas och lägga fram de förslag som behövs.

Utredaren ska därför

- beakta gränsdragningen mellan NIS2-direktivet och CER-direktivet samt relevanta sektorsspecifika unionsrättsakter vid utformningen av sina förslag,
- analysera hur samordningsvinster kan uppnås i entiteternas säkerhetsarbete enligt NIS2-direktivet, CER-direktivet och andra relevanta regelverk samt även i övrigt överväga hur förslagen kan utformas på ett sätt som är kostnadseffektivt och som inte är oproportionerligt administrativt betungande för berörda entiteter,
- överväga hur de olika kategorierna av aktörer ska benämnas i en kommande svensk lagstiftning och hur EU-direktivens terminologi i övrigt kan anpassas till vedertagna begrepp i relevant nationell reglering, och
- lämna förslag till nödvändiga författningsändringar.

Sekretess och dataskydd

Entiteter enligt såväl NIS2-direktivet som CER-direktivet kommer att vara skyldiga att rapportera incidenter. Incidentrapporterna kommer många gånger att innehålla känslig information, t.ex. om incidentens art, orsak och konsekvenser. Entiteterna kommer även vara skyldiga att till tillsynsmyndigheterna tillhandahålla information som är nödvändig för tillsynen, såsom uppgifter om säkerhets- och bevakningsåtgärder och resultat av genomförda säkerhetsrevisioner.

Såväl NIS2-direktivet som CER-direktivet ställer krav på att konfidentialitet för information som utbyts enligt direktiven bevaras. Det behöver mot denna bakgrund säkerställas att det finns ett tillräckligt skydd för uppgifter som ska rapporteras vid incidenter och tillhandahållas vid tillsyn. Av särskilt intresse i detta sammanhang är bestämmelsen i 18 kap. 8 § offentlighets- och sekretesslagen (2009:400), förkortad OSL, som reglerar sekretess för uppgifter som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärder inom vissa närmare angivna områden. Enligt den bestämmelsen gäller sekretess för en sådan uppgift om det kan antas att syftet med åtgärden motverkas om uppgiften röjs.

I samband med remitteringen av betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36) ansåg flera remissinstanser att det fanns behov av ett starkare sekretesskydd. Vissa av remissinstanserna framhöll att en för svag sekretess kan göra att aktörer väljer att inte rapportera incidenter eller att lämna knapphändig information i sina incidentrapporter. Vid genomförandet av NIS-direktivet bedömde regeringen att befintliga bestämmelser om sekretess erbjöd ett tillräckligt skydd (prop. 2017/18:205 s. 81 f.). Frågan behöver emellertid analyseras på nytt med beaktande av NIS2-direktivets och CER-direktivets krav på konfidentialitet. Det behöver bl.a. övervägas om sekretessen enligt 18 kap. 8 § OSL är tillräckligt stark. Särskilt med hänsyn till CER-direktivets tillämpningsområde behöver det även analyseras om de befintliga bestämmelserna i OSL är tillräckligt omfattande och täcker samtliga områden som omfattas av direktivet.

Utredaren behöver även analysera om befintliga bestämmelser i OSL tillgodoser NIS2-direktivets och CER-direktivets krav på utlämnande av uppgifter till andra medlemsstater samt till kommissio-

nen och Europeiska unionens cybersäkerhetsbyrå (Enisa). Detsamma gäller för kraven på skydd av uppgifter som har tagits emot.

Av NIS2-direktivet och CER-direktivet framgår att behandling av personuppgifter ska ske i enlighet med tillämpliga dataskyddsbestämmelser. Utredaren behöver analysera vilken personuppgiftsbehandling som direktiven kommer att ge upphov till och säkerställa att det finns stöd för sådan behandling.

Särskilda överväganden i fråga om såväl sekretess som dataskydd kan behöva göras när det gäller utformningen av systemet för bakgrundskontroller, inbegripet belastningsregisterkontroller, enligt CER-direktivet.

Utredaren ska därför

- ta ställning till om bestämmelserna i OSL innebär ett tillräckligt skydd för sådana uppgifter som kan komma att behandlas enligt direktiven,
- analysera vilken personuppgiftsbehandling som kan bli aktuell vid tillämpningen av direktivens bestämmelser, och
- vid behov lämna förslag till författningsändringar.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för företag eller andra enskilda samt konsekvenserna i övrigt av förslagen. Utredarens förslag ska utformas så att reglerna blir tydliga och ger så låga administrativa och andra kostnader som möjligt för entiteterna. I detta ingår att bedöma de ekonomiska konsekvenserna av förslagen för de behöriga myndigheterna. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. I 14 kap. 3 § regeringsformen anges att en inskränkning av den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till ändamålen. Det innebär att en proportionalitetsprövning ska göras under lagstiftningsprocessen. Om något av förslagen i betänkandet påverkar den kommunala självstyrelsen ska därför, utöver dess konsekvenser, också de särskilda avvägningar som lett fram till förslaget särskilt redovisas.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet, utredningsväsendet och EU.

Utredaren ska i den utsträckning det är lämpligt ha en dialog med berörda myndigheter och organisationer och företag.

Uppdraget ska redovisas senast den 23 februari 2024.

(Försvarsdepartementet)

Kommittédirektiv 2024:3

Tilläggsdirektiv till Utredningen om genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft (Fö 2023:01)

Beslut vid regeringssammanträde den 11 januari 2024

Förlängd tid för en del av uppdraget

Regeringen beslutade den 23 februari 2023 kommittédirektiv om genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, förkortat NIS2-direktivet och EU:s direktiv om kritiska entiteters motståndskraft, förkortat CER-direktivet (dir. 2023:30).

Enligt de ursprungliga direktiven ska uppdraget redovisas senast den 23 februari 2024. Utredningstiden ligger fast för de delar av uppdraget som avser att föreslå hur NIS2-direktivet ska genomföras och frågor som är gemensamma för NIS2- och CER-direktiven i de ursprungliga kommittédirektiven i den mån dessa är hänförliga till genomförandet av NIS2-direktivet. Utredningstiden ska dock förlängas för de delar av de ursprungliga direktiven som avser att

- föreslå hur CER-direktivet ska genomföras och frågor gemensamma för NIS2- och CER-direktiven i de ursprungliga kommittédirektiven i den mån dessa är hänförliga till genomförandet av CER-direktivet eller i övrigt syftar till att uppnå en sammanhängande reglering,

- analysera hur den nya regleringen ska fungera vid sidan av säkerhetsskyddsregleringen och föreslå ändringar som behövs för att uppnå en mer sammanhållen systematik mellan regelverken, särskilt vad gäller tillsynsmyndigheternas befogenheter och sanktionsavgifternas storlek,
- ta ställning till om bestämmelserna i offentlighets- och sekretesslagen (2009:400) innebär ett tillräckligt skydd för sådana uppgifter som kan komma att behandlas enligt direktiven, och
- i anslutning till dessa frågor lämna nödvändiga författningsförslag.

Uppdraget ska i dessa delar redovisas senast den 16 september 2024.

Utredaren har även fortsättningsvis möjlighet att ta upp andra frågor som har samband med de frågeställningar som ska hanteras inom ramen för utredningen under förutsättning att uppdraget ändå kan redovisas i tid.

(Försvarsdepartementet)

L 333/80 SV Europeiska unionens officiella tidning 27.12.2022

DIREKTIV

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555

av den 14 december 2022

om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska centralbankens yttrande ([1]),

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([2]),

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet ([3]), och

av följande skäl:

(1) Syftet med Europaparlamentets och rådets direktiv (EU) 2016/1148 ([4]) var att bygga upp cybersäkerhetskapaciteten i hela unionen, begränsa hoten mot nätverks- och informationssystem som används för att tillhandahålla samhällsviktiga tjänster i centrala sektorer och säkerställa kontinuiteten i sådana tjänster när de utsätts för incidenter, och därigenom bidra till unionens säkerhet och till att dess ekonomi och samhälle kan fungera effektivt.

(2) Sedan direktiv (EU) 2016/1148 trädde i kraft har betydande framsteg gjorts med att öka unionens nivå av cyberresiliens. Översynen av det direktivet har visat att det har fungerat som katalysator för den institutionella och lagstiftningsmässiga strategin för cybersäkerhet i unionen och har banat väg för en betydande attitydförändring. Direktivet har säkerställt fullbordandet av nationella ramar för säkerhet i nätverks- och informationssystem genom att fastställa nationella strategier för säkerhet i nätverks- och informationssystem och inrätta nationell kapacitet och genom att genomföra lagstiftningsåtgärder som omfattar väsentliga infrastrukturer och entiteter som identifierats av varje medlemsstat. Direktiv (EU) 2016/1148 har också bidragit till samarbete på unionsnivå genom inrättandet av samarbetsgruppen samt nätverket av nationella it-incidentcentrum. Trots dessa framsteg har översynen av direktiv (EU) 2016/1148 avslöjat inneboende brister som hindrar det från att effektivt hantera befintliga och framväxande utmaningar på cybersäkerhetsområdet.

(3) Nätverks- och informationssystem har utvecklats till ett centralt inslag i vardagslivet i och med den snabba digitala omställningen och sammankopplingen av samhället, vilket även gäller vid gränsöverskridande utbyten. Denna utveckling har lett till en utvidgad cyberhotbild, som medfört nya utmaningar som kräver anpassade, samordnade och innovativa svarsåtgärder i alla medlemsstater. Incidenter, som blir allt fler och mer omfattande, sofistikerade och vanliga och får allt större inverkan, utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Därför kan sådana incidenter hindra utövandet av ekonomisk verksamhet på den inre marknaden, generera

([1]) EUT C 233, 16.6.2022, s. 22.
([2]) EUT C 286, 16.7.2021, s. 170.
([3]) Europaparlamentets ståndpunkt av den 10 november 2022 (ännu inte offentliggjord i EUT) och rådets beslut av den 28 november 2022.
([4]) Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

ekonomisk förlust, undergräva användarnas förtroende och orsaka allvarlig skada för unionens ekonomi och samhälle. Beredskap och ändamålsenlighet på cybersäkerhetsområdet är därför nu viktigare än någonsin för att den inre marknaden ska fungera väl. Cybersäkerhet är dessutom en viktig förutsättning för att många kritiska sektorer ska kunna tillgodogöra sig den digitala omställningen och fullt ut utnyttja digitaliseringens ekonomiska, sociala och hållbarhetsmässiga fördelar.

(4) Den rättsliga grunden för direktiv (EU) 2016/1148 var artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), vars mål är att upprätta den inre marknaden och säkerställa dess funktion genom att förbättra åtgärderna för tillnärmning av nationella regler. De cybersäkerhetskrav som åläggs entiteter som tillhandahåller tjänster eller utför verksamhet som är ekonomiskt betydelsefull varierar avsevärt mellan medlemsstaterna vad gäller typen av krav, kravens utförlighet och tillsynsmetoden. Dessa skillnader medför extra kostnader och gör det svårt för entiteterna att erbjuda varor och tjänster över gränserna. Krav som ställs av en medlemsstat och som skiljer sig från, eller till och med står i strid med, krav som ställs av en annan medlemsstat kan väsentligt påverka sådan gränsöverskridande verksamhet. Det är dessutom sannolikt att otillräckligt utformade eller genomförda cybersäkerhetskrav i en medlemsstat kommer att få återverkningar för cybersäkerhetsnivån i andra medlemsstater, särskilt med tanke på det intensiva utbytet över gränserna. Översynen av direktiv (EU) 2016/1148 har visat på stora skillnader i medlemsstaternas genomförande, även vad gäller dess tillämpningsområde, då avgränsningen av detta i stor utsträckning har överlåtits på medlemsstaterna. Direktiv (EU) 2016/1148 gav också medlemsstaterna mycket stort utrymme för skönsmässig bedömning vad gäller genomförandet av de säkerhets- och incidentrapporteringsskyldigheter som fastställs i det. Dessa skyldigheter genomfördes därför på väsentligt skilda sätt på nationell nivå. Det finns liknande skillnader i genomförandet av bestämmelserna om tillsyn och efterlevnadskontroll i direktiv (EU) 2016/1148.

(5) Alla dessa skillnader medför en fragmentering av den inre marknaden och kan ha en skadlig inverkan på dess funktion, vilket påverkar i synnerhet tillhandahållandet av tjänster över gränserna och nivån av cyberresiliens till följd av tillämpningen av ett spektrum av åtgärder. Dessa skillnader kan till sist leda till att vissa medlemsstater har större sårbarhet för cyberhot, med potentiella spridningseffekter i hela unionen. Direktivets mål är att undanröja dessa stora skillnader mellan medlemsstaterna, särskilt genom att föreskriva minimiregler för ett fungerande samordnat regelverk genom att fastställa mekanismer för effektivt samarbete mellan de ansvariga myndigheterna i varje medlemsstat, genom att uppdatera förteckningen över sektorer och verksamheter som omfattas av skyldigheter vad gäller cybersäkerhet och genom att föreskriva effektiva rättsmedel och efterlevnadskontrollåtgärder, vilket är centralt för att upprätthålla en effektiv kontroll av att dessa skyldigheter efterlevs. Därför bör direktiv (EU) 2016/1148 upphävas och ersättas av det här direktivet.

(6) I och med upphävandet av direktiv (EU) 2016/1148 bör tillämpningsområdet med avseende på olika sektorer utvidgas till en större del av ekonomin så att den ger en omfattande täckning av sektorer och tjänster som är av avgörande betydelse för viktiga samhälleliga och ekonomiska verksamheter på den inre marknaden. I synnerhet syftar det här direktivet till att åtgärda bristerna i fråga om differentieringen mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, vilken har visat sig vara inaktuell eftersom den inte speglar den betydelse som dessa sektorer och tjänster har för samhälleliga och ekonomiska verksamheter på den inre marknaden.

(7) Enligt direktiv (EU) 2016/1148 hade medlemsstaterna ansvaret för att identifiera de entiteter som uppfyllde kriterierna för att klassificeras som leverantörer av samhällsviktiga tjänster. För att undanröja de stora skillnaderna mellan medlemsstaterna i detta avseende och säkerställa rättslig säkerhet vad gäller riskhanteringsåtgärderna för cybersäkerhet och rapporteringsskyldigheterna för alla relevanta entiteter, bör det fastställas ett enhetligt kriterium för vilka entiteter som ska omfattas av tillämpningsområdet för detta direktiv. Kriteriet bör bestå i tillämpningen av en storleksbaserad regel som innebär att alla entiteter som betraktas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG ([3]), eller överstiger de trösklar för medelstora företag som fastställs i punkt 1 i den artikeln, och som är verksamma i de sektorer och tillhandahåller de typer av tjänster eller

([3]) Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

bedriver de verksamheter som omfattas av det här direktivet också omfattas av tillämpningsområdet för det här direktivet. Medlemsstaterna bör även föreskriva att vissa små företag och mikroföretag, enligt definitionen i artikel 2.2 och 2.3 i den bilagan, som uppfyller specifika kriterier som visar deras nyckelroll för samhället, ekonomin eller för särskilda sektorer eller typer av tjänster ska omfattas av tillämpningsområdet för det här direktivet.

(8) Undantaget för offentliga förvaltningsentiteter från detta direktivs tillämpningsområde bör omfatta entiteter vars verksamhet till övervägande del bedrivs på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet verksamhet som rör utredning, förebyggande, upptäckt och lagföring av brott. Offentliga förvaltningsentiteter vars verksamhet endast marginellt hänför sig till dessa områden bör dock inte vara undantagna från direktivets tillämpningsområde. Vid tillämpningen av detta direktiv anses entiteter med tillsynsbefogenheter inte bedriva verksamhet på brottsbekämpningsområdet, och de är därför inte undantagna från tillämpningsområdet för detta direktiv. Offentliga förvaltningsentiteter som inrättats gemensamt med ett tredjeland i enlighet med ett internationellt avtal är undantagna från detta direktivs tillämpningsområde. Detta direktiv är inte tillämpligt på medlemsstaters diplomatiska och konsulära beskickningar i tredjeländer eller på deras nätverks- och informationssystem, såvida dessa system är belägna inom beskickningen eller drivs för användare i ett tredjeland.

(9) Medlemsstaterna bör kunna vidta de åtgärder som är nödvändiga för att skydda väsentliga nationella säkerhetsintressen, upprätthålla allmän ordning och säkerhet och möjliggöra förebyggande, utredning, upptäckt och lagföring av brott. I detta syfte bör medlemsstaterna kunna undanta särskilda entiteter som bedriver verksamhet på områdena, nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, från vissa skyldigheter i detta direktiv med avseende på sådan verksamhet. Om en entitet tillhandahåller tjänster uteslutande för en offentlig förvaltningsentitet som är undantagen från detta direktivs tillämpningsområde bör medlemsstaterna kunna undanta den entiteten från vissa skyldigheter enligt detta direktiv med avseende på dessa tjänster. Vidare bör ingen medlemsstat vara skyldig att lämna information vars avslöjande skulle strida mot dess väsentliga intressen i fråga om nationell säkerhet, allmän säkerhet eller försvar. Unionsregler eller nationella regler till skydd för säkerhetsskyddsklassificerade uppgifter, sekretessavtal samt informella sekretessavtal såsom Traffic Light Protocol bör beaktas i detta sammanhang. Traffic Light Protocol bör ses som ett medel för att informera om eventuella begränsningar i vidarespridningen av information. Det används inom nästan alla enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) och av vissa informations- och analyscentraler.

(10) Även om detta direktiv tillämpas på entiteter som bedriver verksamhet inom produktion av el från kärnkraftverk kan viss verksamhet vara kopplad till den nationella säkerheten. När så är fallet bör en medlemsstat kunna utöva sitt ansvar för att skydda den nationella säkerheten i samband med sådan verksamhet, inklusive verksamhet inom kärnenergins värdekedja, i enlighet med fördragen.

(11) Vissa entiteter bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, samtidigt som de även tillhandahåller betrodda tjänster. Tillhandahållare av betrodda tjänster som omfattas av Europaparlamentets och rådets förordning (EU) nr 910/2014 ([6]) bör omfattas av detta direktiv för att säkerställa samma nivå på säkerhetskraven och tillsynen som den som tidigare fastställdes i den förordningen vad gäller tillhandahållare av betrodda tjänster. I överensstämmelse med undantaget för vissa specifika tjänster från förordning (EU) nr 910/2014 bör detta direktiv inte vara tillämpligt på tillhandahållande av betrodda tjänster som på grund av nationell rätt eller avtal mellan en avgränsad grupp deltagare endast används inom slutna system.

([6]) Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

(12) Tillhandahållare av posttjänster enligt definitionen i Europaparlamentets och rådets direktiv 97/67/EG ([7]), inklusive tillhandahållare av budtjänster, bör omfattas av detta direktiv om de tillhandahåller minst ett led i postleveranskedjan, särskilt insamling, sortering, transport eller distribution av postförsändelser, inklusive upphämtning, samtidig som hänsyn tas till den grad i vilken de är beroende av nätverks- och informationssystem. Transporttjänster som inte utförs i samband med något av dessa led bör vara undantagna från tillämpningsområdet för posttjänster.

(13) Med tanke på att cyberhoten intensifieras och blir alltmer sofistikerade bör medlemsstaterna sträva efter att säkerställa att entiteter som är undantagna från detta direktivs tillämpningsområde uppnår en hög cybersäkerhetsnivå och stödja tillämpningen av likvärdiga riskhanteringsåtgärder för cybersäkerhet som speglar dessa entiteters känsliga natur.

(14) Unionens dataskyddslagstiftning och integritetslagstiftning är tillämplig på all behandling av personuppgifter inom ramen för detta direktiv. I synnerhet påverkar detta direktiv inte tillämpningen av Europaparlamentets och rådets förordning (EU) 2016/679 ([8]) och Europaparlamentets och rådets direktiv 2002/58/EG ([9]). Därför bör detta direktiv inte påverka exempelvis uppgifterna och befogenheterna för de myndigheter som är behöriga att övervaka efterlevnaden av unionens tillämpliga dataskyddslagstiftning och integritetslagstiftning.

(15) De entiteter som omfattas av tillämpningsområdet för detta direktiv med avseende på efterlevnad av riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter bör indelas i två kategorier, väsentliga entiteter och viktiga entiteter, vilket speglar i vilken mån de är av kritisk betydelse med avseende på sektor eller de typer av tjänster de tillhandahåller samt deras storlek. I detta avseende bör vederbörlig hänsyn i förekommande fall tas till eventuella relevanta sektorsspecifika riskbedömningar eller vägledning från de behöriga myndigheterna. Tillsyns- och efterlevnadskontrollsystemen för dessa båda kategorier av entiteter bör differentieras för att säkerställa en rättvis balans mellan riskbaserade krav och skyldigheter å ena sidan och den administrativa börda som följer av tillsynen av efterlevnaden å den andra.

(16) För att undvika att entiteter som har partnerföretag eller som är anknutna företag betraktas som väsentliga eller viktiga entiteter när detta vore oproportionellt kan medlemsstaterna ta hänsyn till vilken grad av oberoende som entiteten åtnjuter i förhållande till sin partner eller de anknutna företagen vid tillämpningen av artikel 6.2 i bilagan till rekommendation 2003/361/EG. I synnerhet kan medlemsstaterna ta hänsyn till att en entitet är oberoende av sin partner eller de anknutna företagen med avseende på de nätverks- och informationssystem som entiteten använder vid tillhandahållandet av sina tjänster och med avseende på de tjänster som entiteten tillhandahåller. På grundval av detta kan medlemsstaterna när det är lämpligt anse att en sådan entitet inte betraktas som ett medelstort företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG, eller inte överstiger de trösklar för ett medelstort företag som fastställs i punkt 1 i den artikeln, om entiteten, med hänsyn tagen till dess grad av oberoende, inte skulle ha ansetts betraktas som ett medelstort företag eller överstiga dessa trösklar om bara dess egna data hade tagits i beaktande. Detta påverkar inte skyldigheterna enligt detta direktiv för partnerföretag och anknutna företag som omfattas av direktivets tillämpningsområde.

(17) Medlemsstaterna bör kunna besluta att entiteter som före detta direktivs ikraftträdande har identifierats som leverantörer av samhällsviktiga tjänster i enlighet med direktiv (EU) 2016/1148 ska betraktas som väsentliga entiteter.

([7]) Europaparlamentets och rådets direktiv 97/67/EG av den 15 december 1997 om gemensamma regler för utvecklingen av gemenskapens inre marknad för posttjänster och för förbättring av kvaliteten på tjänsterna (EGT L 15, 21.1.1998, s. 14).

([8]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

([9]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

(18) För att skapa en tydlig överblick över entiteter som omfattas av detta direktivs tillämpningsområde bör medlemsstaterna upprätta en förteckning över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster. I detta syfte bör medlemsstaterna ålägga entiteter att till de behöriga myndigheterna lämna åtminstone följande information: namn, adress och aktuella kontaktuppgifter, inklusive entitetens e-postadresser, IP-adressintervall och telefonnummer, och i tillämpliga fall den relevanta sektor och delsektor som avses i de bilagorna samt i tillämpliga fall en förteckning över de medlemsstater där de tillhandahåller tjänster som omfattas av detta direktivs tillämpningsområde. I detta syfte bör kommissionen, med bistånd från Europeiska unionens cybersäkerhetsbyrå (Enisa), utan onödigt dröjsmål tillhandahålla riktlinjer och mallar avseende skyldigheten att lämna information. I syfte att underlätta upprättandet och uppdateringen av förteckningen över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster bör medlemsstaterna kunna fastställa nationella mekanismer för att entiteter ska kunna registrera sig själva. Om det finns register på nationell nivå kan medlemsstaterna besluta om lämpliga mekanismer som gör det möjligt att identifiera entiteter som omfattas av detta direktiv.

(19) Medlemsstaterna bör ansvara för att förse kommissionen åtminstone med uppgifter om antalet väsentliga och viktiga entiteter för varje sektor och delsektor enligt bilagorna samt relevant information om antalet identifierade entiteter och den bestämmelse i detta direktiv på vars grundval dessa identifierats, och den typ av tjänster de tillhandahåller. Medlemsstaterna uppmuntras att utbyta information med kommissionen om väsentliga och viktiga entiteter och, i händelse av en storskalig cybersäkerhetsincident, relevant information såsom den berörda entitetens namn.

(20) Kommissionen bör, i samarbete med samarbetsgruppen och efter samråd med relevanta intressenter, tillhandahålla riktlinjer om genomförandet av de kriterier som ska tillämpas på mikroföretag och små företag för att bedöma om de omfattas av detta direktiv. Kommissionen bör även säkerställa att mikroföretag och små företag som omfattas av detta direktiv får lämplig vägledning. Kommissionen bör, med bistånd från medlemsstaterna, göra information tillgänglig för mikroföretag och små företag i detta avseende.

(21) Kommissionen kan tillhandahålla vägledning för att bistå medlemsstaterna med att genomföra bestämmelserna i detta direktiv om tillämpningsområde och med att utvärdera proportionaliteten i de åtgärder som ska vidtas i enlighet med direktivet, särskilt vad gäller entiteter med komplexa affärsmodeller eller driftsmiljöer, varvid en entitet samtidigt kan uppfylla kriterierna för både väsentliga och viktiga entiteter eller samtidigt kan bedriva viss verksamhet som omfattas av, och viss verksamhet som är undantagen från, detta direktiv.

(22) I detta direktiv fastställs referensscenariot för riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter i alla sektorer som omfattas av dess tillämpningsområde. För att undvika fragmentering av cybersäkerhetsbestämmelserna i unionsrättsakter bör kommissionen, när ytterligare sektorsspecifika unionsrättsakter om riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter anses nödvändiga för att säkerställa en hög cybersäkerhetsnivå i hela unionen, bedöma om sådana ytterligare bestämmelser kan fastställas i en genomförandeakt inom ramen för detta direktiv. Om en sådan genomförandeakt inte är lämplig för detta ändamål skulle sektorsspecifika unionsrättsakter kunna bidra till att säkerställa en hög cybersäkerhetsnivå i hela unionen, samtidigt som de berörda sektorernas särdrag och komplexitet beaktas fullt ut. Därför hindrar detta direktiv inte antagandet av ytterligare sektorsspecifika unionsrättsakter innehållande riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som tar vederbörlig hänsyn till behovet av en övergripande och konsekvent cybersäkerhetsram. Detta direktiv påverkar inte de befintliga genomförandebefogenheter som har tilldelats kommissionen med avseende på ett antal sektorer, däribland transport och energi.

(23) Om en sektorsspecifik unionsrättsakt innehåller bestämmelser som föreskriver att väsentliga eller viktiga entiteter ska anta riskhanteringsåtgärder för cybersäkerhet eller anmäla betydande incidenter, och om dessa krav har minst samma verkan som de skyldigheter som fastställs i detta direktiv, bör de bestämmelserna, inbegripet om tillsyn och

efterlevnadskontroll, tillämpas på sådana entiteter. Om en sektorsspecifik unionsrättsakt inte omfattar alla entiteter inom en viss sektor som omfattas av detta direktivs tillämpningsområde bör de relevanta bestämmelserna i detta direktiv fortsätta att tillämpas på de entiteter som inte omfattas av den rättsakten.

(24) Om bestämmelserna i en sektorsspecifik unionsrättsakt föreskriver att väsentliga eller viktiga entiteter ska uppfylla rapporteringskrav som har minst samma verkan som rapporteringsskyldigheterna enligt detta direktiv bör samstämdhet och ändamålsenlighet säkerställas vid hanteringen av incidentanmälningar. I detta syfte bör den sektorsspecifika unionsrättsaktens bestämmelser om incidentanmälan föreskriva att CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna för cybersäkerhet (de gemensamma kontaktpunkterna) enligt detta direktiv ska ha omedelbar tillgång till de incidentanmälningar som lämnats in i enlighet med den sektorsspecifika unionsrättsakten. I synnerhet kan sådan omedelbar tillgång säkerställas om incidentanmälningar vidarebefordras utan onödigt dröjsmål till CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten enligt detta direktiv. När det är lämpligt bör medlemsstaterna införa en automatisk och direkt rapporteringsmekanism som säkerställer systematisk och omedelbar informationsdelning med CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna angående hanteringen av sådana incidentanmälningar. I syfte att förenkla rapporteringen och genomföra den automatiska och direkta rapporteringsmekanismen kan medlemsstaterna, i enlighet med den sektorsspecifika unionsrättsakten, använda en gemensam kontaktpunkt.

(25) Sektorsspecifika unionsrättsakter som föreskriver riskhanteringsåtgärder för cybersäkerhet eller rapporteringsskyldigheter som minst har samma verkan som de som fastställs i detta direktiv kan föreskriva att behöriga myndigheter inom ramen för de rättsakterna utövar sina tillsyns- och efterlevnadskontrollbefogenheter avseende sådana åtgärder eller skyldigheter med bistånd av de behöriga myndigheterna enligt detta direktiv. De berörda behöriga myndigheterna kan upprätta samarbetsarrangemang för detta ändamål. Sådana samarbetsarrangemang kan bland annat specificera förfarandena för samordning av tillsynsverksamheten, inbegripet förfarandena för utredningar och för inspektioner på plats i enlighet med nationell rätt och en mekanism för utbyte av relevant information om tillsyn och efterlevnadskontroll mellan de behöriga myndigheterna, inklusive tillgång till cyberrelaterad information som begärts av de behöriga myndigheterna enligt detta direktiv.

(26) Om sektorsspecifika unionsrättsakter innehåller skyldigheter eller incitament för entiteter att anmäla betydande cyberhot bör medlemsstaterna även uppmuntra till informationsdelning om betydande cyberhot med CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt detta direktiv för att öka dessa organs medvetenhet om cyberhotbilden och göra det möjligt för dem att reagera ändamålsenligt och i lämplig tid om de betydande cyberhoten skulle bli verklighet.

(27) Framtida sektorsspecifika unionsrättsakter bör ta vederbörlig hänsyn till de definitioner och den ram för tillsyn och efterlevnadskontroll som fastställs i detta direktiv.

(28) Europaparlamentets och rådets förordning (EU) 2022/2554 ([10]) bör betraktas som en sektorsspecifik unionsrättsakt vid tillämpning av detta direktiv med avseende på finansiella entiteter. Bestämmelserna i förordning (EU) 2022/2554 avseende riskhanteringsåtgärder för informations- och kommunikationsteknik (IKT), hantering av IKT-relaterade incidenter, särskilt rapportering om större IKT-relaterade incidenter, samt avseende testning av digital operativ motståndskraft, arrangemang för informationsutbyte och IKT-tredjepartsrisk bör tillämpas i stället för dem som fastställs i detta direktiv. Medlemsstaterna bör därför inte tillämpa detta direktivs bestämmelser om riskhanterings- och rapporteringsskyldigheter beträffande cybersäkerhet och om tillsyn och efterlevnadskontroll på finansiella entiteter som omfattas av förordning (EU) 2022/2554. Det är samtidigt viktigt att upprätthålla starka förbindelser och informationsutbyte med finanssektorn inom ramen för detta direktiv. Därför gör förordning (EU) 2022/2554 det möjligt för de europeiska tillsynsmyndigheterna och de behöriga myndigheterna enligt den förordningen att delta i samarbetsgruppens verksamhet och att utbyta information och samarbeta med de gemensamma kontaktpunkterna och med CSIRT-enheterna och de behöriga myndigheterna enligt detta direktiv. De behöriga myndigheterna enligt förordning (EU) 2022/2554[++] bör även översända uppgifter om större IKT-relaterade incidenter och, i förekommande fall, betydande cyberhot till CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt detta direktiv. Detta kan ske genom att ge omedelbar tillgång till incidentan-

([10]) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (se sidan 1 i detta nummer av EUT).

mälningar, och antingen vidarebefordra dem direkt eller genom en gemensam kontaktpunkt. Vidare bör medlemsstaterna fortsätta att inkludera finanssektorn i sina strategier för cybersäkerhet, och CSIRT-enheterna kan inbegripa finanssektorn i sin verksamhet.

(29) För att undvika luckor eller överlappning mellan de cybersäkerhetsskyldigheter som åläggs entiteter inom luftfartssektorn bör de nationella myndigheterna enligt Europaparlamentets och rådets förordningar (EG) nr 300/2008 ([11]) och (EU) 2018/1139 ([12]) och de behöriga myndigheterna enligt detta direktiv samarbeta när det gäller genomförandet av riskhanteringsåtgärder för cybersäkerhet och tillsynen av efterlevnaden av de åtgärderna på nationell nivå. En entitets efterlevnad av de säkerhetskrav som fastställs i förordningarna (EG) nr 300/2008 och (EU) 2018/1139 och i relevanta delegerade akter och genomförandeakter som antagits i enlighet med de förordningarna kan av de behöriga myndigheterna enligt detta direktiv anses utgöra efterlevnad av motsvarande krav som fastställs i detta direktiv.

(30) Med tanke på kopplingarna mellan cybersäkerhet och entiteters fysiska säkerhet bör man säkerställa samstämmighet mellan Europaparlamentets och rådets direktiv (EU) 2022/2557 ([13]) och det här direktivet. För att uppnå detta bör entiteter som identifieras som kritiska entiteter enligt direktiv (EU) 2022/2557 anses vara väsentliga entiteter enligt det här direktivet. Vidare bör varje medlemsstat säkerställa att dess nationella strategi för cybersäkerhet tillhandahåller en politisk ram för ökad samordning inom den medlemsstaten mellan dess behöriga myndigheter enligt detta direktiv och de behöriga myndigheterna enligt direktiv (EU) 2022/2557 när det gäller informationsutbyte om risker, cyberhot och incidenter, liksom om icke-cyberrelaterade risker, hot och incidenter, samt utövande av tillsynsuppgifter. De behöriga myndigheterna enligt det här direktivet och direktiv (EU) 2022/2557 bör samarbeta och utbyta information utan onödigt dröjsmål, särskilt när det gäller identifiering av kritiska entiteter, risker, cyberhot och incidenter samt när det gäller icke-cyberrelaterade risker, hot och incidenter som påverkar kritiska entiteter, inbegripet cybersäkerhetsåtgärder och fysiska åtgärder som vidtas av kritiska entiteter samt resultaten av den tillsynsverksamhet som bedrivs med avseende på sådana entiteter.

För att effektivisera tillsynsverksamheten mellan de behöriga myndigheterna enligt det här direktivet och direktiv (EU) 2022/2557 och för att minimera den administrativa bördan för de berörda entiteterna bör de behöriga myndigheterna dessutom sträva efter att harmonisera mallarna för incidentanmälningar och tillsynsförfaranden. När så är lämpligt bör behöriga myndigheter enligt direktiv (EU) 2022/2557 kunna begära att behöriga myndigheter enligt det här direktivet utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll gentemot en entitet som identifieras som en kritisk entitet enligt direktiv (EU) 2022/2557. Det här direktivet och direktiv (EU) 2022/2557 bör, om möjligt i realtid, samarbeta och utbyta information i detta syfte.

(31) Entiteter som tillhör sektorn för digital infrastruktur är i huvudsak baserade på nätverks- och informationssystem, och därför bör de skyldigheter som åläggs dessa entiteter genom det här direktivet på ett övergripande sätt omfatta den fysiska säkerheten i sådana system som en del av deras riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter. Eftersom dessa frågor omfattas av det här direktivet är de skyldigheter som fastställs i kapitlen III, IV och VI i direktiv (EU) 2022/2557 inte tillämpliga på sådana entiteter.

([11]) Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).

([12]) Europaparlamentets och rådets förordning (EU) 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91 (EUT L 212, 22.8.2018, s. 1).

([13]) Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (se sidan 164 i detta nummer av EUT).

(32) Att upprätthålla och bevara ett tillförlitligt, resilient och säkert domännamnssystem (DNS) är viktiga faktorer för att upprätthålla internets integritet och är avgörande för en kontinuerlig och stabil drift, vilket den digitala ekonomin och samhället är beroende av. Därför bör detta direktiv vara tillämpligt på registreringsenheter för toppdomäner och leverantörer av DNS-tjänster, som bör förstås som entiteter som tillhandahåller allmänt tillgängliga rekursiva tjänster för att lösa domännamnsfrågor för internetslutanvändare eller auktoritativa tjänster för att lösa domännamnsfrågor för tredjepartsanvändning. Detta direktiv bör inte vara tillämpligt på rotnamnsservrar.

(33) Molntjänster bör omfatta digitala tjänster som möjliggör administration av beställtjänster och bred fjärråtkomst till en skalbar och elastisk pool av delbara och distribuerade dataresurser, även när sådana resurser är distribuerade på flera platser. Beräkningsresurser omfattar resurser såsom nätverk, servrar eller annan infrastruktur, operativsystem, programvara, lagring, applikationer och tjänster. Tjänstemodellerna för molntjänster omfattar bland annat infrastruktur som en tjänst, plattform som en tjänst, program som en tjänst och nätverk som en tjänst. Distribueringsmodellerna för molntjänster bör omfatta privat moln, gemensamt moln, offentligt moln och hybridmoln. Molntjänste- och distribueringsmodellerna har samma innebörd som termerna tjänste- och distribueringsmodeller som definieras i standarden ISO/IEC 17788:2014. Molnanvändarens kapacitet att ensidigt, självständigt tillhandahålla datorkapacitet, såsom servertid eller nätlagring, utan någon mänsklig medverkan från leverantören av molntjänster, kan beskrivas som beställtjänster.

Termen *bred fjärråtkomst* används för att beskriva att molnkapaciteten tillhandahålls över nätet och nås genom mekanismer som främjar användning av heterogena tunna eller tjocka klientplattformar, däribland mobiltelefoner, surfplattor, bärbara datorer och arbetsstationer. Termen *skalbar* avser beräkningsresurser som leverantören av molntjänster fördelar på ett flexibelt sätt, oberoende av resursernas geografiska läge, för att hantera fluktuationer i efterfrågan. Termen *elastisk pool* används för att beskriva beräkningsresurser som tillhandahålls och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna utökas och minskas i takt med arbetsbördan. Termen *delbar* används för att beskriva beräkningsresurser som tillhandahålls flera användare som delar en gemensam åtkomst till tjänsten där behandlingen genomförs separat för varje användare, även om tjänsten tillhandahålls från samma elektroniska utrustning. Termen *distribuerad* används för att beskriva beräkningsresurser som finns på olika nätverksanslutna datorer eller enheter och som kommunicerar och samordnar sig sinsemellan genom meddelandepassning.

(34) Med tanke på framväxten av innovativ teknik och nya affärsmodeller förväntas nya molntjänste- och distribueringsmodeller uppstå på den inre marknaden som svar på kundernas föränderliga behov. I detta sammanhang kan molntjänster levereras i en mycket distribuerad form, ännu närmare den plats där data genereras eller samlas in, och därmed övergå från den traditionella modellen till en mycket distribuerad modell (*edge computing*).

(35) Tjänster som erbjuds av leverantörer av datacentraltjänster tillhandahålls inte alltid i form av molntjänster. Därför ingår inte datacentraler alltid i en molninfrastruktur. För att hantera alla risker för säkerheten i nätverks- och informationssystem bör detta direktiv därför omfatta leverantörer av datacentraltjänster som inte är molntjänster. Vid tillämpningen av detta direktiv bör termen *datacentraltjänst* omfatta strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och datatransporttjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll. Termen *datacentraltjänst* bör inte vara tillämplig på interna datacentraler som ägs och drivs av den berörda entiteten för egen räkning.

(36) Forskningsverksamhet spelar en nyckelroll i utvecklingen av nya produkter och processer. Mycket av den verksamheten genomförs av entiteter som delar, sprider eller utnyttjar resultaten av sin forskning i kommersiella syften. Dessa entiteter kan därför vara viktiga aktörer i värdekedjor, vilket gör säkerheten i deras nätverks- och informationssystem till en integrerad del av den övergripande cybersäkerheten på den inre marknaden. Forskningsorganisationer bör anses inbegripa entiteter som riktar in större delen av sin verksamhet på tillämpad forskning eller experimentell utveckling i den mening som avses i "Frascatimanualen 2015: Riktlinjer för insamling och

rapportering av uppgifter om forskning och experimentell utveckling” från Organisationen för ekonomiskt samarbete och utveckling, i syfte att utnyttja sina resultat i kommersiella syften, såsom tillverkning eller utveckling av en produkt eller process, tillhandahållande av en tjänst, eller marknadsföring därav.

(37) De växande ömsesidiga beroendeförhållandena är resultatet av ett allt mer gränsöverskridande nätverk av tillhandahållande av tjänster, med ett inbördes beroende, som använder central infrastruktur över hela unionen inom sektorer såsom energi, transport, digital infrastruktur, dricks- och avloppsvatten, hälso- och sjukvård, vissa aspekter av offentlig förvaltning, samt rymden i den mån tillhandahållandet av vissa tjänster som är beroende av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter berörs; därför omfattas inte infrastruktur som ägs, förvaltas eller drivs av unionen eller på unionens vägnar som en del av dess rymdprogram. Dessa beroendeförhållanden innebär att alla störningar, även sådana som inledningsvis är begränsade till en entitet eller sektor, kan få dominoeffekter i vidare bemärkelse, vilket kan leda till långtgående och långvariga effekter på tillhandahållandet av tjänster på hela den inre marknaden. De intensifierade cyberattackerna under covid-19-pandemin har visat sårbarheten hos alltmer av varandra beroende samhällena är för risker med låg sannolikhet.

(38) Mot bakgrund av skillnaderna i nationella förvaltningsstrukturer, och för att skydda befintliga sektorsspecifika arrangemang eller unionens tillsyns- och regleringsorgan, bör medlemsstaterna kunna utse eller inrätta en eller flera behöriga myndigheter med ansvar för cybersäkerhet och för tillsynsuppgifterna enligt detta direktiv.

(39) För att underlätta gränsöverskridande samarbete och kommunikation mellan myndigheter och för att göra det möjligt att genomföra detta direktiv på ett effektivt sätt måste varje medlemsstat utse en gemensam kontaktpunkt med ansvar för samordningen av frågor angående säkerhet i nätverks- och informationssystem och gränsöverskridande samarbete på unionsnivå.

(40) De gemensamma kontaktpunkterna bör säkerställa effektivt gränsöverskridande samarbete med relevanta myndigheter i en annan medlemsstat och, när det är lämpligt, med kommissionen och Enisa. De gemensamma kontaktpunkterna bör därför ges i uppgift att vidarebefordra underrättelser om betydande incidenter med gränsöverskridande verkningar till de gemensamma kontaktpunkterna i andra berörda medlemsstater på begäran av CSIRT-enheten eller den behöriga myndigheten. På nationell nivå bör de gemensamma kontaktpunkterna möjliggöra smidigt sektorsövergripande samarbete med andra behöriga myndigheter. De gemensamma kontaktpunkterna kan också vara mottagare av relevant information om incidenter rörande finansiella entiteter från de behöriga myndigheterna enligt förordning (EU) 2022/2554, som de bör kunna vidarebefordra till CSIRT-enheterna eller de behöriga myndigheterna enligt detta direktiv, beroende på vad som är lämpligt.

(41) Medlemsstaterna bör ha både den tekniska och organisatoriska kapacitet som krävs för att förebygga, upptäcka, vidta åtgärder mot och begränsa incidenter och risker. Medlemsstaterna bör därför inrätta eller utse en eller flera CSIRT-enheter enligt detta direktiv och säkerställa att de har tillräckligt med resurser och teknisk kapacitet. CSIRT-enheterna bör uppfylla kraven enligt detta direktiv i syfte att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå. Medlemsstaterna bör kunna utse befintliga incidenthanteringsorganisationer (Cert) till CSIRT-enheter. För att stärka förtroendeförhållandet mellan entiteterna och CSIRT-enheterna bör medlemsstaterna, när en CSIRT-enhet är en del av de behörig myndighet, kunna överväga funktionell åtskillnad mellan de operativa uppgifter som utförs av CSIRT-enheterna, särskilt när det gäller informationsutbyte och bistånd till entiteterna, och de behöriga myndigheternas tillsynsverksamhet.

(42) CSIRT-enheterna ansvarar för incidenthantering. Detta omfattar behandling av stora mängder ibland känsliga uppgifter. Medlemsstaterna bör säkerställa att CSIRT-enheterna har en infrastruktur för utbyte och behandling av information, samt väl rustad personal, som säkerställer verksamhetens konfidentialitet och trovärdighet. CSIRT-enheterna kan även anta uppförandekoder i detta avseende.

(43) Vad gäller personuppgifter bör CSIRT-enheterna, i enlighet med förordning (EU) 2016/679, på begäran av en väsentlig eller viktig entitet tillhandahålla en proaktiv skanning av de nätverks- och informationssystem som används för att tillhandahålla entitetens tjänster. När det är tillämpligt bör medlemsstaterna sträva efter att säkerställa en lika hög nivå av teknisk kapacitet hos alla sektorsspecifika CSIRT-enheter. Medlemsstaterna bör kunna begära Enisas bistånd vid inrättandet av sina CSIRT-enheter.

(44) CSIRT-enheter bör ha förmåga att, på en väsentlig eller viktig entitets begäran, övervaka entitetens internettillvända tillgångar, både inom och utanför lokalerna, för att identifiera, förstå och hantera entitetens övergripande organisatoriska risker med avseende på nyligen identifierade kompromisser i leveranskedjan eller kritiska sårbarheter. Entiteten bör uppmuntras att meddela CSIRT-enheten om den har ett privilegierat hanteringsgränssnitt, då detta kan påverka hur snabbt begränsningsåtgärder kan vidtas.

(45) Med tanke på vikten av internationellt samarbete på området cybersäkerhet bör CSIRT-enheterna kunna delta i internationella samarbetsnätverk utöver det CSIRT-nätverk som inrättas genom detta direktiv. För att utföra sina uppgifter bör CSIRT-enheterna och de behöriga myndigheterna därför kunna utbyta information, inklusive personuppgifter, med de nationella enheterna för hantering av it-säkerhetsincidenter eller behöriga myndigheter i tredjeländer, förutsatt att villkoren i unionens dataskyddslagstiftning för överföring av personuppgifter till tredjeländer är uppfyllda, bland annat villkoren i artikel 49 i förordning (EU) 2016/679.

(46) Det är angeläget att säkerställa tillräckliga resurser för att uppnå målen för detta direktiv och göra det möjligt för de behöriga myndigheterna och CSIRT-enheterna att utföra de uppgifter som fastställs i detta direktiv. Medlemsstaterna kan på nationell nivå införa en finansieringsmekanism för att täcka de nödvändiga utgifterna i samband med att offentliga entiteter med ansvar för cybersäkerheten i medlemsstaterna utför sina uppgifter i enlighet med detta direktiv. En sådan mekanism bör vara förenlig med unionsrätten samt proportionell och icke-diskriminerande och bör beakta olika tillvägagångssätt för att tillhandahålla säkra tjänster.

(47) CSIRT-nätverket bör fortsätta att bidra till att stärka förtroendet och tilliten och främja snabbt och effektivt operativt samarbete mellan medlemsstaterna. För att stärka det operativa samarbetet på unionsnivå bör CSIRT-nätverket överväga att bjuda in unionsorgan och -byråer som arbetar med frågor som rör cybersäkerhetspolitiken, såsom Europol, att delta i dess arbete.

(48) För att uppnå och behålla en hög cybersäkerhetsnivå bör de nationella strategier för cybersäkerhet som krävs enligt detta direktiv bestå av enhetliga ramar med strategiska mål och prioriteringar på cybersäkerhetsområdet samt en styrningsram för att uppnå dem. Dessa strategier kan bestå av ett eller flera instrument av lagstiftningskaraktär eller annan karaktär.

(49) Riktlinjer för cyberhygien utgör grunden för att skydda nätverks- och informationssystemens infrastruktur, maskinvara, programvara och säkerhet för onlinetillämpningar samt affärs- eller slutanvändardata som entiteter förlitar sig på. Riktlinjer för cyberhygien som omfattar en gemensam grundläggande uppsättning rutiner, bland annat uppdateringar av programvara och maskinvara, byte av lösenord, hantering av nya installationer, begränsning av användarkonton på administratörsnivå och säkerhetskopiering av data, möjliggör en proaktiv ram för beredskap samt övergripande säkerhet och trygghet i händelse av incidenter eller cyberhot. Enisa bör övervaka och analysera medlemsstaternas riktlinjer för cyberhygien.

(50) Medvetenhet om cybersäkerhet och cyberhygien är av väsentlig betydelse för att stärka cybersäkerheten inom unionen, särskilt mot bakgrund av det ökande antalet uppkopplade enheter som i tilltagande grad används vid cyberattacker. Ansträngningar bör göras för att öka den allmänna medvetenheten om risker kopplade till sådana enheter, samtidigt som bedömningar på unionsnivå kan bidra till att säkerställa samsyn i fråga om sådana risker på den inre marknaden.

(51) Medlemsstaterna bör uppmuntra användningen av all innovativ teknik, däribland artificiell intelligens, som kan förbättra upptäckten och förebyggandet av cyberattacker och göra det möjligt att styra över resurser till cyberattacker på ett effektivare sätt. Medlemsstaterna bör därför i sin nationella strategi för cybersäkerhet uppmuntra forsknings- och utvecklingsverksamhet för att underlätta användningen av sådan teknik, särskilt sådan som avser automatiserade eller halvautomatiserade cybersäkerhetsverktyg, och i förekommande fall utbyte av data som behövs för att utbilda användarna av sådan teknik och förbättra den. Användningen av innovativ teknik, däribland artificiell intelligens, bör vara förenlig med unionens dataskyddslagstiftning, däribland dataskyddsprinciperna om uppgifternas korrekthet, uppgiftsminimering, rättvisa och transparens samt datasäkerhet, såsom avancerad krypteringsteknik. Kraven på inbyggt dataskydd och dataskydd som standard enligt förordning (EU) 2016/679 bör utnyttjas till fullo.

(52) Cybersäkerhetsverktyg och applikationer med öppen källkod kan bidra till en högre grad av öppenhet och inverka positivt på effektiviteten i industriell innovation. Öppna standarder främjar interoperabilitet mellan säkerhetsverktyg, vilket gynnar säkerheten för berörda parter inom industrin. Cybersäkerhetsverktyg och applikationer med öppen källkod kan dra nytta av utvecklargemenskapen i stort och möjliggöra diversifiering av leverantörer. Öppen källkod kan leda till en mer transparent verifieringsprocess för cybersäkerhetsrelaterade verktyg och till en gemenskapsdriven process för att upptäcka sårbarheter. Medlemsstaterna bör därför kunna främja användningen av programvara med öppen källkod och öppna standarder genom att tillämpa riktlinjer för användning av öppna data och öppen källkod som ett led i säkerhet genom transparens. Riktlinjer som främjar införande och hållbar användning av cybersäkerhetsverktyg med öppen källkod är särskilt viktig för små och medelstora företag som har stora genomförandekostnader som kan minimeras om behovet av specifika applikationer eller verktyg minskades.

(53) Allmännyttiga tjänster är alltmer uppkopplade mot digitala nätverk i städer i syfte att förbättra städernas transportnät, uppgradera anläggningar för vattenförsörjning och avfallshantering och effektivisera belysning och uppvärmning i byggnader. Dessa digitaliserade allmännyttiga tjänster är sårbara för cyberattacker och riskerar i händelse av en lyckad cyberattack att vålla medborgarna omfattande skada på grund av att de är sammankopplade. Medlemsstaterna bör, som ett led i sin nationella strategi för cybersäkerhet, ta fram riktlinjer som hanterar utvecklingen av sådana sammankopplade eller smarta städer, och deras potentiella inverkan på samhället.

(54) På senare år har unionen upplevt en exponentiell ökning av attacker genom utpressningsprogram där sabotageprogram krypterar data och system och kräver en lösensumma för att låsa upp dem. Att attacker genom utpressningsprogram blir vanligare och allvarligare kan bero på flera faktorer, såsom olika attackmönster, kriminella affärsmodeller som kretsar kring ”utpressningsprogram som service” och kryptovalutor, krav på lösensumma och ökat antal attacker i leveranskedjan. Medlemsstaterna bör ta fram riktlinjer för att hantera det ökande antalet utpressningsattacker som ett led i sin nationella strategi för cybersäkerhet.

(55) Offentlig-privata partnerskap inom cybersäkerhet kan utgöra en lämplig ram för kunskapsutbyte, utbyte av bästa praxis och utveckling av samsyn bland berörda parter. Medlemsstaterna bör främja riktlinjer som stöder inrättande av cybersäkerhetsspecifika offentlig-privata partnerskap. Sådana riktlinjer bör bland annat klargöra tillämpningsområdet och de berörda aktörerna, styrningsmodellen, de tillgängliga finansieringsalternativen och samspelet mellan deltagande aktörer i samband med offentlig-privata partnerskap. Offentlig-privata partnerskap kan dra nytta av expertisen hos privata entiteter för att bistå behöriga myndigheter vid utvecklingen av avancerade tjänster och processer med informationsutbyte, tidiga varningar, cyberhots- och incidentövningar, krishantering och resiliensplanering.

(56) Medlemsstaterna bör i sina nationella strategier för cybersäkerhet ta itu med små och medelstora företags särskilda cybersäkerhetsbehov. Små och medelstora företag står, i hela unionen, för en stor andel av industri- och affärsmarknaden och har ofta svårt att anpassa sig till nya affärsmetoder i en mer uppkopplad värld, och till den digitala miljön, med anställda som arbetar hemifrån och en verksamhet som i allt högre grad bedrivs online. Vissa små och medelstora företag upplever särskilda cybersäkerhetsutmaningar, såsom låg cybermedvetenhet, bristande it-säkerhet på distans, höga kostnader för cybersäkerhetslösningar och en förhöjd hotnivå, t.ex. genom utpressningsprogram, och bör för detta få vägledning och bistånd. Små och medelstora företag blir i allt högre grad måltavlor för attacker i leveranskedjan på grund av att de har mindre strikta åtgärder för hantering av cybersäkerhetsrisker och attacker och på grund av det faktum att de har begränsade säkerhetsresurser. Sådana attacker i leveranskedjan påverkar inte bara små och medelstora företag och deras verksamhet isolerat utan kan också få en dominoeffekt i fråga om större attacker mot entiteter som de levererat till. Medlemsstaterna bör genom sina nationella strategier för cybersäkerhet hjälpa små och medelstora företag att ta itu med utmaningarna i sina

leveranskedjor. Medlemsstaterna bör ha en kontaktpunkt för små och medelstora företag på nationell eller regional nivå som antingen ger vägledning och bistånd till små och medelstora företag eller hänvisar dem till lämpliga organ för vägledning och bistånd i cybersäkerhetsrelaterade frågor. Medlemsstaterna uppmanas även att erbjuda tjänster såsom konfiguration av webbplatser och möjliggörande av loggning för mikroföretag och små företag som saknar sådan kapacitet.

(57) Inom ramen för sina nationella strategier för cybersäkerhet bör medlemsstaterna anta riktlinjer för främjande av ett aktivt cyberskydd som ett led i en vidare försvarsstrategi. I stället för reaktiva insatser innebär ett aktivt cyberskydd förebyggande, upptäckt, övervakning, analys och begränsning av överträdelser av nätverkssäkerheten, i kombination med användning av kapacitet som satts in inom och utanför det angripna nätverket. Detta kan bland annat innebära att medlemsstaterna erbjuder vissa entiteter kostnadsfria tjänster eller verktyg, t.ex. självbetjäningskontroller, upptäcktsverktyg och borttagningstjänster. Förmågan att snabbt och automatiskt utbyta och förstå information om och analyser av hot, varningar om cyberverksamhet samt motåtgärder är avgörande för att med förenade ansträngningar lyckas förebygga, upptäcka, hantera och blockera attacker mot nätverks- och informationssystem. Ett aktivt cyberskydd bygger på en defensiv strategi som utesluter offensiva åtgärder.

(58) Eftersom utnyttjandet av sårbarheter i nätverks- och informationssystem kan orsaka betydande störningar och skada, är snabb identifiering och snabbt åtgärdande av sådana sårbarheter en viktig faktor för att minska risken. Entiteter som utvecklar eller administrerar nätverks- och informationssystem bör därför inrätta lämpliga förfaranden för att hantera sårbarheter när de upptäcks. Eftersom sårbarheter ofta upptäcks och meddelas av tredjeparter, bör tillverkaren eller leverantören av IKT-produkter eller IKT-tjänster även införa nödvändiga förfaranden för att motta sårbarhetsinformation från tredjeparter. I detta avseende ger de internationella standarderna ISO/IEC 30111 och ISO/IEC 29147 vägledning om sårbarhetshantering och om delgivning av information om sårbarheter. En stärkt samordning mellan rapporterande fysiska och juridiska personer och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster är särskilt viktig för att underlätta den frivilliga ramen för delgivning av information om sårbarheter. Samordnad delgivning av information om sårbarheter specificerar en strukturerad process genom vilken sårbarheter rapporteras till tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna på ett sätt som gör det möjligt för denne att diagnostisera och åtgärda sårbarheten innan detaljerad information om sårbarheten meddelas tredjeparter eller allmänheten. Samordnad delgivning av information om sårbarheter bör även inbegripa samordning mellan den rapporterande fysiska eller juridiska personen och tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna vad gäller tidpunkten för åtgärdandet och offentliggörandet av sårbarheter.

(59) Kommissionen, Enisa och medlemsstaterna bör fortsätta att främja anpassningar till internationella standarder och befintlig bästa branschpraxis inom hantering av cybersäkerhetrisker, exempelvis inom säkerhetsbedömningar i leveranskedjan, informationsutbyte och delgivning av information om sårbarheter.

(60) Medlemsstaterna bör, i samarbete med Enisa, vidta åtgärder för att underlätta samordnad delgivning av information om sårbarheter genom att fastställa en relevant nationell policy. Som ett led i den nationella policyn bör medlemsstaterna sträva efter att i största möjliga utsträckning ta itu med de utmaningar som sårbarhetsforskare ställs inför, inbegripet deras potentiella utsatthet för straffrättsligt ansvar, i enlighet med nationell rätt. Med tanke på att fysiska och juridiska personer som forskar om sårbarheter kan riskera straff- och civilrättsligt ansvar i vissa medlemsstater uppmuntras medlemsstaterna att anta riktlinjer för icke-lagföring av forskare i informationssäkerhet och befrielse från civilrättsligt ansvar för deras verksamhet.

(61) Medlemsstaterna bör utse en av sina CSIRT-enheter till samordnare, som bör fungera som betrodd mellanhand mellan rapporterande fysiska eller juridiska personer och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster som sannolikt kommer att påverkas av sårbarheten, när detta är nödvändigt. Den CSIRT-enhet som utsetts till samordnare bör bland annat ha i uppgift att identifiera och kontakta de berörda entiteterna, bistå de fysiska eller juridiska personer som rapporterar en sårbarhet, förhandla om tidsfrister för delgivning av information och hantera

sårbarheter som påverkar flera entiteter (samordnad delgivning av information om sårbarheter omfattande flera parter). Om den rapporterade sårbarheten kan ha en betydande påverkan på entiteter i fler än en medlemsstat bör de CSIRT-enheter som utsetts till samordnare samarbeta inom CSIRT-nätverket när så är lämpligt.

(62) Tillträde till korrekt information i lämplig tid om sårbarheter som påverkar IKT-produkter och IKT-tjänster bidrar till en förbättrad riskhantering på cybersäkerhetsområdet. Källor till offentligt tillgänglig information om sårbarheter är ett viktigt verktyg för entiteterna och användarna av deras tjänster, men även för behöriga myndigheter och CSIRT-enheter. Av denna anledning bör Enisa upprätta en europeisk sårbarhetsdatabas där entiteter, oberoende av om de omfattas av tillämpningsområdet för detta direktiv, och deras leverantörer av nätverks- och informationssystem, samt de behöriga myndigheterna och CSIRT-enheterna på frivillig basis kan meddela information om och registrera allmänt kända sårbarheter för att möjliggöra för användarna att vidta lämpliga riskreducerande åtgärder. Syftet med databasen är att hantera de unika utmaningar som risker innebär för entiteter i unionen. Vidare bör Enisa inrätta ett lämpligt förfarande för offentliggörandet för att ge entiteterna tid att vidta riskreducerande åtgärder när det gäller deras sårbarheter och använda avancerade riskhanteringsåtgärder på cybersäkerhetsområdet samt maskinläsbara dataset och motsvarande gränssnitt. För att uppmuntra en kultur där information lämnas om sårbarheter bör informationslämnande inte få negativa effekter för den rapporterande fysiska eller juridiska personen.

(63) Även om liknande sårbarhetsregister eller -databaser finns, förvaltas och underhålls de av entiteter som inte är etablerade i unionen. En europeisk sårbarhetsdatabas som underhålls av Enisa skulle ge förbättrad insyn i processen för offentliggörande innan sårbarheten meddelas offentligt samt motståndskraft i händelse av en störning eller ett avbrott i tillhandahållandet av liknande tjänster. För att i möjligaste mån undvika dubbelarbete och eftersträva komplementaritet bör Enisa undersöka möjligheten att ingå avtal om strukturerat samarbete med liknande register eller databaser som omfattas av ett tredjelands jurisdiktion. Enisa bör särskilt undersöka möjligheten till ett nära samarbete med operatörerna av systemet för gemensamma sårbarheter och exponeringar (*Common Vulnerabilities and Exposures* – CVE).

(64) Samarbetsgruppen bör stödja och underlätta strategiskt samarbete och informationsutbyte samt stärka förtroendet och tilliten mellan medlemsstaterna. Samarbetsgruppen bör upprätta ett arbetsprogram vartannat år. Arbetsprogrammet bör omfatta de åtgärder som samarbetsgruppen ska vidta för att genomföra sina mål och uppgifter. Tidsramen för att inrätta det första arbetsprogrammet enligt detta direktiv bör anpassas till tidsramen för det senaste arbetsprogram som inrättats enligt direktiv (EU) 2016/1148 i syfte att undvika potentiella avbrott i samarbetsgruppens arbete.

(65) Vid utarbetandet av vägledningsdokument bör samarbetsgruppen konsekvent kartlägga nationella lösningar och erfarenheter, bedöma hur samarbetsgruppens resultat påverkar nationella strategier, diskutera utmaningar i samband med genomförandet och formulera särskilda rekommendationer, särskilt om hur ett samordnat införlivande av direktivet kan underlättas bland medlemsstaterna, som bör beaktas genom ett bättre genomförande av befintliga bestämmelser. Samarbetsgruppen skulle även kunna kartlägga de nationella lösningarna för att främja kompatibiliteten mellan de cybersäkerhetslösningar som tillämpas inom varje specifik sektor i unionen. Detta är särskilt relevant för sektorer av internationell eller gränsöverskridande karaktär.

(66) Samarbetsgruppen bör förbli ett flexibelt forum och kunna reagera på föränderliga och nya politiska prioriteringar och utmaningar samtidigt som tillgången till resurser beaktas. Den kan anordna regelbundna gemensamma möten med relevanta privata intressenter från hela unionen för att diskutera samarbetsgruppens verksamhet och inhämta uppgifter och synpunkter avseende framväxande politiska frågor. Dessutom bör samarbetsgruppen göra en regelbunden bedömning av läget när det gäller cyberhot eller incidenter, såsom utpressningsprogram. För att stärka

samarbetet på unionsnivå bör samarbetsgruppen överväga att bjuda in relevanta unionsinstitutioner, -organ, -kontor och -byråer som arbetar med frågor som rör cybersäkerhetspolitiken, såsom Europaparlamentet, Europol, Europeiska dataskyddsstyrelsen, Europeiska unionens byrå för luftfartssäkerhet, som inrättats genom förordning (EU) 2018/1139, och Europeiska unionens rymdprogrambyrå, som inrättats genom Europaparlamentets och rådets förordning (EU) 2021/696 ([14]), att delta i dess arbete.

(67) De behöriga myndigheterna och CSIRT-enheterna bör kunna delta i utbytesprogram för tjänstemän från andra medlemsstater inom en särskild ram och, i tillämpliga fall, efter det erforderliga säkerhetsgodkännandet för tjänstemän som deltar i sådana utbytesprogram, i syfte att förbättra samarbetet och stärka tilliten mellan medlemsstaterna. De behöriga myndigheterna bör vidta nödvändiga åtgärder för att tjänstemän från andra medlemsstater ska kunna spela en faktisk roll i verksamheten inom den behöriga värdmyndigheten eller CSIRT-värdenheten.

(68) Medlemsstaterna bör bidra till inrättandet av en EU-ram för hantering av cyberkriser enligt kommissionens rekommendation (EU) 2017/1584 ([15]) genom de befintliga samarbetsnätverken, särskilt Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), CSIRT-nätverket och samarbetsgruppen. EU- CyCLONe och CSIRT-nätverket bör samarbeta på grundval av förfaranden som specificerar detaljerna för detta samarbete och undvika dubbelarbete. Arbetsordningen för EU-CyCLONe bör ytterligare specificera de arrangemang enligt vilka det nätverket ska fungera, däribland nätverkets roller, samarbetsformer, samverkan med andra relevanta aktörer och mallar för informationsutbyte, samt kommunikationsmedel. För krishantering på unionsnivå bör berörda parter stödja sig på EU-arrangemangen för integrerad politisk krishantering enligt rådets genomförandebeslut (EU) 2018/1993 ([16]) (IPCR-arrangemang). Kommissionen bör använda Argus-förfarandet för gränsöverskridande krissamordning på hög nivå för detta ändamål. Om krisen har en yttre dimension eller en dimension som rör den gemensamma säkerhets- och försvarspolitiken (GSFP) och denna dimension är betydande, bör Europeiska utrikestjänstens krishanteringsmekanism aktiveras.

(69) I enlighet med bilagan till rekommendation (EU) 2017/1584 bör en storskalig incident anses vara en cybersäkerhetsincident som orsakar störningar som är så omfattande att en medlemsstat inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater. Beroende på orsak och verkan kan storskaliga cybersäkerhetsincidenter eskalera och förvandlas till fullt utvecklade kriser som hindrar den inre marknaden från att fungera korrekt eller som allvarligt hotar den allmänna tryggheten och säkerheten för entiteter eller medborgare i flera medlemsstater eller i unionen som helhet. Med beaktande av sådana incidenters stora omfattning och, i de flesta fall, gränsöverskridande karaktär, bör medlemsstater och relevanta unionsinstitutioner, -organ, -kontor och -byråer samarbeta på teknisk, operativ och politisk nivå i syfte att på lämpligt sätt samordna insatserna i hela unionen.

(70) Storskaliga cybersäkerhetsincidenter och kriser på unionsnivå kräver samordnade åtgärder för att säkerställa snabba och effektiva insatser på grund av den höga graden av ömsesidigt beroende mellan sektorer och medlemsstater. Tillgången till cyberresilienta nätverks- och informationssystem och uppgifternas tillgänglighet, konfidentialitet och riktighet är av vital betydelse för unionens säkerhet och skyddet av dess medborgare, företag och institutioner mot incidenter och cyberhot och för att stärka människors och organisationers tilltro till unionens förmåga att främja och skydda en global, öppen, fri, stabil och säker cyberrymd som bygger på mänskliga rättigheter, grundläggande friheter, demokrati och rättsstatliga principer.

([14]) Europaparlamentets och rådets förordning (EU) 2021/696 av den 28 april 2021 om inrättande av unionens rymdprogram och Europeiska unionens rymdprogrambyrå och om upphävande av förordningarna (EU) nr 912/2010, (EU) nr 1285/2013 och (EU) nr 377/2014 och beslut nr 541/2014/EU (EUT L 170, 12.5.2021, s. 69).

([15]) Kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (EUT L 239, 19.9.2017, s. 36).

([16]) Rådets genomförandebeslut (EU) 2018/1993 av den 11 december 2018 om EU-arrangemangen för integrerad politisk krishantering (EUT L 320, 17.12.2018, s. 28).

(71) EU-CyCLONe bör fungera som mellanhand mellan den tekniska och politiska nivån under storskaliga cybersäkerhetsincidenter och kriser och bör stärka samarbetet på operativ nivå och stödja beslutsfattandet på politisk nivå. I samarbete med kommissionen, och med beaktande av kommissionens behörighet inom krishantering, bör EU-CyCLONe ta fasta på CSIRT-nätverkets slutsatser och använda sin egen kapacitet för att göra en konsekvensanalys av storskaliga cybersäkerhetsincidenter och kriser.

(72) Cyberattacker är av en gränsöverskridande natur, och en betydande incident kan störa och skada kritisk informationsinfrastruktur som en välfungerande inre marknad är beroende av. Rekommendation (EU) 2017/1584 tar upp alla relevanta aktörers roller. Vidare är kommissionen inom ramen för unionens civilskyddsmekanism, som inrättats genom Europaparlamentets och rådets beslut nr 1313/2013/EU ([17]), ansvarig för allmänna beredskapsåtgärder, bland annat för att förvalta centrumet för samordning av katastrofberedskap och det gemensamma kommunikations- och informationssystemet för olyckor, upprätthålla och vidareutveckla situationsmedvetenhet och analyskapacitet samt upprätta och förvalta kapacitet att mobilisera och sända ut expertgrupper vid förfrågan om bistånd från en medlemsstat eller ett tredjeland. Kommissionen är även ansvarig för tillhandahållande av analytiska rapporter inför IPCR-arrangemang enligt genomförandebeslut (EU) 2018/1993, bland annat med avseende på situationsmedvetenhet och beredskap på cybersäkerhetsområdet, samt för situationsmedvetenhet och krishantering på områdena jordbruk, ogynnsamma väderförhållanden, kartläggning av och prognoser för konflikter, system för tidig varning vid naturkatastrofer, hälsokriser, övervakning av infektionssjukdomar, växtskydd, kemiska incidenter, livsmedels- och fodersäkerhet, djurhälsa, migration, tull, nukleära och radiologiska nödsituationer och energi.

(73) Unionen kan när det är lämpligt ingå internationella avtal, i enlighet med artikel 218 i EUF-fördraget, med tredjeländer eller internationella organisationer och därvid tillåta och organisera deras deltagande i särskild verksamhet inom samarbetsgruppen, CSIRT-nätverket och EU-CyCLONe. Sådana avtal bör säkerställa unionens intressen och ändamålsenligt skydd av uppgifter. Detta bör inte utesluta medlemsstaternas rätt att samarbeta med tredjeländer om hantering av sårbarheter och riskhantering på cybersäkerhetsområdet och därvid underlätta rapportering och allmänt informationsutbyte i enlighet med unionsrätten.

(74) För att underlätta ett effektivt genomförande av detta direktiv i fråga om bland annat hantering av sårbarheter, riskhanteringsåtgärder för cybersäkerhet, rapporteringsskyldigheter och arrangemang för informationsutbyte om cybersäkerhet kan medlemsstaterna samarbeta med tredjeländer och bedriva verksamhet som anses lämplig för detta ändamål, bland annat informationsutbyte om cyberhot, incidenter, sårbarheter, verktyg, metoder, taktik, tekniker och förfaranden, beredskap och övningar för cybersäkerhetskrishantering, utbildning, förtroendeskapande åtgärder och arrangemang för ett strukturerat informationsutbyte.

(75) Sakkunnigbedömningar bör införas i syfte att dra lärdom av delade erfarenheter, stärka det ömsesidiga förtroendet och uppnå en hög gemensam cybersäkerhetsnivå. Sakkunnigbedömningarna kan leda till värdefulla insikter och rekommendationer som kan stärka den övergripande cybersäkerhetskapaciteten, skapa ytterligare en funktionell väg för utbyte av bästa praxis mellan medlemsstater och bidra till att förbättra medlemsstaternas mognadsnivå inom cybersäkerhet. Vidare bör sakkunnigbedömningarna beakta resultaten av liknande mekanismer, såsom systemet för sakkunnigbedömning inom ramen för CSIRT-nätverket, samt tillföra mervärde och undvika dubbelarbete. Genomförandet av sakkunnigbedömningarna bör inte påverka tillämpningen av unionsrätt eller nationell rätt om skydd av konfidentiella eller säkerhetsskyddsklassificerade uppgifter.

(76) Samarbetsgruppen bör fastställa en självbedömningsmetod för medlemsstaterna för att täcka in faktorer såsom genomförandenivån för riskhanteringsåtgärderna för cybersäkerhet och rapporteringsskyldigheterna, kapacitetsnivån och effektiviteten i utförandet av de behöriga myndigheternas uppgifter, CSIRT-enheternas operativa kapacitet, genomförandenivån för det ömsesidiga biståndet, genomförandenivån för arrangemangen för informationsutbyte om cybersäkerhet eller särskilda frågor av gränsöverskridande eller sektorsövergripande karaktär. Medlemsstaterna bör uppmuntras att regelbundet genomföra självbedömningar och att presentera och diskutera resultaten av sina självbedömningar i samarbetsgruppen.

([17]) Europaparlamentets och rådets beslut nr 1313/2013/EU av den 17 december 2013 om en civilskyddsmekanism för unionen (EUT L 347, 20.12.2013, s. 924).

(77) Ansvaret för att säkerställa säkerheten i nätverks- och informationssystemen vilar i hög grad på väsentliga och viktiga entiteter. En riskhanteringskultur som inbegriper riskbedömningar och genomförande av riskhanteringsåtgärder för cybersäkerhet som är anpassade till riskerna bör främjas och utvecklas.

(78) Riskhanteringsåtgärder för cybersäkerhet bör ta hänsyn till i vilken grad den väsentliga eller viktiga entiteten är beroende av nätverks- och informationssystem och omfatta åtgärder för att identifiera eventuella incidentrisker, för att förebygga, upptäcka, hantera och återhämta sig från incidenter och för att begränsa deras inverkan. Säkerheten i nätverks- och informationssystem bör omfatta lagrade, överförda och behandlade uppgifters säkerhet. Riskhanteringsåtgärder för cybersäkerhet bör föreskriva systemanalys, med beaktande av den mänskliga faktorn, för att få en fullständig bild av nätverks- och informationssystemets säkerhet.

(79) Eftersom hot mot säkerheten i nätverks- och informationssystem kan ha olika ursprung bör riskhanteringsåtgärder för cybersäkerhet bygga på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö mot händelser såsom stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysisk åtkomst till och skada eller störning på en väsentlig eller viktig entitets information och informationsbehandlingsresurser, som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem. Riskhanteringsåtgärderna för cybersäkerhet bör därför också omfatta den fysiska säkerheten och miljösäkerheten i nätverks- och informationssystem genom att inbegripa åtgärder för att skydda sådana system mot systemfel, mänskliga misstag, avsiktligt skadliga handlingar eller naturfenomen i överensstämmelse med europeiska och internationella standarder, såsom de som ingår i ISO/IEC 27000-serien. I detta avseende bör väsentliga och viktiga entiteter som ett led i sina riskhanteringsåtgärder för cybersäkerhet också ägna sig åt personalsäkerhet och inrätta lämpliga strategier för åtkomstkontroll. Dessa åtgärder bör vara förenliga med direktiv (EU) 2022/2557.

(80) För att påvisa efterlevnaden av riskhanteringsåtgärder för cybersäkerhet, och i frånvaro av lämpliga europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881 ([18]), bör medlemsstaterna efter samråd med samarbetsgruppen och den europeiska gruppen för cybersäkerhetscertifiering främja användningen av relevanta europeiska och internationella standarder bland väsentliga och viktiga entiteter, eller så får de ålägga entiteter att använda certifierade IKT-produkter, IKT-tjänster och IKT-processer.

(81) För att undvika oproportionella finansiella och administrativa bördor för väsentliga och viktiga entiteter bör riskhanteringsåtgärderna för cybersäkerhet stå i proportion till riskerna för det berörda nätverks- och informationssystemet, med beaktande av teknikens ståndpunkt i fråga om sådana åtgärder, och i förekommande fall relevanta europeiska och internationella standarder, samt kostnaden för deras genomförande.

(82) Riskhanteringsåtgärder för cybersäkerhet bör stå i proportion till den väsentliga eller viktiga entitetens grad av exponering för risker och samhälleliga och ekonomiska konsekvenser som en incident skulle få. Vid fastställandet av riskhanteringsåtgärder för cybersäkerhet som är anpassade till väsentliga och viktiga entiteter bör vederbörlig hänsyn tas till väsentliga och viktiga entiteters olika riskexponering, t.ex. hur kritisk entiteten är, vilka risker, inklusive samhällsrisker, som den är exponerad för, hur stor entiteten är, hur sannolikt det är med incidenter och hur allvarliga de är, inklusive deras samhälleliga och ekonomiska konsekvenser.

([18]) Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

(83) Väsentliga och viktiga entiteter bör säkerställa säkerheten i de nätverks- och informationssystem som de använder i sin verksamhet. Det rör sig framför allt om privata nätverks- och informationssystem som antingen förvaltas av de väsentliga och viktiga entiteternas interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. De riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som fastställs i detta direktiv bör tillämpas på de relevanta väsentliga och viktiga entiteterna oavsett om dessa entiteter underhåller sina nätverks- och informationssystem internt eller lägger ut underhållet på entreprenad.

(84) Med beaktande av deras gränsöverskridande karaktär bör leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster samt tillhandahållare av betrodda tjänster omfattas av en hög nivå av harmonisering på unionsnivå. Genomförandet av riskhanteringsåtgärder för cybersäkerhet vad gäller dessa entiteter bör därför underlättas genom en genomförandeakt.

(85) Det är särskilt viktigt att hantera risker som härrör från en entitets leveranskedja och dess förhållande till sina leverantörer, såsom leverantörer av datalagrings- och databehandlingstjänster eller leverantörer av hanterade säkerhetstjänster och programredigerare, med tanke på förekomsten av incidenter där entiteter har varit föremål för cyberattacker och där inkräktare med avsikt att vålla skada har kunnat äventyra säkerheten i en entitets nätverks- och informationssystem genom att utnyttja sårbarheter som påverkar tredje parts produkter och tjänster. Väsentliga och viktiga entiteter bör därför bedöma och beakta den övergripande kvaliteten och resiliensen hos produkter och tjänster och de riskhanteringsåtgärder för cybersäkerhet som är inbyggda i dem samt cybersäkerhetspraxis hos sina leverantörer och tjänsteleverantörer, inbegripet deras förfaranden för säker utveckling. Väsentliga och viktiga entiteter bör framför allt uppmuntras att införliva riskhanteringsåtgärder för cybersäkerhet i avtal med sina direkta leverantörer och tjänsteleverantörer. Dessa entiteter kan beakta risker som härrör från leverantörer och tjänsteleverantörer på andra nivåer.

(86) Bland tjänsteleverantörerna har leverantörer av hanterade säkerhetstjänster på områden som incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster en särskilt viktig roll när det gäller att bistå entiteter i deras arbete med att förebygga, upptäcka, reagera på eller återhämta sig från incidenter. Leverantörer av hanterade säkerhetstjänster har dock också själva varit mål för cyberattacker, och eftersom de är nära integrerade i entiteternas verksamhet utgör de en särskild risk. Väsentliga och viktiga entiteter bör därför visa större noggrannhet vid valet av en leverantör av hanterade säkerhetstjänster.

(87) De behöriga myndigheterna kan också inom ramen för sina tillsynsuppgifter dra nytta av cybersäkerhetstjänster såsom säkerhetsrevisioner, penetrationstester eller incidenthantering.

(88) Väsentliga och viktiga entiteter bör också hantera risker som härrör från deras samverkan och förbindelser med andra intressenter inom ett vidare ekosystem, bland annat med avseende på att motverka industrispionage och skydda företagshemligheter. I synnerhet bör dessa entiteter vidta lämpliga åtgärder för att säkerställa att deras samarbete med akademiska institutioner och forskningsinstitut sker i linje med deras cybersäkerhetstrategier och följer god praxis när det gäller säker tillgång till och spridning av information i allmänhet och skydd av immateriella rättigheter i synnerhet. Likaså bör de väsentliga och viktiga entiteterna, med tanke på hur viktiga och värdefulla data är för deras verksamhet, vidta alla lämpliga riskhanteringsåtgärder för cybersäkerhet när de förlitar sig på dataomvandlings- och dataanalystjänster från tredje parter.

(89) Väsentliga och viktiga entiteter bör anta ett brett spektrum av grundläggande cyberhygienrutiner, såsom nollförtroende-principer, programuppdateringar, enhetskonfiguration, nätverkssegmentering, identitets- och åtkomsthantering eller användarmedvetenhet, anordna utbildning för sin personal och öka medvetenheten om cyberhot, nätfiske eller sociala manipuleringstekniker. Vidare bör dessa entiteter utvärdera sin egen cybersäkerhetskapacitet och när det är lämpligt fortsätta att integrera teknik för ökad cybersäkerhet, såsom artificiell intelligens eller maskininlärningssystem, för att förbättra sin kapacitet och säkerheten i nätverks- och informationssystemen.

(90) För att ytterligare hantera centrala risker i leveranskedjan och bistå väsentliga och viktiga entiteter som är verksamma i sektorer som omfattas av detta direktiv att på lämpligt sätt hantera risker i leveranskedjan och leverantörsrelaterade risker bör samarbetsgruppen, i samarbete med kommissionen och Enisa, och när så är lämpligt efter samråd med relevanta intressenter, även från industrin, utföra samordnade säkerhetsriskbedömningar av kritiska leveranskedjor, vilket redan gjorts för 5G-nät efter kommissionens rekommendation (EU) 2019/534 ([19]), i syfte att per sektor identifiera kritiska IKT-tjänster, IKT-system eller IKT-produkter, relevanta hot och sårbarheter. Sådana samordnade säkerhetsriskbedömningar bör fastställa åtgärder, riskreduceringsplaner och bästa praxis för att motverka kritiska beroenden, potentiella felkritiska systemdelar, hot, sårbarheter och andra risker kopplade till leveranskedjan och bör undersöka olika sätt att ytterligare uppmuntra en bredare användning av dessa från väsentliga och viktiga entiteters sida. Potentiella icke-tekniska riskfaktorer, såsom otillbörlig påverkan från ett tredjeland på leverantörer och tjänsteleverantörer, särskilt i samband med alternativa styrningsmodeller, inbegriper dolda sårbarheter eller bakdörrar och potentiella systemiska leveransstörningar, särskilt i samband med teknikinlåsning eller leverantörsberoende.

(91) De samordnade säkerhetsriskbedömningarna av kritiska leveranskedjor bör, mot bakgrund av den berörda sektorns särdrag, ta hänsyn till både tekniska och när så är lämpligt icke-tekniska faktorer, inbegripet de som anges i rekommendation (EU) 2019/534, i EU:s samordnade riskbedömning av cybersäkerheten för 5G-nät och i EU:s verktygslåda för 5G-cybersäkerhet som samarbetsgruppen enats om. För att identifiera de leveranskedjor som bör bli föremål för en samordnad säkerhetsriskbedömning bör följande kriterier beaktas: i) i vilken utsträckning väsentliga och viktiga entiteter använder och förlitar sig på specifika kritiska IKT-tjänster, IKT-system eller IKT-produkter, ii) specifika kritiska IKT-tjänsters, IKT-systems eller IKT-produkters relevans för att utföra kritiska eller känsliga funktioner, inbegripet behandling av personuppgifter, iii) tillgången till alternativa IKT-tjänster, IKT-system eller IKT-produkter, iv) motståndskraften i hela leveranskedjan för IKT-tjänster, IKT-system eller IKT-produkter under deras livscykel mot störningar, och v) för framväxande IKT-tjänster, IKT-system eller IKT-produkter, deras potentiella framtida betydelse för entiteternas verksamhet. Vidare bör särskild tonvikt läggas vid IKT-tjänster, IKT-system eller IKT-produkter som omfattas av särskilda krav som härrör från tredjeländer.

(92) För att rationalisera de skyldigheter som åläggs tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, och tillhandahållare av betrodda tjänster, med anknytning till säkerheten i deras nätverks- och informationssystem, samt för att göra det möjligt för dessa entiteter och de behöriga myndigheterna enligt Europaparlamentets och rådets direktiv (EU) 2018/1972 ([20]) respektive förordning (EU) nr 910/2014 att dra nytta av den rättsliga ram som inrättas genom detta direktiv, inbegripet utnämning av en CSIRT-enhet med ansvar för risk- och incidenthantering och deltagande av berörda behöriga myndigheter i samarbetsgruppens och CSIRT-nätverkets verksamhet, bör dessa entiteter omfattas av tillämpningsområdet för detta direktiv. De motsvarande bestämmelser som anges i förordning (EU) nr 910/2014 och i direktiv (EU) 2018/1972och som gäller införande av säkerhets- och anmälningskrav för dessa typer av entiteter bör därför utgå. De regler om rapporteringsskyldigheter som fastställs i det här direktivet bör inte påverka tillämpningen av förordning (EU) 2016/679 och direktiv 2002/58/EG.

(93) De cybersäkerhetsskyldigheter som fastställs i detta direktiv bör anses komplettera de krav som åläggs tillhandahållare av betrodda tjänster enligt förordning (EU) nr 910/2014. Tillhandahållare av betrodda tjänster bör vara skyldiga att vidta alla lämpliga och proportionella åtgärder för att hantera riskerna för sina tjänster, även med avseende på kunder och tredje parter som förlitar sig på dessa tjänster, och att rapportera incidenter enligt detta direktiv. Sådana cybersäkerhets- och rapporteringsskyldigheter bör även avse det fysiska skyddet av de tjänster som tillhandahålls. De krav för kvalificerade tillhandahållare av betrodda tjänster som fastställs i artikel 24 i förordning (EU) nr 910/2014 bör fortsätta att vara tillämpliga.

([19]) Kommissionens rekommendation (EU) 2019/534 av den 26 mars 2019 om it-säkerhet i 5G-nät (EUT L 88, 29.3.2019, s. 42).

([20]) Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (EUT L 321, 17.12.2018, s. 36).

(94) Medlemsstaterna kan utse tillsynsorganen enligt förordning (EU) nr 910/2014 till behöriga myndigheter för betrodda tjänster för att säkerställa att nuvarande praxis upprätthålls och för att ta fasta på den kunskap och erfarenhet som förvärvats genom tillämpningen av den förordningen. I detta fall bör de behöriga myndigheterna enligt detta direktiv samarbeta nära och i lämplig tid med dessa tillsynsorgan genom att utbyta relevant information i syfte att säkerställa att tillsynen är effektiv och att tillhandahållare av betrodda tjänster uppfyller kraven i detta direktiv och i förordning (EU) nr 910/2014. I förekommande fall bör CSIRT-enheten eller den behöriga myndigheten enligt detta direktiv omedelbart informera tillsynsorganet enligt förordning (EU) nr 910/2014 om eventuella betydande cyberhot eller incidenter som anmälts och som påverkar betrodda tjänster samt ifall en tillhandahållare av betrodda tjänster bryter mot detta direktiv. Medlemsstaterna kan för rapporteringsändamål i förekommande fall använda den gemensamma kontaktpunkt som inrättats för att uppnå en gemensam och automatisk rapportering av incidenter till både tillsynsorganet enligt förordning (EU) nr 910/2014 och CSIRT-enheten eller den behöriga myndigheten enligt detta direktiv.

(95) När så är lämpligt och för att undvika onödiga störningar bör befintliga nationella riktlinjer som antagits för att införliva bestämmelserna om säkerhetsåtgärder i artiklarna 40 och 41 i direktiv (EU) 2018/1972 beaktas vid införlivandet av det här direktivet för att ta fasta på den kunskap och kompetens som redan förvärvats inom ramen för direktiv (EU) 2018/1972 avseende säkerhetsåtgärder och incidentunderrättelser. Enisa kan också ta fram vägledning om säkerhetskrav och rapporteringsskyldigheter för tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster för att underlätta harmonisering och övergång och minimera störningar. Medlemsstaterna kan utse de nationella regleringsmyndigheterna till behöriga myndigheter för elektronisk kommunikation enligt direktiv (EU) 2018/1972 för att säkerställa att nuvarande praxis upprätthålls och för att ta fasta på den kunskap och erfarenhet som förvärvats som en följd av genomförandet av det direktivet.

(96) Mot bakgrund av den ökande betydelsen av nummeroberoende interpersonella kommunikationstjänster enligt definitionen i direktiv (EU) 2018/1972 är det nödvändigt att säkerställa att sådana tjänster också omfattas av lämpliga säkerhetskrav med tanke på deras särskilda karaktär och ekonomiska betydelse. I takt med att attackytan fortsätter att växa blir nummeroberoende interpersonella kommunikationstjänster, såsom meddelandetjänster, utbredda attackvektorer. Inkräktare med uppsåt att vålla skada använder plattformar för att kommunicera och locka offer att öppna komprometterade webbsidor, vilket ökar sannolikheten för incidenter som involverar utnyttjande av personuppgifter och i förlängningen säkerhet i nätverks- och informationssystemen. Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster bör säkerställa en säkerhetsnivå i nätverks- och informationssystemen som är lämplig i förhållande till de föreliggande riskerna. Eftersom tillhandahållare av nummeroberoende interpersonella kommunikationstjänster i allmänhet inte utövar faktisk kontroll över överföringen av signaler via nät kan graden av risk för sådana tjänster i vissa avseenden anses lägre än för traditionella elektroniska kommunikationstjänster. Detsamma gäller för interpersonella kommunikationstjänster enligt definitionen i direktiv (EU) 2018/1972 som använder nummer och som inte utövar faktisk kontroll över signalöverföringen.

(97) Den inre marknaden är mer beroende av ett fungerande internet än någonsin. Tjänster från nästan alla väsentliga och viktiga entiteter är beroende av tjänster som tillhandahålls via internet. För att säkerställa ett smidigt tillhandahållande av tjänster som levereras av väsentliga och viktiga entiteter är det viktigt att alla tillhandahållare av allmänna elektroniska kommunikationsnät har infört lämpliga riskhanteringsåtgärder för cybersäkerhet och rapporterar betydande incidenter i samband med dessa. Medlemsstaterna bör säkerställa att säkerheten i de allmänna elektroniska kommunikationsnäten upprätthålls och att deras vitala säkerhetsintressen skyddas mot sabotage och spionage. Eftersom internationell konnektivitet förstärker och påskyndar en konkurrenskraftig digitalisering av unionen och dess ekonomi bör incidenter som påverkar undervattenskablar rapporteras till CSIRT-enheten eller i förekommande fall den behöriga myndigheten. Den nationella strategin för cybersäkerhet bör när så är relevant beakta cybersäkerheten för undervattenskablar och inbegripa kartläggning av potentiella cybersäkerhetsrisker och riskreduceringsåtgärder för att säkerställa högsta skyddsnivå för dem.

(98) För att trygga säkerheten för allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster bör användningen av krypteringsteknik främjas, särskilt totalsträckskryptering samt datacentrerade säkerhetskoncept, såsom kartografi, segmentering, taggning, åtkomstpolicy och åtkomsthantering samt automatiserade beslut om åtkomst. Vid behov bör användningen av kryptering, särskilt totalsträckskryptering, vara obligatorisk för tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster i enlighet med principerna om automatisk och inbyggd säkerhet och automatiskt och inbyggt integritetsskydd vid tillämpningen av detta direktiv. Användningen av totalsträckskryptering bör förenas med medlemsstaternas befogenheter att säkerställa skyddet av sina väsentliga säkerhetsintressen och sin allmänna säkerhet och att möjliggöra förebyggande, utredning, upptäckt och lagföring av brott i enlighet med unionsrätten. Detta bör dock inte försvaga totalsträckskrypteringen, som är en kritisk teknik för ett effektivt dataskydd, integritet och kommunikationssäkerhet.

(99) I syfte att trygga säkerheten för, och förebygga missbruk och manipulering av, allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster bör användningen av säkra dirigeringsstandarder främjas för att säkerställa dirigeringsfunktionernas integritet och robusthet längs hela ekosystemet av internetåtkomstleverantörer.

(100) I syfte att skydda internets funktion och integritet och främja domännamnssystemets säkerhet och resiliens bör relevanta intressenter, däribland privata unionsentiteter, tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, särskilt internetåtkomstleverantörer, och leverantörer av sökmotorer uppmuntras att anta en strategi för diversifiering av DNS-uppslagning. Vidare bör medlemsstaterna uppmuntra utvecklingen och användningen av en allmän och säker europeisk DNS-resolvertjänst.

(101) I detta direktiv fastställs en flerstegsstrategi för rapportering av betydande incidenter för att hitta rätt balans mellan, å ena sidan, snabb rapportering som bidrar till att begränsa den potentiella spridningen av betydande incidenter och gör det möjligt för väsentliga och viktiga entiteter att söka bistånd och, å andra sidan, ingående rapportering som drar värdefulla lärdomar av enskilda incidenter och med tiden förbättrar cyberresiliensen hos enskilda entiteter och hela sektorer. I detta avseende bör detta direktiv omfatta rapportering av incidenter som, baserat på en första bedömning som utförts av den berörda entiteten, kan orsaka allvarliga störningar i tjänsterna eller ekonomiska förluster för den berörda entiteten eller påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada. En sådan inledande bedömning bör bland annat ta hänsyn till de drabbade nätverks- och informationssystemen, särskilt deras betydelse för tillhandahållandet av entitetens tjänster, allvaret i och de tekniska egenskaperna hos cyberhotet och eventuella underliggande sårbarheter som utnyttjas, samt entitetens erfarenhet av liknande incidenter. Indikatorer såsom i vilken utsträckning tjänstens funktion påverkas, hur länge incidenten pågår eller hur många tjänstemottagare som drabbas kan spela en viktig roll när man fastställer om tjänstens driftsstörning är allvarlig.

(102) Om väsentliga eller viktiga entiteter får kännedom om en betydande incident bör de vara skyldiga att lämna in en tidig varning utan onödigt dröjsmål och under alla omständigheter inom 24 timmar. Denna tidiga varning bör åtföljas av en incidentanmälan. De berörda entiteterna bör lämna in en incidentanmälan utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande incidenten, särskilt i syfte att uppdatera den information som lämnats via den tidiga varningen och göra en inledande bedömning av den betydande incidenten, inbegripet dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer. En slutrapport bör lämnas in senast en månad efter incidentunderrättelsen. Den tidiga varningen bör endast innehålla den information som är nödvändig för att göra CSIRT-enheten, eller i förekommande fall den behöriga myndigheten, medveten om den betydande incidenten och ge den berörda entiteten möjlighet att vid behov söka bistånd. Den tidiga varningen bör i tillämpliga fall ange om den betydande incidenten misstänks vara orsakad av olagliga eller avsiktligt skadliga handlingar och om det är troligt att den kommer att få gränsöverskridande verkningar. Medlemsstaterna bör säkerställa att skyldigheten att lämna in den tidiga varningen, eller den efterföljande incidentunderrättelsen, inte avleder den underrättande entitetens resurser från verksamheter i samband med incidenthantering som bör prioriteras, i syfte att förhindra att skyldigheterna att rapportera incidenter antingen avleder resurser från hantering av betydande incidenter eller på annat sätt undergräver entitetens ansträngningar i

detta avseende. I händelse av en pågående incident vid den tidpunkt då slutrapporten lämnas in bör medlemsstaterna säkerställa att berörda entiteter tillhandahåller en lägesrapport vid den tidpunkten och en slutrapport inom en månad efter det att de hanterat den betydande incidenten.

(103) I tillämpliga fall bör väsentliga och viktiga entiteter utan dröjsmål underrätta sina tjänstemottagare om eventuella åtgärder eller avhjälpande arrangemang som dessa kan genomföra för att begränsa de risker som följer av ett betydande cyberhot. När så är lämpligt, och i synnerhet om det är sannolikt att det betydande cyberhotet kommer att förverkligas, bör dessa entiteter även informera sina tjänstemottagare om själva hotet. Kravet på att informera dessa mottagare om betydande cyberhot bör uppfyllas efter bästa förmåga men bör inte befria entiteter från skyldigheten att på egen bekostnad vidta lämpliga och omedelbara åtgärder för att förebygga eller avhjälpa sådana hot och återställa tjänstens normala säkerhetsnivå. Sådan information om betydande cyberhot bör tillhandahållas tjänstemottagarna kostnadsfritt och vara formulerad på ett lättbegripligt sätt.

(104) Tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster bör tillämpa inbyggd säkerhet och säkerhet som standard och informera sina tjänstemottagare om betydande cyberhot och om åtgärder dessa kan vidta för att skydda säkerheten för sina enheter och sin kommunikation, t.ex. genom att använda särskilda typer av programvara eller krypteringsteknik.

(105) En proaktiv strategi mot cyberhot är en viktig del av riskhanteringsåtgärderna för cybersäkerhet som bör göra det möjligt för de behöriga myndigheterna att effektivt förhindra att cyberhot blir incidenter som kan vålla betydande materiell eller immateriell skada. Det är därför av avgörande vikt att cyberhot anmäls. I detta syfte uppmuntras entiteter att rapportera cyberhot på frivillig basis.

(106) För att förenkla rapporteringen av information som krävs enligt detta direktiv och för att minska den administrativa bördan för entiteter bör medlemsstaterna tillhandahålla tekniska hjälpmedel såsom en gemensam kontaktpunkt, automatiserade system, onlineformulär, användarvänliga gränssnitt, mallar och särskilda plattformar för entiteter, oberoende av om de omfattas av tillämpningsområdet för detta direktiv, som de kan använda för att lämna in den relevanta information som ska rapporteras. Unionsfinansiering till stöd för genomförandet av detta direktiv, särskilt inom programmet för ett digitalt Europa, som inrättats genom Europaparlamentets och rådets förordning (EU) 2021/694 ([21]), kan inkludera stöd till gemensamma kontaktpunkter. Vidare befinner sig entiteter ofta i en situation där en viss incident på grund av sina särdrag måste rapporteras till flera olika myndigheter till följd av underrättelseskyldigheter enligt olika rättsliga instrument. Sådana fall skapar ytterligare administrativa bördor och kan också leda till osäkerhet om format och förfaranden för sådana underrättelser. Om en gemensam kontaktpunkt inrättas, uppmuntras medlemsstaterna även att använda denna gemensamma kontaktpunkt för underrättelser om säkerhetsincidenter enligt annan unionsrätt, såsom förordning (EU) 2016/679 och direktiv 2002/58/EG. Användningen av en sådan gemensam kontaktpunkt för att rapportera säkerhetsincidenter enligt förordning (EU) 2016/679 och direktiv 2002/58/EG bör inte påverka tillämpningen av bestämmelserna i förordning (EU) 2016/679 och direktiv 2002/58/EG, särskilt de som rör den oberoende ställningen för de myndigheter som avses i dessa. Enisa bör i samarbete med samarbetsgruppen utarbeta gemensamma mallar för underrättelser med hjälp av riktlinjer för att förenkla och rationalisera den information som ska rapporteras enligt unionsrätten och minska den administrativa bördan för de underrättande entiteterna.

(107) Om en incident misstänks ha samband med allvarlig brottslig verksamhet enligt unionsrätt eller nationell rätt, bör medlemsstaterna uppmuntra väsentliga och viktiga entiteter att, på grundval av tillämpliga straffrättsliga bestämmelser i enlighet med unionsrätten, rapportera incidenter som misstänks vara av allvarlig brottslig art till de relevanta rättsvårdande myndigheterna. Där så är lämpligt, och utan att det påverkar de bestämmelser om skydd av personuppgifter som gäller för Europol, är det önskvärt att samordning mellan behöriga myndigheter och rättsvårdande myndigheter i olika medlemsstater underlättas av Europeiska it-brottcentrumet (EC3) och Enisa.

([21]) Europaparlamentets och rådets förordning (EU) 2021/694 av den 29 april 2021 om inrättande av programmet för ett digitalt Europa och om upphävande av beslut (EU) 2015/2240 (EUT L 166, 11.5.2021, s. 1).

(108) Säkerheten för personuppgifter undergrävs ofta till följd av incidenter. I detta sammanhang bör de behöriga myndigheterna samarbeta och utbyta information om alla relevanta frågor med de myndigheter som avses i förordning (EU) 2016/679 och direktiv 2002/58/EG.

(109) Att upprätthålla korrekta och fullständiga databaser med registreringsuppgifter för domännamn (WHOIS-data) och ge laglig åtkomst till sådana uppgifter är avgörande för att säkerställa domännamnssystemets säkerhet, stabilitet och resiliens, vilket i sin tur bidrar till en hög gemensam nivå av cybersäkerhet i hela unionen. För detta specifika ändamål bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster vara skyldiga att behandla vissa uppgifter som är nödvändiga för detta. Sådan behandling bör vara en rättslig förpliktelse i den mening som avses i artikel 6.1 c i förordning (EU) 2016/679. Denna förpliktelse bör inte påverka möjligheten att samla in registreringsuppgifter för domännamn för andra ändamål, exempelvis på grundval av avtal eller rättsliga skyldigheter som fastställs i annan unionsrätt eller nationell rätt. Denna förpliktelse syftar till att erhålla en fullständig och korrekt uppsättning registreringsuppgifter och bör inte resultera i att samma uppgifter samlas in flera gånger. Registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör samarbeta med varandra för att undvika dubbelarbete.

(110) Tillgänglighet avseende, och åtkomst i lämplig tid till, domännamnsregistreringsuppgifter för legitima åtkomstsökande är avgörande för att förebygga och bekämpa missbruk av domännamnssystem och för att förebygga, upptäcka och reagera på incidenter. Legitima åtkomstsökande bör tolkas som varje fysisk eller juridisk person som gör en begäran i enlighet med unionsrätten eller nationell rätt. Det kan inbegripa myndigheter som är behöriga enligt detta direktiv och sådana som enligt unionsrätten eller nationell rätt är behöriga i fråga om förebyggande, utredning, upptäckt eller lagföring av brott, samt Cert eller CSIRT-enheter. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör vara skyldiga att möjliggöra för legitima åtkomstsökande att få laglig åtkomst till specifika domännamnsregistreringsuppgifter som är nödvändiga för åtkomstbegärans syfte, i enlighet med unionsrätten och nationell rätt. Begäran från legitima åtkomstsökande bör åtföljas av en motivering som gör det möjligt att bedöma nödvändigheten av att få åtkomst till uppgifterna.

(111) För att säkerställa tillgången till korrekta och fullständiga registreringsuppgifter för domännamn bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster samla in registreringsuppgifter för domännamn och garantera deras integritet och tillgänglighet. I synnerhet bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster fastställa policyer och förfaranden för insamling och lagring av korrekta och fullständiga registreringsuppgifter för domännamn samt för att förhindra och korrigera felaktiga registreringsuppgifter i enlighet med unionens dataskyddslagstiftning. Dessa policyer och förfaranden bör så långt det är möjligt beakta de standarder som utvecklats av flerpartsförvaltningsstrukturerna på internationell nivå. Registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör anta och genomföra proportionella förfaranden för att verifiera registreringsuppgifterna för domännamn. Dessa förfaranden bör spegla bästa branschpraxis och, så långt det är möjligt, de framsteg som gjorts inom elektronisk identifiering. Exempel på verifieringsförfaranden kan vara förhandskontroller som görs i samband med registreringen och efterhandskontroller som görs efter registreringen. Registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör, i synnerhet, verifiera minst ett av registrantens kontaktsätt.

(112) Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör vara skyldiga att offentliggöra domännamnsregistreringsuppgifter som inte omfattas av unionens dataskyddslagstiftning, till exempel uppgifter som rör juridiska personer, i överensstämmelse med ingressen till förordning (EU) 2016/679. När det gäller juridiska personer bör registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster offentliggöra åtminstone registrantens namn och telefonnummer. E-postadressen bör också offentliggöras förutsatt att den inte innehåller några personuppgifter, såsom när det gäller e-postalias eller funktionsbrevlådor. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör också möjliggöra för legitima åtkomstsökande att få laglig åtkomst till specifika domännamnsregistreringsuppgifter som rör fysiska personer, i enlighet med unionens dataskyddslagstiftning. Medlemsstaterna bör ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål besvara ansökningar om utlämnande av registreringsuppgifter för domännamn från legitima åtkomstsökande. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör fastställa policyer och förfaranden för offentliggörande och utlämnande av registreringsuppgifter, inbegripet servicenivåavtal för att hantera ansökningar om åtkomst från legitima åtkomstsökande. Dessa policyer och förfaranden bör så långt det är möjligt beakta eventuell vägledning

och de standarder som utvecklats av flerpartsförvaltningsstrukturerna på internationell nivå. Åtkomstförfarandet kan också omfatta användning av ett gränssnitt, en portal eller annat tekniskt verktyg som ett effektivt system för att begära och få tillgång till registreringsuppgifter. I syfte att främja harmoniserad praxis på hela den inre marknaden kan kommissionen, utan att det påverkar Europeiska dataskyddsstyrelsens befogenheter, tillhandahålla riktlinjer för sådana förfaranden, som i möjligaste mån beaktar de standarder som utvecklats av flerpartsförvaltningsstrukturerna på internationell nivå. Medlemsstaterna bör säkerställa att alla typer av åtkomst till registreringsuppgifter för domännamn, både personuppgifter och icke-personuppgifter, är kostnadsfria.

(113) Entiteter som omfattas av detta direktivs tillämpningsområde bör anses omfattas av jurisdiktionen i den medlemsstat där de är etablerade. Tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster bör dock anses omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster. Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster bör anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen. Offentliga förvaltningsentiteter bör anses omfattas av jurisdiktionen i den medlemsstat som inrättat dem. Om entiteten tillhandahåller tjänster eller är etablerad i mer än en medlemsstat bör den omfattas av dessa medlemsstaters separata och parallella jurisdiktioner samtidigt. De behöriga myndigheterna i dessa medlemsstater bör samarbeta, ge varandra ömsesidigt bistånd och när det är lämpligt genomföra gemensamma tillsynsåtgärder. När medlemsstater utövar jurisdiktion bör de inte påföra efterlevnadskontrollåtgärder eller sanktioner mer än en gång för samma beteende, i överensstämmelse med principen *ne bis in idem*.

(114) För att ta hänsyn till den gränsöverskridande karaktären hos de tjänster och den verksamhet som utförs av leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster bör endast en medlemsstat ha jurisdiktion över dessa entiteter. Jurisdiktion bör tilldelas den medlemsstat där den berörda entiteten har sitt huvudsakliga etableringsställe i unionen. Kriteriet för etableringsställe i detta direktiv förutsätter att verksamhet faktiskt bedrivs genom en stabil struktur. Den rättsliga formen för en sådan struktur, oavsett om det är en filial eller ett dotterföretag med status som juridisk person, bör inte vara den avgörande faktorn i detta avseende. Huruvida kriteriet är uppfyllt bör inte vara beroende av om nätverks- och informationssystemen är fysiskt belägna på en viss plats. Förekomsten och användningen av sådana system utgör inte i sig en sådan huvudsaklig etablering och är därför inte avgörande kriterier för att fastställa det huvudsakliga etableringsstället. Det huvudsakliga etableringsstället bör anses ligga i den medlemsstat där besluten om åtgärder för att hantera cybersäkerhetsrisker i huvudsak fattas i unionen. Detta motsvarar vanligtvis platsen för entiteternas huvudkontor i unionen. Om en sådan medlemsstat inte kan fastställas eller om sådana beslut inte fattas i unionen bör det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där cybersäkerhetsoperationer utförs. Om en sådan medlemsstat inte kan fastställas bör det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där entiteten har etableringsstället med flest anställda i unionen. Om tjänsterna utförs av en koncern bör det kontrollerande företagets huvudsakliga etableringsställe betraktas som koncernens huvudsakliga etableringsställe.

(115) När en allmänt tillgänglig rekursiv DNS-tjänst tillhandahålls av en tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster endast som en del av internetanslutningstjänsten, bör entiteten anses omfattas av jurisdiktionen i alla de medlemsstater där dess tjänster tillhandahålls.

(116) Om en leverantör av DNS-tjänster, en registreringsenhet för toppdomäner, en entitet som tillhandahåller domännamnsregistreringstjänster, en leverantör av molntjänster, en leverantör av datacentraltjänster, en leverantör av nätverk för leverans av innehåll, driftsentreprenad, en leverantör av hanterade säkerhetstjänster eller en leverantör av en marknadsplats online, en sökmotor eller en plattform för sociala nätverkstjänster, vilken inte är etablerad i unionen, erbjuder tjänster inom unionen bör den utse en företrädare i unionen. I syfte att fastställa om en sådan entitet erbjuder tjänster inom unionen bör det kontrolleras om entiteten planerar att erbjuda tjänster till personer i en eller flera medlemsstater. Enbart den omständigheten att en entitets eller en mellanhands webbplats eller en e-postadress eller andra kontaktuppgifter är tillgängliga i unionen, eller att ett språk används som allmänt används i det tredjeland där entiteten är etablerad, bör inte betraktas som tillräcklig för att fastställa en sådan avsikt. Emellertid kan faktorer som att det används ett visst språk eller en viss valuta som allmänt används i en eller flera medlemsstater med möjligheten att beställa tjänster på det språket, eller att kunder eller användare i unionen omnämns, göra det uppenbart att entiteten planerar att erbjuda tjänster inom unionen. Företrädaren bör agera på entitetens vägnar, och det bör vara möjligt för de behöriga myndigheterna eller CSIRT-enheterna att vända sig till företrädaren. Företrädaren bör utses uttryckligen genom en skriftlig fullmakt från entiteten att agera på dess vägnar med avseende på dess skyldigheter enligt detta direktiv, inklusive incidentrapportering.

(117) För att säkerställa en tydlig överblick över leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster, vilka tillhandahåller tjänster i unionen som omfattas av detta direktivs tillämpningsområde, bör Enisa skapa och upprätthålla ett register över sådana entiteter på grundval av information från medlemsstaterna, i förekommande fall via nationella mekanismer som inrättats för entiteter att registrera sig. De gemensamma kontaktpunkterna bör till Enisa vidarebefordra informationen och eventuella ändringar av densamma. För att säkerställa att den information som ska ingå i registret är korrekt och fullständig kan medlemsstaterna till Enisa lämna in den information som finns tillgänglig i nationella register om dessa entiteter. Enisa och medlemsstaterna bör vidta åtgärder för att underlätta kompatibilitet mellan sådana register, samtidigt som skydd av konfidentiell eller säkerhetsskyddsklassificerade uppgifter säkerställs. Enisa bör införa lämplig klassificering av information och förvaltningsprotokoll för att säkerställa den utlämnade informationens säkerhet och konfidentialitet och begränsa åtkomsten till samt lagringen och överföringen av sådan information till de avsedda användarna.

(118) Om uppgifter som är säkerhetsskyddsklassificerade enligt unionsrätt eller nationell rätt utbyts, rapporteras eller på annat sätt delas enligt detta direktiv, bör motsvarande regler för hantering av säkerhetsskyddsklassificerade uppgifter tillämpas. Vidare bör Enisa ha infrastruktur, förfaranden och regler för att hantera känsliga och säkerhetsskyddsklassificerade uppgifter i enlighet med tillämpliga säkerhetsregler för skydd av säkerhetsskyddsklassificerade EU-uppgifter.

(119) I och med att cyberhoten blir mer komplexa och sofistikerade är god upptäckt av sådana hot och förebyggande åtgärder mot dem i stor utsträckning beroende av ett regelbundet utbyte av underrättelser om hot och sårbarhet mellan entiteter. Informationsutbyte bidrar till ökad medvetenhet om cyberhot, vilket i sin tur ökar entiteternas förmåga att förhindra att hot blir till incidenter och gör det möjligt för entiteterna att bättre begränsa effekterna av incidenter och återhämta sig mer effektivt. I avsaknad av vägledning på unionsnivå verkar olika faktorer ha hindrat sådant utbyte av underrättelser, särskilt osäkerheten om förenligheten med konkurrens- och ansvarsreglerna.

(120) Entiteter bör uppmuntras och bistås av medlemsstaterna för att kollektivt utnyttja sina individuella kunskaper och praktiska erfarenheter på strategisk, taktisk och operativ nivå i syfte att förbättra sin förmåga att på lämpligt sätt förebygga, upptäcka, reagera på eller återhämta sig från incidenter eller begränsa deras verkningar. Det är därför nödvändigt att på unionsnivå möjliggöra framväxten av arrangemang för frivilligt informationsutbyte om cybersäkerhet. I detta syfte bör medlemsstaterna aktivt bistå och uppmuntra entiteter, såsom de som erbjuder cybersäkerhetstjänster och forskning, samt relevanta entiteter som inte omfattas av detta direktiv, att delta i sådana arrangemang för informationsutbyte om cybersäkerhet. Dessa arrangemang bör fastställas i enlighet med unionens konkurrensregler och unionens dataskyddslagstiftning.

(121) Behandling av personuppgifter i den utsträckning som är nödvändig och proportionell för att säkerställa säkerhet i nätverks- och informationssystem genom väsentliga och viktiga entiteter kan anses vara laglig på grund av att sådan behandling är förenlig med en rättslig förpliktelse som åvilar den personuppgiftsansvarige i enlighet med kraven i artikel 6.1 c och artikel 6.3 i förordning (EU) 2016/679. Behandling av personuppgifter kan även vara nödvändig på grund av berättigade intressen hos väsentliga och viktiga entiteter, samt tillhandahållare av säkerhetsteknik och säkerhetstjänster som agerar på dessa entiteters vägnar, i enlighet med artikel 6.1 f i förordning (EU) 2016/679, bland annat när sådan behandling är nödvändig för arrangemang för informationsutbyte om cybersäkerhet eller frivillig underrättelse om relevant information i enlighet med detta direktiv. Åtgärder som rör förebyggande, upptäckt, identifiering, begränsning, analys och hantering av incidenter, åtgärder för att öka medvetenheten om specifika cyberhot, informationsutbyte i samband med avhjälpande av sårbarheter och samordnat meddelande av sårbarhetsinformation, frivilligt informationsutbyte om sådana incidenter samt cyberhot och sårbarheter, angreppsindikatorer, taktik, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg kan kräva behandling av vissa kategorier av personuppgifter, såsom ip-adresser, webbadresser (URL), domännamn, e-postadresser och tidsstämplar, när dessa avslöjar personuppgifter. Personuppgiftsbehandling av behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter kan utgöra en rättslig förpliktelse eller anses vara nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den ansvariges myndighetsutövning i enlighet med artikel 6.1 c eller e och artikel 6.3 i förordning (EU) 2016/679 eller på grund av ett berättigat intresse hos de väsentliga och viktiga entiteterna enligt vad som avses i artikel 6.1 f i den förordningen. Vidare kan nationell rätt innehålla bestämmelser som tillåter att behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter, i den utsträckning som är nödvändig och proportionell för att säkerställa säkerhet i nätverks- och informationssystem hos väsentliga och viktiga entiteter, behandlar särskilda kategorier av personuppgifter i enlighet med artikel 9 i förordning (EU) 2016/679, särskilt genom att föreskriva lämpliga och särskilda åtgärder för att skydda fysiska personers grundläggande rättigheter och intressen, däribland tekniska begränsningar för vidareutnyttjande av sådana uppgifter samt användning av moderna säkerhetsåtgärder och integritetsbevarande åtgärder, såsom pseudonymisering, eller kryptering där anonymisering avsevärt kan påverka det eftersträvade ändamålet.

(122) För att stärka de tillsynsbefogenheter och tillsynsåtgärder som bidrar till att säkerställa ett effektivt fullgörande av skyldigheter bör detta direktiv innehålla en minimiförteckning över tillsynsåtgärder och tillsynsmedel genom vilka behöriga myndigheter kan utöva tillsyn över väsentliga och viktiga entiteter. Dessutom bör detta direktiv fastställa en differentiering av tillsynssystemet mellan väsentliga och viktiga entiteter i syfte att säkerställa en rättvis balans vad gäller skyldigheterna för dessa entiteter och de behöriga myndigheterna. Väsentliga entiteter bör därför omfattas av ett heltäckande tillsynssystem med förhandstillsyn och efterhandstillsyn, medan viktiga entiteter bör omfattas av enklare tillsyn, endast i efterhand. Viktiga entiteter bör därför inte vara skyldiga att systematiskt dokumentera efterlevnad av riskhanteringsåtgärderna för cybersäkerhet, medan de behöriga myndigheterna bör tillämpa en reaktiv efterhandstillsyn och därmed inte ha någon allmän skyldighet att utöva tillsyn över dessa entiteter. Efterhandstillsynen av viktiga entiteter kan utlösas av bevis, indikationer eller uppgifter som har kommit till de behöriga myndigheternas kännedom och som enligt dessa myndigheter tyder på potentiella överträdelser av detta direktiv. Sådana bevis, indikationer eller uppgifter kan exempelvis vara av den typ som de behöriga myndigheterna mottar från andra myndigheter, entiteter, medborgare, medier eller andra källor eller offentligt tillgänglig information eller härröra från annan verksamhet som de behöriga myndigheterna bedriver i samband med fullgörandet av sina uppgifter.

(123) Behöriga myndigheters utförande av tillsynsuppgifter bör inte i onödan hämma den berörda entitetens affärsverksamhet. När behöriga myndigheter utför sina tillsynsuppgifter avseende väsentliga entiteter, bland annat genom inspektioner på plats och distansbaserad tillsyn, utredning av överträdelser av detta direktiv, säkerhetsrevisioner eller säkerhetsskanningar, bör de minimera konsekvenserna för den berörda entitetens affärsverksamhet.

(124) Vid genomförandet av förhandstillsyn bör de behöriga myndigheterna kunna besluta att prioritera användningen av de tillsynsåtgärder och tillsynsmedel som står till deras förfogande på ett proportionellt sätt. Detta innebär att de behöriga myndigheterna kan besluta om en sådan prioritering på grundval av tillsynsmetoder som bör bygga på en riskbaserad ansats. Mer specifikt kan sådana metoder omfatta kriterier eller riktmärken för klassificering av väsentliga entiteter i riskkategorier och motsvarande tillsynsåtgärder och tillsynsmedel som rekommenderas per riskkategori, såsom användning av frekvens för eller typ av inspektion på plats, riktade säkerhetsrevisioner eller säkerhetsskanningar, vilken typ av information som ska begäras och detaljnivån på denna information. Sådana

tillsynsmetoder skulle även kunna åtföljas av arbetsprogram och utvärderas och ses över regelbundet, inklusive med avseende på aspekter som resursfördelning och resursbehov. När det gäller offentliga förvaltningsentiteter bör tillsynsbefogenheterna utövas i överensstämmelse med nationella lagstiftningsmässiga och institutionella ramar.

(125) De behöriga myndigheterna bör säkerställa att deras tillsynsuppgifter med avseende på väsentliga och viktiga entiteter utförs av utbildad personal, som bör ha de nödvändiga färdigheterna för att utföra dessa uppgifter, särskilt i fråga om att genomföra inspektioner på plats och distansbaserad tillsyn, bland annat identifiering av svagheter i databaser, maskinvara, brandväggar, kryptering och nätverk. Inspektionerna och tillsynen bör utföras på ett objektivt sätt.

(126) I vederbörligen motiverade fall bör den behöriga myndigheten, när den fått kännedom om ett betydande cyberhot eller en överhängande risk, kunna fatta omedelbara beslut om efterlevnadskontroll i syfte att förhindra eller reagera på en incident.

(127) För att efterlevnadskontrollen ska bli effektiv bör det fastställas en minimiförteckning över efterlevnadskontrollbefogenheter som kan utövas för brott mot de riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som föreskrivs i detta direktiv, med en tydlig och konsekvent ram för sådan efterlevnadskontroll i hela unionen. Vederbörlig hänsyn bör tas till arten, allvarlighetsgraden och varaktigheten av överträdelsen av detta direktiv, de materiella eller immateriella skador som orsakats, om överträdelsen var avsiktlig eller berodde på försumlighet, åtgärder som vidtagits för att förhindra eller begränsa de materiella eller immateriella skadorna, graden av ansvar eller relevanta tidigare överträdelser, graden av samarbete med den behöriga myndigheten och andra försvårande eller förmildrande omständigheter. Efterlevnadskontrollåtgärderna, inklusive administrativa sanktionsavgifter, bör vara proportionella och påförandet av dem bör omfattas av lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och Europeiska unionens stadga om de grundläggande rättigheterna (*stadgan*), inbegripet rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar.

(128) Detta direktiv ålägger inte medlemsstaterna att föreskriva att fysiska personer med ansvar för att säkerställa att en entitet efterlever direktivet ska omfattas av straffrättsligt eller civilrättsligt ansvar för skada som åsamkats tredjeparter till följd av en överträdelse av direktivet.

(129) För att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i detta direktiv bör varje behörig myndighet ha befogenhet att påföra eller begära påförande av administrativa sanktionsavgifter.

(130) Om en administrativ sanktionsavgift påförs en väsentlig eller viktig entitet som är ett företag, bör ett företag i detta sammanhang anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget. Om en administrativ sanktionsavgift påförs en person som inte är ett företag, bör den behöriga myndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation när den överväger lämplig sanktionsavgift. Medlemsstaterna bör fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter. Föreläggande av en administrativ sanktionsavgift påverkar inte de behöriga myndigheternas tillämpning av andra befogenheter eller andra sanktioner som fastställs i de nationella bestämmelser som införlivar detta direktiv.

(131) Medlemsstaterna bör kunna fastställa bestämmelser om straffrättsliga påföljder för överträdelser av de nationella bestämmelser som införlivar detta direktiv. Påförandet av straffrättsliga påföljder för överträdelser av sådana nationella bestämmelser och relaterade administrativa sanktioner bör dock inte medföra ett åsidosättande av principen *ne bis in idem* enligt Europeiska unionens domstols tolkning.

(132) När detta direktiv inte harmoniserar administrativa sanktioner eller när så är nödvändigt i andra fall, till exempel i händelse av en allvarlig överträdelse av detta direktiv, bör medlemsstaterna genomföra ett system med effektiva, proportionella och avskräckande sanktioner. Dessa påföljders art, och frågan om de är straffrättsliga eller administrativa, bör fastställas i nationell rätt.

(133) För att de sanktioner som är tillämpliga på överträdelser av efterlevnadskontrollåtgärder detta direktiv ska bli mer effektiva och avskräckande bör de behöriga myndigheterna ges befogenhet att tillfälligt upphäva eller begära tillfälligt upphävande av en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls av en väsentlig entitet samt begära införande av ett tillfälligt förbud för en fysisk person som har ledningsansvar på nivån för verkställande direktör eller juridiskt ombud att utöva ledande funktioner. Med tanke på deras stränghet och påverkan på entiteternas verksamheter och i sista hand på användarna bör sådana tillfälliga upphävanden eller förbud endast tillämpas proportionellt mot överträdelsens allvarlighetsgrad och med beaktande av omständigheterna i varje enskilt fall, inbegripet om överträdelsen var avsiktlig eller berodde på försumlighet, samt åtgärder som vidtagits för att förhindra eller begränsa de materiella eller immateriella skadorna. Sådana tillfälliga upphävanden eller förbud bör endast tillämpas som sista utväg, dvs. först efter det att de andra relevanta åtgärder för efterlevnadskontroll som fastställs i detta direktiv har uttömts, och endast fram till dess att den berörda entiteten vidtar nödvändiga åtgärder för att avhjälpa de brister eller uppfylla de krav från den behöriga myndigheten för vilka de tillfälliga upphävandena eller förbuden tillämpades. Införandet av sådana tillfälliga upphävanden eller förbud bör omfattas av lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och stadgan, inbegripet rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar.

(134) För att säkerställa att entiteter fullgör sina skyldigheter enligt detta direktiv bör medlemsstaterna samarbeta med och bistå varandra med avseende på tillsyns- och efterlevnadskontrollåtgärder, särskilt om en entitet tillhandahåller tjänster i mer än en medlemsstat eller om dess nätverks- och informationssystem är belägna i en annan medlemsstat än den där den tillhandahåller tjänster. När den tillfrågade behöriga myndigheten tillhandahåller bistånd bör den vidta åtgärder för tillsyns- och efterlevnadskontrollåtgärder i enlighet med nationell rätt. För att säkerställa ett välfungerande ömsesidigt bistånd enligt detta direktiv bör de behöriga myndigheterna använda samarbetsgruppen som ett forum där de kan diskutera fall och enskilda biståndsansökningar.

(135) För att säkerställa effektiv tillsyn och efterlevnadskontroll, framför allt i en situation med en gränsöverskridande dimension, bör de medlemsstater som har mottagit en begäran om ömsesidigt bistånd, inom ramen för begäran, vidta lämpliga tillsyns- och efterlevnadskontrollåtgärder med avseende på den entitet som är föremålet för den begäran och som tillhandahåller tjänster eller som har ett nätverks- och informationssystem inom den medlemsstatens territorium.

(136) Detta direktiv bör fastställa regler för samarbete mellan de behöriga myndigheterna och tillsynsmyndigheterna enligt förordning (EU) 2016/679 för att hantera överträdelser av detta direktiv som rör personuppgifter.

(137) Detta direktiv bör syfta till att säkerställa en hög ansvarsnivå för riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter för väsentliga och viktiga entiteter. Därför bör ledningsorganen för väsentliga och viktiga entiteter godkänna riskåtgärderna för cybersäkerhet och övervaka deras genomförande.

(138) För att säkerställa en hög gemensam cybersäkerhetsnivå i unionen på grundval av detta direktiv bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på att komplettera detta direktiv genom att ange vilka kategorier av väsentliga och viktiga entiteter som ska vara skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhålla ett certifikat enligt en europeisk ordning för cybersäkerhetscertifiering. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning ([22]). För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

([22]) EUT L 123, 12.5.2016, s. 1.

(139) För att säkerställa enhetliga villkor för genomförandet av detta direktiv bör kommissionen tilldelas genomförandebefogenheter för att fastställa de förfaranden som krävs för samarbetsgruppens verksamhet och de tekniska och metodologiska kraven samt sektorskraven avseende riskhanteringsåtgärder för cybersäkerhet, samt ytterligare precisera typen av information samt formatet och förfarandet för underrättelser om incidenter, cyberhot och tillbud och för kommunikation om betydande cyberhot, samt i vilka fall en incident ska betraktas som betydande. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([23]).

(140) Detta direktiv bör med jämna mellanrum ses över av kommissionen i samråd med berörda parter, främst i syfte att avgöra huruvida det är lämpligt att föreslå ändringar med hänsyn till samhällsutvecklingen, den politiska utvecklingen, den tekniska utvecklingen eller ändrade marknadsvillkor. Som en del av de översynerna bör kommissionen bedöma vilken relevans de berörda entiteternas storlek och de sektorer, delsektorer och typer av entiteter som avses i bilagorna till detta direktiv har för ekonomins och samhällets funktion när det gäller cybersäkerhet. Kommissionen bör bland annat bedöma huruvida leverantörer som omfattas av tillämpningsområdet för detta direktiv vilka klassificeras som mycket stora onlineplattformar i den mening som avses i artikel 33 i Europaparlamentets och rådets förordning (EU) 2022/2065 ([24]) kan identifieras som väsentliga entiteter enligt detta direktiv.

(141) Detta direktiv skapar nya uppgifter för Enisa och stärker därigenom dess roll, och kan också leda till att Enisa tvingas utföra sina befintliga uppgifter enligt förordning (EU) 2019/881 på en högre nivå än tidigare. För att säkerställa att Enisa har de ekonomiska resurser och den personal som krävs för att utföra befintliga och nya uppgifter och uppnå en eventuellt högre nivå på genomförandet av dessa uppgifter till följd av dess utökade roll, bör dess budget ökas i motsvarande grad. För att säkerställa en effektiv resursanvändning bör Enisa dessutom ges större flexibilitet när det gäller möjligheten att fördela resurser internt, i syfte att kunna utföra sina uppgifter och infria förväntningarna på ett ändamålsenligt sätt.

(142) Eftersom målet för detta direktiv, nämligen att uppnå en hög gemensam cybersäkerhetsnivå i unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå detta mål.

(143) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i stadgan, i synnerhet rätten till respekt för privatliv och kommunikationer, skydd av personuppgifter, näringsfriheten, rätten till egendom, rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar. Rätten till ett effektivt rättsmedel inbegriper mottagarna av tjänster som tillhandahålls av väsentliga och viktiga entiteter. Detta direktiv bör genomföras i enlighet med dessa rättigheter och principer.

(144) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([25]) och avgav ett yttrande den 11 mars 2021 ([26]).

([23]) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

([24]) Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (rättsakten om digitala tjänster) (EUT L 277, 27.10.2022, s. 1).

([25]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

([26]) EUT C 183, 11.5.2021, s. 3.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

1. I detta direktiv fastställs åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion.

2. Direktivet fastställer i detta syfte följande:

a) Skyldigheter som ålägger medlemsstaterna att anta nationella strategier för cybersäkerhet och att utse eller inrätta behöriga myndigheter, myndigheter för hantering av cyberkriser, gemensamma kontaktpunkter för cybersäkerhet (gemensamma kontaktpunkter) och enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter).

b) Riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter för entiteter av den typ som avses i bilaga I eller II samt för entiteter som identifieras som kritiska entiteter enligt direktiv (EU) 2022/2557.

c) Regler och skyldigheter när det gäller informationsutbyte om cybersäkerhet.

d) Skyldigheter för medlemsstaterna när det gäller tillsyn och efterlevnadskontroll.

Artikel 2

Tillämpningsområde

1. Detta direktiv är tillämpligt på offentliga eller privata entiteter av den typ som avses i bilaga I eller II som betecknas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG eller överstiger de trösklar för medelstora företag som avses i punkt 1 i den artikeln och som tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen.

Artikel 3.4 i bilagan till den rekommendationen är inte tillämplig med avseende på detta direktiv.

2. Oavsett entiteternas storlek är detta direktiv också tillämpligt på entiteter av en typ som avses i bilaga I eller II, i följande fall:

a) Om tjänster tillhandahålls av

   i) tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster,

   ii) tillhandahållare av betrodda tjänster,

   iii) registreringsenheter för toppdomäner och leverantörer av domännamnssystemtjänster.

b) Om entiteten är den enda leverantören i en medlemsstat av en tjänst som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet.

c) Om en störning av den tjänst som entiteten tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa.

d) Om en störning av den tjänst som entiteten tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser.

e) Entiteten är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer i medlemsstaten som är beroende av denna entitet.

f) Om entiteten är en offentlig förvaltningsentitet

i) på statlig nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, eller

ii) på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, som enligt en riskbaserad bedömning tillhandahåller tjänster vars störning kan ha en betydande effekt på kritisk samhällelig eller ekonomisk verksamhet.

3. Oavsett entiteternas storlek är detta direktiv tillämpligt på entiteter som identifieras som kritiska entiteter enligt direktiv (EU) 2022/2557.

4. Oavsett entiteternas storlek är detta direktiv tillämpligt på entiteter som tillhandahåller domännamnsregistreringstjänster.

5. Medlemsstaterna får föreskriva att detta direktiv ska tillämpas på

a) offentliga förvaltningsentiteter på lokal nivå,

b) utbildningsinstitut, särskilt om de utför kritisk forskningsverksamhet.

6. Detta direktiv påverkar inte medlemsstaternas ansvar för att skydda nationell säkerhet och deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning.

7. Detta direktiv är inte tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott.

8. Medlemsstaterna får undanta särskilda entiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, eller som tillhandahåller tjänster uteslutande till en offentlig förvaltningsentitet som avses i punkt 7 i den här artikeln, från skyldigheterna i artikel 21 eller 23 med avseende på sådan verksamhet eller sådana tjänster. I sådana fall ska de tillsyns- och efterlevnadskontrollåtgärder som avses i kapitel VII inte tillämpas på denna specifika verksamhet eller dessa specifika tjänster. Om entiteterna bedriver verksamhet eller tillhandahåller tjänster uteslutande av den typ som avses i den här punkten, får medlemsstaterna besluta att befria dessa entiteter också från skyldigheterna i artiklarna 3 och 27.

9. Punkterna 7 och 8 är inte tillämpliga om en entitet agerar som tillhandahållare av betrodda tjänster.

10. Detta direktiv är inte tillämpligt på entiteter som medlemsstaterna har undantagit från tillämpningsområdet för förordning (EU) 2022/2554 i enlighet med artikel 2.4 i den förordningen.

11. De skyldigheter som fastställs i detta direktiv ska inte medföra tillhandahållande av information vars utlämnande strider mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar.

12. Detta direktiv påverkar inte tillämpningen av förordning (EU) 2016/679, direktiv 2002/58/EG, Europaparlamentets och rådets direktiv 2011/93/EU ([27]) och 2013/40/EU ([28]) och direktiv (EU) 2022/2557.

13. Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget ska information som är konfidentiell enligt unionsbestämmelser eller nationella bestämmelser, såsom bestämmelser om affärshemligheter, utbytas med kommissionen och andra berörda myndigheter i enlighet med detta direktiv endast när ett sådant utbyte är nödvändigt för att tillämpa detta direktiv. Den information som utbyts ska begränsas till vad som är relevant och proportionellt för ändamålet med utbytet. Vid utbytet ska informationens konfidentialitet bevaras och berörda entiteters säkerhets- och affärsintressen skyddas.

([27]) Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF (EUT L 335, 17.12.2011, s. 1).

([28]) Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF (EUT L 218, 14.8.2013, s. 8).

14. Entiteter, behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter ska behandla personuppgifter i den utsträckning som krävs för tillämpningen av detta direktiv och i enlighet med förordning (EU) 2016/679, i synnerhet ska sådan behandling baseras på artikel 6 i denna.

Behandlingen av personuppgifter enligt detta direktiv av tillhandahållare av allmänna elektroniska kommunikationsnät eller tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster ska utföras i enlighet med unionens dataskydds- och integritetslagstiftning, särskilt direktiv 2002/58/EG.

Artikel 3

Väsentliga och viktiga entiteter

1. Med avseende på tillämpningen av detta direktiv ska följande entiteter anses vara väsentliga entiteter:

a) Entiteter av en typ som avses i bilaga I som överstiger trösklarna för medelstora företag som fastställs i artikel 2.1 i bilagan till rekommendation 2003/361/EG.

b) Kvalificerade tillhandahållare av betrodda tjänster och registreringsenheter för toppdomäner samt leverantörer av DNS-tjänster, oavsett storlek.

c) Tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som betraktas som medelstora företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG.

d) Offentliga förvaltningsentiteter som avses i artikel 2.2 f i.

e) Alla andra entiteter av en typ som avses i bilaga I eller II som av en medlemsstat identifierats som väsentliga entiteter i enlighet med artikel 2.2 b–e.

f) Entiteter som identifierats som kritiska entiteter enligt direktiv (EU) 2022/2557, som avses i artikel 2.3 i det här direktivet.

g) Entiteter som medlemsstaterna före den 16 januari 2023 har identifierat som leverantörer av samhällsviktiga tjänster i enlighet med direktiv (EU) 2016/1148 eller nationell rätt, om så föreskrivs av medlemsstaten.

2. Vid tillämpningen av detta direktiv ska alla entiteter av en typ som avses i bilaga I eller II och som inte betraktas som väsentliga entiteter enligt punkt 1 i denna artikel betraktas som viktiga entiteter. Detta inkluderar entiteter som av en medlemsstat identifierats som viktiga entiteter i enlighet med artikel 2.2 b–e.

3. Senast den 17 april 2025 ska medlemsstaterna upprätta en förteckning över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster. Medlemsstaterna ska regelbundet och minst vartannat år därefter se över förteckningen och när det är lämpligt uppdatera den.

4. Vid upprättandet av den förteckning som avses i punkt 3 ska medlemsstaterna ålägga de entiteter som avses i den punkten att lämna minst följande information till de behöriga myndigheterna:

a) Entitetens namn.

b) Adress och aktuella kontaktuppgifter, inklusive e-postadresser, IP-adresser och telefonnummer.

c) I tillämpliga fall, den eller de relevanta sektorer och delsektorer som avses i bilaga I eller II.

d) I tillämpliga fall, en förteckning över de medlemsstater där de tillhandahåller tjänster som omfattas av detta direktiv.

De entiteter som avses i punkt 3 ska meddela alla ändringar av de uppgifter som de lämnat in enligt första stycket i denna punkt utan dröjsmål och under alla omständigheter inom två veckor från datumet för ändringen.

Kommissionen ska, med bistånd från Europeiska unionens cybersäkerhetsbyrå (Enisa), utan onödigt dröjsmål tillhandahålla riktlinjer och mallar för de skyldigheter som fastställs i denna punkt.

Medlemsstaterna får inrätta nationella mekanismer som gör det möjligt för entiteterna att registrera sig själva.

5. Senast den 17 april 2025 och därefter vartannat år ska de behöriga myndigheterna

a) underrätta kommissionen och samarbetsgruppen om antalet väsentliga och viktiga entiteter som förtecknats enligt punkt 3 för varje sektor och delsektor som avses i bilaga I eller II, och

b) lämna relevant information till kommissionen om antalet väsentliga och viktiga entiteter som identifierats i enlighet med artikel 2.2 b–e, den sektor och delsektor som avses i bilaga I eller II som de tillhör, den typ av tjänst som de tillhandahåller och de bestämmelser i artikel 2.2 b–e i enlighet med vilka de identifierades.

6. Fram till den 17 april 2025 och på begäran av kommissionen får medlemsstaterna meddela kommissionen namnen på de väsentliga och viktiga entiteter som avses i punkt 5 b.

Artikel 4

Sektorsspecifika unionsrättsakter

1. Om det i sektorsspecifika unionsrättsakter föreskrivs att väsentliga eller viktiga entiteter ska anta riskhanteringsåtgärder för cybersäkerhet eller underrätta om betydande incidenter, och om dessa krav har minst samma verkan som de skyldigheter som fastställs i detta direktiv, ska de relevanta bestämmelserna i detta direktiv, inbegripet bestämmelserna om tillsyn och efterlevnadskontroll i kapitel VII, inte tillämpas på sådana entiteter. Om de sektorsspecifika unionsrättsakterna inte omfattar alla entiteter inom en viss sektor som omfattas av detta direktivs tillämpningsområde, ska de relevanta bestämmelserna i detta direktiv fortsätta att tillämpas på de entiteter som inte omfattas av dessa sektorsspecifika unionsrättsakter.

2. De krav som avses i punkt 1 i denna artikel ska anses ha samma verkan som de skyldigheter som fastställs i detta direktiv om

a) riskhanteringsåtgärderna för cybersäkerhet minst är likvärdiga som de åtgärder som föreskrivs i artikel 21.1 och 21.2, eller

b) respektive sektorsspecifik unionsrättsakt föreskriver omedelbar, och när det är lämpligt automatisk och direkt, tillgång till incidentunderrättelser från CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt detta direktiv och om kraven på underrättelse av betydande incidenter har minst samma verkan som de krav som fastställs i artikel 23.1–23.6 i detta direktiv.

3. Kommissionen ska senast den 17 juli 2023 tillhandahålla riktlinjer som klargör tillämpningen av punkterna 1 och 2. Kommissionen ska regelbundet se över dessa riktlinjer. Vid utarbetandet av dessa riktlinjer ska kommissionen ta hänsyn till eventuella synpunkter från samarbetsgruppen och Enisa.

Artikel 5

Minimiharmonisering

Detta direktiv hindrar inte medlemsstaterna från att anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten.

Artikel 6

Definitioner

I detta direktiv gäller följande definitioner:

1. nätverks- och informationssystem:

a) Ett elektroniskt kommunikationsnät enligt definitionen i artikel 2.1 i direktiv (EU) 2018/1972.

b) En enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter.

c) Digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av leden a och b för att de ska kunna drivas, användas, skyddas och underhållas.

2. *säkerhet i nätverks- och informationssystem*: nätverks- och informationssystems förmåga att med en viss tillförlitlighetsnivå motstå händelser som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem.

3. *cybersäkerhet*: cybersäkerhet enligt definitionen i artikel 2.1 i förordning (EU) 2019/881.

4. *nationell strategi för cybersäkerhet*: en enhetlig ram i en medlemsstat med strategiska mål och prioriteringar på cybersäkerhetsområdet och en styrningsram för att uppnå dem i den medlemsstaten.

5. *tillbud*: en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod.

6. *incident*: en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.

7. *storskalig cybersäkerhetsincident*: en incident som orsakar störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater.

8. *incidenthantering*: alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident.

9. *risk*: risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att en sådan incident inträffar.

10. *cyberhot*: ett cyberhot enligt definitionen i artikel 2.8 i förordning (EU) 2019/881.

11. *betydande cyberhot*: ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en entitets nätverks- och informationssystem eller användarna av entitetens tjänster genom att vålla betydande materiell eller immateriell skada.

12. *IKT-produkt*: en IKT-produkt enligt definitionen i artikel 2.12 i förordning (EU) 2019/881.

13. *IKT-tjänst*: en IKT-tjänst enligt definitionen i artikel 2.13 i förordning (EU) 2019/881.

14. *IKT-process*: en IKT-process enligt definitionen i artikel 2.14 i förordning (EU) 2019/881.

15. *sårbarhet*: en svaghet, känslighet eller brist hos IKT-produkter eller IKT-tjänster som kan utnyttjas genom ett cyberhot.

16. *standard*: en standard enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 1025/2012 ([29]).

17. *teknisk specifikation*: en teknisk specifikation enligt definitionen i artikel 2.4 i förordning (EU) nr 1025/2012.

([29]) Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

18. *internetknutpunkt*: en nätfacilitet som möjliggör sammankoppling av mer än två oberoende nät (autonoma system), främst i syfte att underlätta utbytet av internettrafik, som tillhandahåller sammankoppling enbart för autonoma system och som varken kräver att den internettrafik som passerar mellan två deltagande autonoma system ska passera genom ett tredje autonomt system eller ändrar trafiken eller påverkar den på något annat sätt.

19. *domännamnssystem* eller *DNS*: ett hierarkiskt distribuerat namnsystem som möjliggör identifieringen av tjänster och resurser på internet, vilket gör det möjligt för slutanvändarenheter att använda internetrouting- och internetuppkopplingstjänster för att nå dessa tjänster och resurser.

20. *leverantör av DNS-tjänster*: en entitet som tillhandahåller

    a) allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare, eller

    b) auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar.

21. *registreringsenhet för toppdomäner* eller *TLD-registreringsenhet*: en enhet som har delegerats en specifik toppdomän och som ansvarar för administrationen av toppdomänen, inbegripet registreringen av domännamn under toppdomänen och den tekniska driften av toppdomänen, inbegripet drift av dess namnservrar, underhåll av dess databaser och distribution av zonfiler för toppdomänen mellan namnservrar, oberoende av huruvida någon aspekt av denna drift utförs av enheten själv eller har utkontrakterats, dock inte situationer där toppdomäner används av en registreringsenhet endast för dess eget bruk.

22. *entitet som erbjuder domännamnsregistreringstjänster*: en registrar som verkar på uppdrag av en regeringsenhet eller ett ombud för en registreringsenhet, såsom återförsäljare och leverantörer av integritetsregistreringstjänster och proxyregistreringstjänster.

23. *digital tjänst*: en tjänst enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ([30]).

24. *betrodd tjänst*: en betrodd tjänst enligt definitionen i artikel 3.16 i förordning (EU) nr 910/2014.

25. *tillhandahållare av betrodda tjänster*: en tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.19 i förordning (EU) nr 910/2014.

26. *kvalificerad betrodd tjänst*: en kvalificerad betrodd tjänst enligt definitionen i artikel 3.17 i förordning (EU) nr 910/2014.

27. *kvalificerad tillhandahållare av betrodda tjänster*: en kvalificerad tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.20 i förordning (EU) nr 910/2014.

28. *marknadsplats online*: en marknadsplats online enligt definitionen i artikel 2 n i Europaparlamentets och rådets direktiv 2005/29/EG ([31]).

29. *sökmotor*: en sökmotor enligt definitionen i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 ([32]).

30. *molntjänst*: en digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma beräkningstjänster, inbegripet när sådana resurser är distribuerade på flera platser.

([30]) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

([31]) Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder) (EUT L 149, 11.6.2005, s. 22).

([32]) Europaparlamentets och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster (EUT L 186, 11.7.2019, s. 57).

31. *datacentraltjänst*: en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll.

32. *nätverk för leverans av innehåll*: ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för, tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning.

33. *plattform för sociala nätverkstjänster*: en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, särskilt genom chattar, inlägg, videor och rekommendationer.

34. *företrädare*: en i unionen etablerad fysisk eller juridisk person som uttryckligen har utsetts att agera för en leverantör av DNS-tjänster, en registreringsenhet för toppdomäner, en entitet som tillhandahåller domännamnsregistreringstjänster, en leverantör av molntjänster, en leverantör av datacentraltjänster, en leverantör av nätverk för leverans av innehåll, driftsentreprenad, en leverantör av hanterade säkerhetstjänster, en leverantör av marknadsplatser online, av sökmotorer eller av en plattform för sociala nätverkstjänster som inte är etablerad i unionen, till vilka en behörig myndighet eller en CSIRT-enhet kan vända sig i stället för entiteten, i frågor som gäller de skyldigheter som den entiteten har enligt detta direktiv.

35. *offentlig förvaltningsentitet*: en entitet som erkänts som sådan i en medlemsstat i enlighet med nationell rätt, med undantag för rättsväsendet, parlament och centralbanker, som uppfyller följande kriterier:

    a) Den har inrättats för att tillgodose behov i det allmännas intresse och har inte industriell eller kommersiell karaktär.

    b) Den har ställning som juridisk person eller har lagstadgad rätt att agera för en annan entitet som har ställning som juridisk person.

    c) Den finansieras till största delen av staten, regionala myndigheter eller andra offentligrättsliga organ, står under administrativ tillsyn av dessa myndigheter eller organ, eller har ett förvaltnings-, lednings- eller kontrollorgan där mer än hälften av ledamöterna utses av staten, regionala myndigheter eller andra offentligrättsliga organ.

    d) Den har befogenhet att rikta administrativa eller reglerande beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.

36. *allmänt elektroniskt kommunikationsnät*: ett allmänt elektroniskt kommunikationsnät enligt definitionen i artikel 2.8 i direktiv (EU) 2018/1972.

37. *elektronisk kommunikationstjänst*: en elektronisk kommunikationstjänst enligt definitionen i artikel 2.4 i direktiv (EU) 2018/1972.

38. *entitet*: en fysisk eller juridisk person som bildats och erkänts som sådan enligt nationell rätt där den etablerats och som i eget namn får utöva rättigheter och ha skyldigheter.

39. *driftsentreprenad*: en entitet som tillhandahåller tjänster som rör installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans.

40. *leverantör av hanterade säkerhetstjänster*: en leverantör av hanterade säkerhetstjänster som utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker.

41. *forskningsorganisation*: en entitet vars främsta mål är att bedriva tillämpad forskning eller experimentell utveckling i syfte att utnyttja resultaten av denna forskning i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner.

KAPITEL II

SAMORDNADE RAMVERK FÖR CYBERSÄKERHET

Artikel 7

Nationell strategi för cybersäkerhet

1. Varje medlemsstat ska anta en nationell strategi för cybersäkerhet som tillhandahåller strategiska mål, de resurser som krävs för att uppnå dessa mål och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå. Den nationella strategin för cybersäkerhet ska inbegripa

a) mål och prioriteringar för medlemsstatens strategi för cybersäkerhet som särskilt omfattar de sektorer som avses i bilagorna I och II,

b) en styrningsram för att uppnå de mål och prioriteringar som avses i led a i denna punkt, inbegripet de politiska åtgärder som avses i punkt 2,

c) en styrningsram som klargör roller och ansvarsområden för relevanta intressenter på nationell nivå och som stöder samarbetet och samordningen på nationell nivå mellan de gemensamma myndigheterna, de gemensamma kontaktpunkterna och CSIRT-enheterna enligt detta direktiv, samt samordningen och samarbetet mellan dessa organ och behöriga myndigheter enligt sektorsspecifika unionsrättsakter,

d) en mekanism för att identifiera relevanta tillgångar och en bedömning av riskerna i den medlemsstaten,

e) en identifiering av åtgärder som säkerställer beredskap inför, svar på och återställande efter incidenter, inklusive samarbete mellan offentlig och privat sektor,

f) en förteckning över de olika myndigheter och intressenter som är involverade i genomförandet av den nationella strategin för cybersäkerhet,

g) en politisk ram för förbättrad samordning mellan de behöriga myndigheterna enligt detta direktiv och de behöriga myndigheterna enligt direktiv (EU) 2022/2557, i syfte att utbyta information om risker, cyberhot och incidenter och icke-cyberrelaterade risker, hot och incidenter och utföra tillsynsuppgifter, beroende på vad som är lämpligt,

h) en plan, med nödvändiga åtgärder, för att höja medborgarnas allmänna medvetenhet om cybersäkerhetshot.

2. Som en del av den nationella strategin för cybersäkerhet ska medlemsstaterna särskilt anta följande:

a) Riktlinjer för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av entiteter när de tillhandahåller sina tjänster.

b) Riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod.

c) Riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter enligt artikel 12.1.

d) Riktlinjer för att upprätthålla den allmänna tillgängligheten, integriteten och konfidentialiteten hos den offentliga kärnan i det öppna internet, inbegripet, i tillämpliga fall, cybersäkerheten hos undervattenskablar.

e) Riktlinjer för att främja utveckling och integrering av relevant avancerad teknik som syftar till att genomföra moderna riskhanteringsåtgärder för cybersäkerhet.

f) Riktlinjer för att främja och utveckla cybersäkerhetsutbildning, cybersäkerhetskompetens, medvetandehöjande åtgärder och forsknings- och utvecklingsinitiativ, samt vägledning om god praxis och kontroll för cyberhygien som riktar sig till medborgare, intressenter och entiteter.

g) Riktlinjer för stöd till akademiska institutioner och forskningsinstitut för att utveckla, förbättra och främja användningen av cybersäkerhetsverktyg och säker nätinfrastruktur.

h) Riktlinjer, inbegripet relevanta förfaranden och lämpliga verktyg för informationsutbyte för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan entiteter i enlighet med unionsrätten.

i) Riktlinjer som stärker cyberresiliensen och cyberhygienen hos små och medelstora företag, särskilt de som inte omfattas av detta direktiv, genom att tillhandahålla lättillgänglig vägledning och stöd för deras specifika behov.

j) Riktlinjer för att främja ett aktivt cyberskydd.

3. Medlemsstaterna ska meddela sina nationella strategier för cybersäkerhet till kommissionen inom tre månader från det att de antagits. Härvid får medlemsstaterna undanta information som rör den nationella säkerheten.

4. Medlemsstaterna ska regelbundet och minst vart femte år bedöma sina nationella strategier för cybersäkerhet på grundval av centrala resultatindikatorer och vid behov uppdatera dem. Enisa ska på medlemsstaternas begäran bistå medlemsstaterna vid utarbetandet eller uppdateringen av en nationell strategi för cybersäkerhet och centrala resultatindikatorer för bedömningen av strategin, i syfte att anpassa den till de krav och skyldigheter som fastställs i detta direktiv.

Artikel 8

Behöriga myndigheter och gemensamma kontaktpunkter

1. Varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter med ansvar för cybersäkerhet och för de tillsynsuppgifter som avses i kapitel VII (behöriga myndigheter).

2. De behöriga myndigheter som avses i punkt 1 ska övervaka genomförandet av detta direktiv på nationell nivå.

3. Varje medlemsstat ska utse eller inrätta en gemensam kontaktpunkt. Om en medlemsstat bara utser eller inrättar en behörig myndighet i enlighet med punkt 1, ska denna behöriga myndighet också vara den gemensamma kontaktpunkten i den medlemsstaten.

4. Varje gemensam kontaktpunkt ska utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater och, när det är lämpligt, kommissionen och Enisa samt ett sektorsövergripande samarbete med andra behöriga myndigheter i medlemsstaten.

5. Medlemsstaterna ska säkerställa att deras behöriga myndigheter och gemensamma kontaktpunkter har tillräckliga resurser för att på ett ändamålsenligt och effektivt sätt utföra de uppgifter de tilldelas och därigenom uppnå målen med detta direktiv.

6. Varje medlemsstat ska utan onödigt dröjsmål meddela kommissionen identiteten för den behöriga myndighet som avses i punkt 1 och den gemensamma kontaktpunkt som avses i punkt 3, dessa myndigheters uppgifter samt eventuella senare ändringar. Varje medlemsstat ska offentliggöra sin behöriga myndighets identitet. Kommissionen ska upprätta en förteckning över offentligt tillgängliga gemensamma kontaktpunkter.

Artikel 9

Nationella ramar för hantering av cybersäkerhetskriser

1. Varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter). Medlemsstaterna ska säkerställa att dessa myndigheter har tillräckliga resurser för att kunna utföra sina uppgifter på ett ändamålsenligt och effektivt sätt. Medlemsstaterna ska säkerställa samstämmighet med befintliga ramar för allmän nationell krishantering.

2. Om en medlemsstat utser eller inrättar mer än en cyberkrishanteringsmyndighet enligt punkt 1 ska den tydligt ange vilken av dessa myndigheter som ska samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser.

3. För tillämpning av detta direktiv ska varje medlemsstat identifiera vilka kapaciteter, tillgångar och förfaranden som kan användas i händelse av en kris.

4. Varje medlemsstat ska anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser där mål och villkor för hanteringen av storskaliga cybersäkerhetsincidenter och kriser fastställs. Planen ska särskilt innehålla följande:

a) Målen för nationella beredskapsåtgärder och beredskapsverksamheter.

b) Cyberkrishanteringsmyndigheternas uppgifter och ansvarsområden.

c) Cyberkrishanteringsförfaranden, inbegripet deras integrering i den allmänna nationella ramen för krishantering och kanaler för informationsutbyte.

d) Nationella beredskapsåtgärder, inbegripet övningar och utbildningsverksamhet.

e) Berörda offentliga och privata intressenter och berörd infrastruktur.

f) Nationella förfaranden och arrangemang mellan relevanta nationella myndigheter och organ för att säkerställa att medlemsstaten på ett ändamålsenligt sätt kan delta i och stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på unionsnivå.

5. Inom tre månader från det att den cyberkrishanteringsmyndighet som avses i punkt 1 har utsetts eller inrättats ska varje medlemsstat meddela kommissionen sin myndighets identitet samt alla senare ändringar. Medlemsstaterna ska till kommissionen och Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) lämna relevant information avseende kraven i punkt 4 om sina nationella planer för hanteringen av storskaliga cybersäkerhetsincidenter och kriser inom tre månader från det att dessa planer antagits. Medlemsstaterna får undanta information om och i den utsträckning det är nödvändigt för den nationella säkerheten.

Artikel 10

Enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter)

1. Varje medlemsstat ska utse eller inrätta en eller flera CSIRT-enheter. CSIRT-enheterna får utses eller inrättas inom en behörig myndighet. CSIRT-enheterna ska uppfylla kraven i artikel 11.1, ska omfatta minst de sektorer, delsektorer och typer av entiteter som avses i bilagorna I och II och ska ansvara för incidenthantering i enlighet med ett tydligt fastställt förfarande.

2. Medlemsstaterna ska säkerställa att varje CSIRT-enhet har tillräckliga resurser för att på ett ändamålsenligt sätt kunna utföra sina uppgifter enligt artikel 11.3.

3. Medlemsstaterna ska säkerställa att varje CSIRT-enhet har tillgång till en lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur för utbyte av information med väsentliga och viktiga entiteter och andra relevanta intressenter. För detta ändamål ska medlemsstaterna säkerställa att varje CSIRT-enhet bidrar till införandet av säkra verktyg för informationsutbyte.

4. CSIRT-enheterna ska samarbeta och, när det är lämpligt, utbyta relevant information i enlighet med artikel 29 med sektoriella eller sektorsövergripande grupper av väsentliga och viktiga entiteter.

5. CSIRT-enheterna ska delta i sakkunnigbedömningar som organiseras i enlighet med artikel 19.

6. Medlemsstaterna ska säkerställa ett ändamålsenligt, effektivt och säkert samarbete mellan sina CSIRT-enheter i CSIRT-nätverket.

7. CSIRT-enheter får upprätta samarbetsförbindelser med tredjeländers nationella enheter för hantering av it-säkerhetsincidenter. Som en del av sådana samarbetsförbindelser ska medlemsstaterna underlätta ett ändamålsenligt, effektivt och säkert informationsutbyte med dessa nationella enheter för hantering av it-säkerhetsincidenter i tredjeländer, med hjälp av relevanta protokoll för informationsutbyte, inbegripet Traffic Light Protocol. CSIRT-enheter får utbyta relevant information med tredjeländers nationella enheter för hantering av it-säkerhetsincidenter, inbegripet personuppgifter i enlighet med unionens dataskyddslagstiftning.

8. CSIRT-enheter får samarbeta med tredjeländers nationella enheter för hantering av it-säkerhetsincidenter eller motsvarande organ i tredjeländer, särskilt i syfte att ge dem cybersäkerhetsstöd.

9. Varje medlemsstat ska utan onödigt dröjsmål meddela kommissionen identiteten för den CSIRT-enhet som avses i punkt 1 i denna artikel och för den CSIRT-enhet som utsetts till samordnare i enlighet med artikel 12.1, deras respektive uppgifter i förhållande till de väsentliga och viktiga entiteterna samt alla senare ändringar.

10. Medlemsstaterna får begära Enisas bistånd vid inrättandet av sina CSIRT-enheter.

Artikel 11

Krav på CSIRT-enheter och deras tekniska kapacitet och uppgifter

1. CSIRT-enheter ska uppfylla följande krav:

a) CSIRT-enheterna ska säkerställa en hög nivå av tillgänglighet för sina kommunikationskanaler genom att undvika felkritiska systemdelar och ska kunna kontaktas och kontakta andra när som helst och på flera olika sätt. De ska tydligt ange kommunikationskanalerna och underrätta användargrupper och samarbetspartner om dessa.

b) CSIRT-enheternas lokaler och de informationssystem som de använder sig av ska vara belägna på säkra platser.

c) CSIRT-enheterna ska ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar, särskilt för att underlätta ändamålsenliga och effektiva överlämnanden.

d) CSIRT-enheterna ska säkerställa verksamhetens konfidentialitet och trovärdighet.

e) CSIRT-enheterna ska ha tillräckligt med personal för att säkerställa att deras tjänster är ständigt tillgängliga och de ska säkerställa att personalen har fått lämplig utbildning.

f) CSIRT-enheterna ska utrustas med redundanta system och reservlokaler för att säkerställa kontinuiteten i deras tjänster.

De ska kunna delta i internationella samarbetsnätverk.

2. Medlemsstaterna ska säkerställa att deras CSIRT-enheter tillsammans har nödvändig teknisk kapacitet för att utföra de uppgifter som avses i punkt 3. Medlemsstaterna ska säkerställa att tillräckliga resurser anslås till deras CSIRT-enheter för att säkerställa en tillräcklig personalstyrka för att göra det möjligt för CSIRT-enheterna att utveckla sin tekniska kapacitet.

3. CSIRT-enheterna ska ha följande uppgifter:

a) Övervakning och analys av cyberhot, sårbarheter och incidenter på nationell nivå och, på begäran, tillhandahållande av stöd till berörda väsentliga och viktiga entiteter avseende realtidsövervakning eller nära realtidsövervakning av deras nätverks- och informationssystem.

b) Tillhandahållande av tidiga varningar, larm, meddelanden och spridning av information till väsentliga och viktiga entiteter samt till behöriga myndigheter och andra relevanta intressenter om cyberhot, sårbarheter och incidenter, om möjligt i nära realtid.

c) Vidtagande av åtgärder till följd av incidenter och, i tillämpliga fall, tillhandahållande av stöd till de berörda väsentliga och viktiga entiteterna.

d) Insamling och analys av forensiska uppgifter och tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet när det gäller cybersäkerhet.

e) Tillhandahållande, på begäran av den väsentliga eller viktiga entiteten, av en proaktiv skanning av den berörda entitetens nätverks- och informationssystem i syfte att upptäcka sårbarheter med en potentiellt betydande påverkan.

f) Deltagande i CSIRT-nätverket och ömsesidigt bistånd i enlighet med deras kapacitet och befogenheter till andra medlemmar i CSIRT-nätverket på deras begäran.

g) I tillämpliga fall, fungera som processamordnare för den samordnade delgivningen av information om sårbarheter enligt artikel 12.1.

h) Bidrag till införandet av säkra verktyg för informationsutbyte enligt artikel 10.3.

CSIRT-enheterna får utföra en proaktiv, icke-inkräktande skanning av väsentliga och viktiga entiteters allmänt tillgängliga nätverks- och informationssystem. Sådan skanning ska utföras för att upptäcka sårbara eller osäkert konfigurerade nätverks- och informationssystem och informera de berörda enheterna. Sådan skanning får inte ha någon negativ inverkan på hur entiteternas tjänster fungerar.

När CSIRT-enheterna utför de uppgifter som avses i första stycket får de prioritera särskilda uppgifter på grundval av en riskbaserad metod.

4. CSIRT-enheterna ska upprätta samarbetsförbindelser med relevanta intressenter inom den privata sektorn i syfte att uppnå målen för detta direktiv.

5. För att underlätta det samarbete som avses i punkt 4 ska CSIRT-enheterna främja antagande och användning av gemensamma eller standardiserade metoder, klassificeringssystem och taxonomier när det gäller

a) förfaranden för incidenthantering,

b) krishantering, och

c) samordnad delgivning av information om sårbarheter enligt artikel 12.1.

Artikel 12

Samordnad delgivning av information om sårbarheter och en europeisk sårbarhetsdatabas

1. Varje medlemsstat ska utse en av sina CSIRT-enheter till samordnare för den samordnade delgivningen av informationen om sårbarheter. Den CSIRT-enhet som utsetts till samordnare ska fungera som betrodd mellanhand och vid behov underlätta interaktionen mellan en fysisk eller juridisk person som rapporterar en sårbarhet och tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna, på begäran av endera parten. Den CSIRT-enhet som utsetts till samordnare ska bland annat

a) identifiera och kontakta de berörda entiteterna,

b) stödja de fysiska eller juridiska personer som rapporterar en sårbarhet, och

c) förhandla om tidsramar för delgivning av information och hantera sårbarheter som påverkar flera entiteter.

Medlemsstaterna ska säkerställa att fysiska eller juridiska personer kan, anonymt om de så begär, rapportera en sårbarhet till den CSIRT-enhet som utsetts till samordnare. Den CSIRT-enhet som utsetts till samordnare ska säkerställa att skyndsamma uppföljningsåtgärder vidtas med avseende på den rapporterade sårbarheten och ska säkerställa anonymiteten för den fysiska eller juridiska person som rapporterar sårbarheten. Om en rapporterad sårbarhet kan ha en betydande påverkan på entiteter i fler än en medlemsstat, ska den CSIRT-enhet som utsetts till samordnare i varje berörd medlemsstat, när det är lämpligt, samarbeta med andra CSIRT-enheter som utsetts till samordnare inom CSIRT-nätverket.

2. Enisa ska, efter samråd med samarbetsgruppen, utveckla och underhålla en europeisk sårbarhetsdatabas. I detta syfte ska Enisa inrätta och underhålla lämpliga informationssystem, riktlinjer och förfaranden och anta nödvändiga tekniska och organisatoriska åtgärder för att säkerställa den europeiska sårbarhetsdatabasens säkerhet och integritet, särskilt för att göra det möjligt för entiteter, oberoende om de omfattas av tillämpningsområdet för detta direktiv, och deras leverantörer av nätverks- och informationssystem, att på frivillig basis lämna information om och registrera allmänt kända sårbarheter hos IKT-produkter eller IKT-tjänster. Alla intressenter ska få tillgång till informationen om de sårbarheter som finns i den europeiska sårbarhetsdatabasen. Databasen ska innehålla

a) information som beskriver sårbarheten,

b) den berörda IKT-produkten eller IKT-tjänsten och hur allvarlig sårbarheten är med tanke på de omständigheter under vilka den kan utnyttjas,

c) tillgången till relaterade programfixar och, i avsaknad av tillgängliga programfixar, vägledning som tillhandahållits av behöriga myndigheter eller CSIRT-enheter riktad till användare av sårbara IKT-produkter och IKT-tjänster om hur riskerna med meddelade sårbarheter kan begränsas.

Artikel 13

Samarbete på nationell nivå

1. Om de är separata ska de behöriga myndigheterna, den gemensamma kontaktpunkten och CSIRT-enheterna i en och samma medlemsstat samarbeta sinsemellan när det gäller fullgörandet av skyldigheter enligt detta direktiv.

2. Medlemsstaterna ska säkerställa att deras CSIRT-enheter eller, i tillämpliga fall, deras behöriga myndigheter, mottar underrättelser om betydande incidenter enligt artikel 23, och incidenter, cyberhot och tillbud enligt artikel 30.

3. Medlemsstaterna ska säkerställa att deras CSIRT-enheter eller, i tillämpliga fall, deras behöriga myndigheter informerar sina gemensamma kontaktpunkter om de underrättelser om incidenter, cyberhot och tillbud som lämnas in i enlighet med detta direktiv.

4. För att säkerställa att de behöriga myndigheternas, de gemensamma kontaktpunkternas och CSIRT-enheternas uppgifter och skyldigheter utförs på ett effektivt sätt, ska medlemsstaterna, i den utsträckning det är möjligt, säkerställa ett lämpligt samarbete mellan dessa organ och brottsbekämpande myndigheter, dataskyddsmyndigheter, nationella myndigheter enligt förordningarna (EG) nr 300/2008 och (EU) 2018/1139, tillsynsorganen enligt förordning (EU) nr 910/2014, behöriga myndigheter enligt förordning (EU) 2022/2554, nationella regleringsmyndigheter enligt direktiv (EU) 2018/1972, behöriga myndigheter enligt direktiv (EU) 2022/2557 samt behöriga myndigheter enligt andra sektorsspecifika unionsrättsakter, i den medlemsstaten.

5. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv och deras behöriga myndigheter enligt direktiv (EU) 2022/2557 regelbundet samarbetar och utbyter information avseende identifieringen av kritiska entiteter, om risker, cyberhot och incidenter samt icke-cyberrelaterade risker, hot och incidenter som berör väsentliga entiteter som identifierats som kritiska i enlighet med direktiv (EU) 2022/2557, samt om de åtgärder som vidtagits till följd av sådana risker, hot och incidenter. Medlemsstaterna ska också säkerställa att deras behöriga myndigheter enligt detta direktiv och deras behöriga myndigheter enligt förordning (EU) nr 910/2014, förordning (EU) 2022/2554 och direktiv (EU) 2018/1972 regelbundet utbyter relevant information, även när det gäller relevanta incidenter och cyberhot.

6. Medlemsstaterna ska förenkla rapporteringen med tekniska medel för de underrättelser som avses i artiklarna 23 och 30.

KAPITEL III

SAMARBETE PÅ UNIONSNIVÅ OCH PÅ INTERNATIONELL NIVÅ

Artikel 14

Samarbetsgrupp

1. För att stödja och underlätta strategiskt samarbete och informationsutbyte mellan medlemsstaterna samt stärka förtroende och tillit inrättas härmed en samarbetsgrupp.

2. Samarbetsgruppen ska utföra sina uppgifter på grundval av de tvååriga arbetsprogram som avses i punkt 7.

3. Samarbetsgruppen ska bestå av företrädare för medlemsstater, kommissionen och Enisa. Europeiska utrikestjänsten ska delta som observatör i samarbetsgruppens verksamhet. De europeiska tillsynsmyndigheterna och de behöriga myndigheterna i enlighet med förordning (EU) 2022/2554 får delta i samarbetsgruppens verksamhet i enlighet med artikel 47.1 i den förordningen.

När så är lämpligt får samarbetsgruppen bjuda in Europaparlamentet och företrädare för relevanta intressenter att delta i arbetet.

Kommissionen ska tillhandahålla sekretariatet.

4. Samarbetsgruppen ska ha följande uppgifter:

a) Tillhandahålla vägledning till behöriga myndigheter angående införlivande och genomförande av detta direktiv.

b) Tillhandahålla vägledning till behöriga myndigheter angående utarbetande och genomförande av strategier för den samordnade delgivningen av information om sårbarheter som avses i artikel 7.2 c.

c) Utbyte av bästa praxis och information i fråga om genomförandet av detta direktiv, bland annat när det gäller cyberhot, incidenter, sårbarheter, tillbud, initiativ för att öka medvetenheten, utbildning, övningar och kompetens, kapacitetsuppbyggnad, standarder och tekniska specifikationer, samt identifiering av väsentliga och viktiga entiteter i enlighet med artikel 2.2 b–e.

d) Utbyta råd och samarbeta med kommissionen om framväxande politiska initiativ för cybersäkerhet samt om den övergripande förenligheten mellan sektorsspecifika cybersäkerhetskrav.

e) Utbyta råd och samarbeta med kommissionen om utkast till delegerade akter eller genomförandeakter som antas i enlighet med detta direktiv.

f) Utbyta bästa praxis och information med relevanta institutioner, organ och byråer på unionsnivå.

g) Diskutera genomförandet av sektorsspecifika unionsrättsakter som innehåller bestämmelser om cybersäkerhet.

h) När så är lämpligt, diskutera de rapporter från sakkunnigbedömningar som avses i artikel 19.9 samt utarbeta slutsatser och rekommendationer.

i) Genomföra samordnade säkerhetsriskbedömningar av kritiska leveranskedjor i enlighet med artikel 22.1.

j) Diskutera fall av ömsesidigt bistånd, inbegripet erfarenheter och resultat av sådan gränsöverskridande gemensam tillsynsverksamhet som avses i artikel 37.

k) På begäran av en eller flera berörda medlemsstater, diskutera särskilda begäranden om ömsesidigt bistånd som avses i artikel 37.

l) Tillhandahålla strategisk vägledning till CSIRT-nätverket och EU-CyCLONe om specifika framväxande frågor.

m) Utbyta åsikter om politiken för uppföljningsåtgärder efter storskaliga cybersäkerhetsincidenter och kriser på grundval av lärdomarna från CSIRT-nätverket och EU-CyCLONe.

n) Bidra till cybersäkerhetskapaciteten i hela unionen genom att underlätta utbytet av nationella tjänstemän i form av ett kapacitetsuppbyggnadsprogram som inbegriper personal från behöriga myndigheter eller CSIRT-enheter.

o) Anordna regelbundna gemensamma möten med relevanta privata intressenter från hela unionen för att diskutera samarbetsgruppens verksamhet och inhämta synpunkter på framväxande politiska frågor.

p) Diskutera det arbete som utförts i samband med cybersäkerhetsövningar, inbegripet det arbete som utförs av Enisa.

q) Fastställa metoder och organisatoriska aspekter för de sakkunnigbedömningar som avses i artikel 19.1 samt fastställa en självbedömningsmetod för medlemsstaterna i enlighet med artikel 19.5, med bistånd av kommissionen och Enisa, och, i samarbete med kommissionen och Enisa, utarbeta uppförandekoder som ligger till grund för de utsedda cyberssäkerhetsexperternas arbetsmetoder i enlighet med artikel 19.6.

r) Utarbeta rapporter för den översyn som avses i artikel 40 om de erfarenheter som förvärvats på strategisk nivå och från sakkunnigbedömningar.

s) Regelbundet diskutera och genomföra en bedömning av läget när det gäller cyberhot eller cyberincidenter, såsom utpressningsprogram.

Samarbetsgruppen ska överlämna de rapporter som avses i första stycket led r till kommissionen, Europaparlamentet och rådet.

5. Medlemsstaterna ska säkerställa att deras företrädare i samarbetsgruppen samarbetar på ett ändamålsenligt, effektivt och säkert sätt.

6. Samarbetsgruppen får begära en teknisk rapport från CSIRT-nätverket om utvalda frågor.

7. Samarbetsgruppen ska senast den 1 februari 2024 och därefter vartannat år utarbeta ett arbetsprogram för de åtgärder som ska vidtas för att genomföra dess mål och uppgifter.

8. Kommissionen får anta genomförandeakter i vilka de förfaranden som krävs för samarbetsgruppens verksamhet fastställs.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Kommissionen ska utbyta råd och samarbeta med samarbetsgruppen om de utkast till genomförandeakter som avses i första stycket i denna punkt i enlighet med punkt 4 e.

9. Samarbetsgruppen ska regelbundet och under alla omständigheter minst en gång om året sammanträda med den grupp för kritiska entiteters motståndskraft som inrättats enligt direktiv (EU) 2022/2557, för att främja och underlätta strategiskt samarbete och informationsutbyte.

Artikel 15

CSIRT-nätverk

1. För att bidra till utvecklingen av förtroende och tillit och för att främja ett snabbt och ändamålsenligt operativt samarbete mellan medlemsstaterna inrättas härmed ett nätverk för nationella CSIRT-enheter.

2. CSIRT-nätverket ska bestå av företrädare för de CSIRT-enheter som utsetts eller inrättats i enlighet med artikel 10 och incidenthanteringsorganisationen för unionens institutioner, organ och byråer (Cert-EU). Kommissionen ska som observatör delta i CSIRT-nätverket. Enisa ska tillhandahålla sekretariatet och aktivt bidra med stöd till samarbetet mellan CSIRT-enheterna.

3. CSIRT-nätverket ska ha följande uppgifter:

a) Utbyta information om CSIRT-enheternas kapacitet.

b) Underlätta delning, överföring och utbyte av teknik och relevanta åtgärder, strategier, verktyg, processer, bästa praxis och ramar mellan CSIRT-enheterna.

c) Utbyta relevant information om incidenter, tillbud, cyberhot, risker och sårbarheter.

d) Utbyta information med avseende på publikationer och rekommendationer om cybersäkerhet.

e) Säkerställa interoperabilitet när det gäller specifikationer och protokoll för informationsutbyte.

f) På begäran av en medlem av CSIRT-nätverket som potentiellt berörs av en incident, utbyta och diskutera information om den incidenten och relaterade cyberhot, risker och sårbarheter.

g) På begäran av en medlem av CSIRT-nätverket, diskutera och om möjligt genomföra en samordnad åtgärd till följd av en incident som har identifierats inom den medlemsstatens jurisdiktion.

h) Ge medlemsstaterna stöd när det gäller att hantera gränsöverskridande incidenter i enlighet med detta direktiv.

i) Samarbeta och utbyta bästa praxis med och ge stöd till CSIRT-enheter som utsetts till samordnare i enlighet med artikel 12.1 när det gäller hanteringen av samordnad information om sårbarheter som kan ha en betydande påverkan på entiteter i mer än en medlemsstat.

j) Diskutera och identifiera ytterligare former av operativt samarbete, inbegripet när det gäller

   i) kategorier av cyberhot och incidenter,

   ii) tidiga varningar,

   iii) ömsesidigt bistånd,

   iv) principer och metoder för samordning i samband med åtgärder mot gränsöverskridande risker och incidenter,

   v) bidrag till den nationella plan för hantering av storskaliga cybersäkerhetsincidenter och kriser som avses i artikel 9.4 på begäran av en medlemsstat.

k) Informera samarbetsgruppen om sin verksamhet och om ytterligare former av operativt samarbete som diskuteras enligt led j och vid behov begära vägledning i detta avseende.

l) Utvärdera cybersäkerhetsövningar, bland annat sådana som anordnas av Enisa.

m) På begäran av en enskild CSIRT-enhet diskutera den enhetens kapacitet och beredskap.

n) Samarbeta och utbyta information med säkerhetscentrum (SOC) på regional nivå och unionsnivå, för att förbättra den gemensamma situationsmedvetenheten om incidenter och cyberhot i hela unionen.

o) När så är lämpligt, diskutera de rapporter från sakkunnigbedömningar som avses i artikel 19.9.

p) Tillhandahålla riktlinjer för att underlätta en mer enhetlig operativ praxis när det gäller tillämpningen av bestämmelserna i denna artikel om operativt samarbete.

4. CSIRT-nätverket ska senast den 17 januari 2025 och därefter vartannat år, i samband med den översyn som avses i artikel 40, bedöma de framsteg som gjorts när det gäller det operativa samarbetet och anta en rapport. Rapporten ska särskilt innehålla slutsatser och rekommendationer om resultaten av de sakkunnigbedömningar som avses i artikel 19, som utförs med avseende på de nationella CSIRT-enheterna. Rapporten ska lämnas till samarbetsgruppen.

5. CSIRT-nätverket ska anta sin arbetsordning.

6. CSIRT-nätverket och EU-CyCLONe ska komma överens om förfaranden och samarbeta på grundval av dessa.

Artikel 16

Det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe)

1. EU-CyCLONe inrättas för att stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på operativ nivå och säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer.

2. EU-CyCLONe ska bestå av företrädare för medlemsstaternas myndigheter för hantering av cyberkriser samt, i fall där en potentiell eller pågående storskalig cybersäkerhetsincident har eller sannolikt kommer att ha en betydande påverkan på tjänster och verksamhet som omfattas av detta direktiv, kommissionen. I andra fall ska kommissionen delta som observatör i arbetet inom EU-CyCLONe.

Enisa ska tillhandahålla EU-CyCLONes sekretariat och stödja ett säkert informationsutbyte samt tillhandahålla nödvändiga verktyg för att stödja samarbete mellan medlemsstaterna så att ett säkert informationsutbyte säkerställs.

När så är lämpligt får EU-CyCLONe bjuda in företrädare för relevanta intressenter att delta i arbetet som observatörer.

3. EU-CyCLONe ska ha följande uppgifter:

a) Öka beredskapen för hantering av storskaliga cybersäkerhetsincidenter och kriser.

b) Utveckla en gemensam situationsmedvetenhet om storskaliga cybersäkerhetsincidenter och kriser.

c) Bedöma konsekvenserna och effekterna av relevanta storskaliga cybersäkerhetsincidenter och kriser och föreslå möjliga begränsningsåtgärder.

d) Samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser och ge stöd till beslutsfattande på politisk nivå i samband med sådana incidenter och kriser.

e) På begäran av en berörd medlemsstat, diskutera de nationella planer för hantering av storskaliga nationella cybersäkerhetsincidenter och kriser som avses i artikel 9.4.

4. EU-CyCLONe ska anta sin arbetsordning.

5. EU-CyCLONe ska regelbundet rapportera till samarbetsgruppen om hanteringen av storskaliga cybersäkerhetsincidenter och kriser, samt om trender, med särskild inriktning på deras inverkan på väsentliga och viktiga entiteter.

6. EU-CyCLONe ska samarbeta med CSIRT-nätverket på grundval av överenskomna förfaranden i enlighet med artikel 15.6.

7. Senast den 17 juli 2024 och därefter var 18:e månad ska EU-CyCLONe lägga fram en rapport för Europaparlamentet och rådet med en bedömning av sitt arbete.

Artikel 17

Internationellt samarbete

Unionen får, när det är lämpligt, ingå internationella avtal, i enlighet med artikel 218 i EUF-fördraget, med tredjeländer eller internationella organisationer, och därvid tillåta och organisera deras deltagande i vissa av samarbetsgruppens, CSIRT-nätverkets och EU-CyCLONes verksamheter. Sådana avtal ska vara förenliga med unionens dataskyddslagstiftning.

Artikel 18

Rapport om cybersäkerhetssituationen i unionen

1. Enisa ska, i samarbete med kommissionen och samarbetsgruppen, vartannat år anta en rapport om cybersäkerhetssituationen i unionen samt lämna in den till och lägga fram den för Europaparlamentet. Rapporten ska, bland annat, göras tillgänglig i maskinläsbart format och innehålla följande:

a) En riskbedömning av cybersäkerheten på unionsnivå, med beaktande av cyberhotbilden.

b) En bedömning av utvecklingen av cybersäkerhetskapaciteten i den offentliga och privata sektorn i hela unionen.

c) En bedömning av den allmänna nivån av cybersäkerhetsmedvetenhet och cyberhygien bland medborgare och entiteter, inbegripet små och medelstora företag.

d) En aggregerad bedömning av resultaten av de sakkunnigbedömningar som avses i artikel 19.

e) En aggregerad bedömning av nivån på cybersäkerhetskapaciteten och cybersäkerhetsresurserna i hela unionen, inbegripet på sektorsnivå, samt av i vilken utsträckning medlemsstaternas nationella cybersäkerhetsstrategier är anpassade till varandra.

2. Rapporten ska innehålla särskilda politiska rekommendationer, i syfte att åtgärda brister och höja cybersäkerhetsnivån i hela unionen, och en sammanfattning av resultaten för den aktuella perioden från de tekniska lägesrapporter om cybersäkerheten i EU som Enisa utarbetat i enlighet med artikel 7.6 i förordning (EU) 2019/881.

3. Enisa ska, i samarbete med kommissionen, samarbetsgruppen och CSIRT-nätverket, utarbeta metoderna, bland annat de relevanta variablerna, såsom kvalitativa och kvantitativa indikatorer, för den aggregerade bedömning som avses i punkt 1 e.

Artikel 19

Sakkunnigbedömningar

1. Samarbetsgruppen ska med bistånd av kommissionen och Enisa och, i relevanta fall, av CSIRT-nätverket, och senast den 17 januari 2025, fastställa metoden för och de organisatoriska aspekterna av sakkunnigbedömningar i syfte att dra lärdom av delade erfarenheter, stärka det ömsesidiga förtroendet, uppnå en hög gemensam cybersäkerhetsnivå samt stärka medlemsstaternas nödvändiga cybersäkerhetskapacitet och cybersäkerhetsriktlinjer för att genomföra detta direktiv. Deltagandet i sakkunnigbedömningar är frivilligt. Sakkunnigbedömningarna ska utföras av cybersäkerhetsexperter. Experterna för cybersäkerhet ska utses av minst två medlemsstater, andra än den medlemsstat som granskas.

Sakkunnigbedömningarna ska omfatta åtminstone ett av följande:

a) Genomförandenivån för de riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som fastställs i artiklarna 21 och 23.

b) Kapacitetsnivån, inbegripet tillgängliga ekonomiska, tekniska och mänskliga resurser, och effektiviteten i de behöriga myndigheternas arbete.

c) CSIRT-enheternas operativa kapacitet.

d) Genomförandenivån för det ömsesidiga bistånd som avses i artikel 37.

e) Genomförandenivån för de arrangemang för informationsutbyte om cybersäkerhet som avses i artikel 29.

f) Särskilda frågor av gränsöverskridande eller sektorsövergripande karaktär.

2. Den metod som avses i punkt 1 ska innefatta objektiva, icke-diskriminerande, rättvisa och transparenta kriterier på grundval av vilka medlemsstaterna utser de cybersäkerhetsexperter som ska få utföra sakkunnigbedömningarna. Kommissionen och Enisa ska delta som observatörer i sakkunnigbedömningarna.

3. Medlemsstaterna får identifiera sådana särskilda frågor som avses i punkt 1 f, med avseende på en sakkunnigbedömning.

4. Innan en sakkunnigbedömning som avses i punkt 1 inleds ska medlemsstaterna meddela de deltagande medlemsstaterna omfattningen av sakkunnigbedömningen, inbegripet de särskilda frågor som identifierats i enlighet med punkt 3.

5. Innan sakkunnigbedömningen inleds får medlemsstaterna genomföra en självbedömning av de granskade aspekterna och tillhandahålla denna självbedömning till de utsedda experterna för cybersäkerhet. Samarbetsgruppen ska, med bistånd av kommissionen och Enisa, fastställa metoden för medlemsstaternas självbedömning.

6. Sakkunnigbedömningar ska inbegripa fysiska eller virtuella besök på plats och distansbaserade informationsutbyten. Med hänsyn till principen om gott samarbete ska den medlemsstat som är föremål för sakkunnigbedömningen förse de utsedda cybersäkerhetsexperterna med den information som krävs för bedömningen, utan att det påverkar unionsrätten eller nationell rätt om skydd av konfidentiella eller säkerhetsskyddsklassificerade uppgifter samt skyddet av väsentliga statliga funktioner, såsom nationell säkerhet. Samarbetsgruppen ska, i samarbete med kommissionen och Enisa, utarbeta lämpliga uppförandekoder till stöd för de utsedda cybersäkerhetsexperternas arbetsmetoder. All information som erhålls genom sakkunnigbedömningen får endast användas för dess ändamål. De cybersäkerhetsexperter som deltar i sakkunnigbedömningen får inte lämna ut känslig eller konfidentiell information som erhållits under sakkunnigbedömningen till någon tredje part.

7. När aspekter har varit föremål för en sakkunnigbedömning i en medlemsstat ska de inte bli föremål för ytterligare sakkunnigbedömning i den medlemsstaten under de två år som följer på slutförandet av sakkunnigbedömningen, om inte annat begärs av medlemsstaten eller beslutas efter ett förslag från samarbetsgruppen.

8. Medlemsstaterna ska säkerställa att de andra medlemsstaterna, samarbetsgruppen, kommissionen och Enisa får information om alla risker för intressekonflikter som rör utsedda cybersäkerhetsexperter innan sakkunnigbedömningen inleds. Den medlemsstat som är föremål för sakkunnigbedömningen får invända mot utnämningen av särskilda cybersäkerhetsexperter av vederbörligen motiverade skäl som meddelas den medlemsstat som utser dessa.

9. Cybersäkerhetsexperter som deltar i sakkunnigbedömningar ska utarbeta rapporter om resultat och slutsatser av dessa. De medlemsstater som är föremål för en sakkunnigbedömning får lämna synpunkter på de utkast till rapporter som berör dem och sådana synpunkter ska bifogas rapporterna. Rapporterna ska innefatta rekommendationer som möjliggör förbättringar när det gäller de aspekter som ingår i sakkunnigbedömningen. Rapporterna ska i relevanta fall överlämnas till samarbetsgruppen och CSIRT-nätverket. En medlemsstat som är föremål för sakkunnigbedömningen får besluta att offentliggöra sin rapport eller en redigerad version av den.

KAPITEL IV

ÅTGÄRDER FÖR RISKHANTERING OCH RAPPORTERINGSKRAV FÖR CYBERSÄKERHET

Artikel 20

Styrning

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteters ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för entiteternas överträdelser av den artikeln.

Tillämpningen av denna punkt påverkar inte nationell rätt när det gäller de ansvarsregler som är tillämpliga på offentliga institutioner, samt ansvaret för statligt anställda och valda eller utnämnda tjänstepersoner.

2. Medlemsstaterna ska säkerställa att medlemmarna i väsentliga och viktiga entiteters ledningsorgan är skyldiga att genomgå utbildning, och ska uppmuntra väsentliga och viktiga entiteter att regelbundet erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av entiteten.

Artikel 21

Riskhanteringsåtgärder för cybersäkerhet

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster.

Med beaktande av de senaste, och i tillämpliga fall, relevanta europeiska och internationella standarder samt genomförandekostnaderna, ska de åtgärder som avses i första stycket säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken. Vid bedömningen av dessa åtgärders proportionalitet ska vederbörlig hänsyn tas till entitetens grad av riskexponering, entitetens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser.

2. De åtgärder som avses i punkt 1 ska baseras på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö från incidenter, och ska minst inbegripa

a) strategier för riskanalys och informationssystemens säkerhet,

b) incidenthantering,

c) driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering,

d) säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess direkta leverantörer eller tjänsteleverantörer,

e) säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation,

f) strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,

g) grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,

h) strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering,

i) personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning,

j) användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.

3. Medlemsstaterna ska säkerställa att entiteter, när de överväger lämpliga åtgärder enligt punkt 2 d i denna artikel, beaktar de sårbarheter som är specifika för varje direktleverantör och tjänsteleverantör och den övergripande kvaliteten på deras leverantörers och tjänsteleverantörers produkter och cybersäkerhetspraxis, inbegripet deras förfaranden för säker utveckling. Medlemsstaterna ska också säkerställa att entiteter, när de överväger lämpliga åtgärder enligt den punkten är skyldiga att beakta resultatet av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor som utförs i enlighet med artikel 22.1.

4. Medlemsstaterna ska säkerställa att en entitet som finner att den inte följer de åtgärder som föreskrivs i punkt 2 utan onödigt dröjsmål vidtar alla nödvändiga, lämpliga och proportionella korrigerande åtgärder.

5. Senast den 17 oktober 2024 ska kommissionen anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna för de åtgärder som avses i punkt 2 med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer och för plattformar för sociala nätverkstjänster samt kvalificerade tillhandahållare av betrodda tjänster.

Kommissionen får anta genomförandeakter för att fastställa tekniska och metodologiska krav samt, vid behov, sektorskrav för de åtgärder som avses i punkt 2 med avseende på andra väsentliga och viktiga entiteter än de som avses i första stycket i denna punkt.

När kommissionen utarbetar de genomförandeakter som avses i första och andra stycket i denna punkt ska den i största möjliga utsträckning följa europeiska och internationella standarder samt relevanta tekniska specifikationer. Kommissionen ska utbyta råd och samarbeta med samarbetsgruppen och Enisa om de utkast till genomförandeakter som avses i artikel 14.4 e.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 22

Samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor

1. Samarbetsgruppen får, i samarbete med kommissionen och Enisa, utföra samordnade säkerhetsriskbedömningar av specifika kritiska leveranskedjor för IKT-tjänster, IKT-system eller IKT-produkter, med beaktande av tekniska och, i relevanta fall, icke-tekniska riskfaktorer.

2. Kommissionen ska, efter samråd med samarbetsgruppen och Enisa och, vid behov, relevanta intressenter, identifiera de specifika kritiska IKT-tjänster, IKT-system eller IKT-produkter som kan bli föremål för den samordnade säkerhetsriskbedömning som avses i punkt 1.

Artikel 23

Rapporteringsskyldigheter

1. Varje medlemsstat ska säkerställa att väsentliga och viktiga entiteter utan onödigt dröjsmål underrättar sin CSIRT-enhet eller, i tillämpliga fall, sin behöriga myndighet i enlighet med punkt 4 om alla incidenter som har en betydande inverkan på tillhandahållandet av deras tjänster enligt punkt 3 (betydande incident). När så är lämpligt ska berörda entiteter utan onödigt dröjsmål underrätta mottagarna av deras tjänster om betydande incidenter som sannolikt inverkar negativt på tillhandahållandet av de tjänsterna. Varje medlemsstat ska säkerställa att dessa entiteter bland annat rapporterar information som gör det möjligt för CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten att fastställa incidentens eventuella gränsöverskridande verkningar. Själva underrättelsen ska inte medföra ökat ansvar för den underrättande entiteten.

Om de berörda entiteterna underrättar den behöriga myndigheten om en betydande incident enligt första stycket ska medlemsstaten säkerställa att den behöriga myndigheten vidarebefordrar underrättelsen till CSIRT-enheten vid mottagandet.

Vid en gränsöverskridande eller sektorsövergripande betydande incident ska medlemsstaterna säkerställa att deras gemensamma kontaktpunkter i god tid förses med relevant information som meddelats i enlighet med punkt 4.

2. I tillämpliga fall ska medlemsstaterna säkerställa att väsentliga och viktiga entiteter utan onödigt dröjsmål underrättar de mottagare av deras tjänster som kan påverkas av ett betydande cyberhot om eventuella åtgärder eller avhjälpande arrangemang som dessa mottagare kan vidta som svar på hotet. När så är lämpligt ska entiteterna också informera dessa mottagare om själva det betydande cyberhotet.

3. En incident ska anses vara betydande om

a) den har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten,

b) den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

4. När det gäller det underrättelseförfarande som avses i punkt 1 ska medlemsstaterna säkerställa att de berörda entiteterna lämnar följande till CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten:

a) Utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande incidenten, en tidig varning som i tillämpliga fall ska ange om den betydande incidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller kan ha gränsöverskridande verkningar.

b) Utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande incidenten, en incidentanmälan som, i tillämpliga fall, ska uppdatera den information som avses i led a och ange en inledande bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer.

c) På begäran av en CSIRT-enhet eller, i tillämpliga fall, den behöriga myndigheten, en delrapport om relevanta statusuppdateringar.

d) Senast en månad efter inlämningen av den incidentanmälan som avses i led b, en slutrapport som ska innehålla följande:

   i) En detaljerad beskrivning av incidenten, inbegripet dess allvarlighetsgrad och konsekvenser.

   ii) Den typ av hot eller grundorsak som sannolikt har utlöst incidenten.

   iii) Tillämpade och pågående begränsande åtgärder.

   iv) I tillämpliga fall, incidentens gränsöverskridande verkningar.

e) I händelse av en pågående incident vid tidpunkten för inlämnandet av den slutrapport som avses i led d ska medlemsstaterna säkerställa att de berörda entiteterna tillhandahåller en lägesrapport vid den tidpunkten och en slutrapport inom en månad efter det att de hanterat incidenten.

Genom undantag från första stycket b ska en tillhandahållare av betrodda tjänster, när det gäller betydande incidenter som påverkar tillhandahållandet av de betrodda tjänsterna, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande incidenten, underrätta CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten.

5. CSIRT-enheten eller den behöriga myndigheten ska utan onödigt dröjsmål och om möjligt inom 24 timmar från mottagandet av den tidiga varning som avses i punkt 4 a lämna ett svar till den underrättande entiteten, inbegripet initial återkoppling om den betydande incidenten och, på entitetens begäran, vägledning eller operativa råd om genomförandet av möjliga begränsande åtgärder. Om CSIRT-enheten inte är den ursprungliga mottagaren av den underrättelse som avses i punkt 1 ska vägledningen tillhandahållas av den behöriga myndigheten i samarbete med CSIRT-enheten. CSIRT-enheten ska tillhandahålla ytterligare tekniskt stöd om den berörda entiteten begär det. Om den betydande incidenten misstänks vara av brottslig art ska CSIRT-enheten eller den behöriga myndigheten också tillhandahålla vägledning om rapporteringen av den betydande incidenten till de brottsbekämpande myndigheterna.

6. När så är lämpligt, och särskilt om den betydande incidenten berör två eller flera medlemsstater, ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten utan onödigt dröjsmål informera andra berörda medlemsstater och Enisa om den betydande incidenten. Sådan information ska åtminstone inbegripa den typ av information som mottagits i enlighet med punkt 4. Därvid ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten, i enlighet med unionsrätten eller nationell rätt, bevara entitetens säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet.

7. Om allmänhetens medvetenhet är nödvändig för att förhindra en betydande incident eller för att hantera en pågående betydande incident, eller om information om den betydande incidenten på annat sätt ligger i allmänhetens intresse, får en medlemsstats CSIRT-enhet eller, i tillämpliga fall, dess behöriga myndighet och, om det är lämpligt, CSIRT-enheterna eller de behöriga myndigheterna i andra berörda medlemsstater, efter samråd med den berörda entiteten, informera allmänheten om den betydande incidenten eller ålägga entiteten att göra detta.

8. På begäran av CSIRT-enheten eller den behöriga myndigheten ska den gemensamma kontaktpunkten vidarebefordra underrättelser som mottagits i enlighet med punkt 1 till de gemensamma kontaktpunkterna i andra berörda medlemsstater.

9. Den gemensamma kontaktpunkten ska var tredje månad lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud om vilket underrättats i enlighet med punkt 1 i denna artikel och med artikel 30. För att bidra till att jämförbar information lämnas får Enisa anta teknisk vägledning om parametrarna för den information som ska tas med i den sammanfattande rapporten. Enisa ska var sjätte månad informera samarbetsgruppen och CSIRT-nätverket om sina slutsatser om de mottagna anmälningarna.

10. CSIRT-enheterna eller, i tillämpliga fall, de behöriga myndigheterna ska förse de behöriga myndigheterna enligt direktiv (EU) 2022/2557 med information om betydande incidenter, incidenter, cyberhot och tillbud om vilket underrättats i enlighet med punkt 1 i denna artikel och med artikel 30 av entiteter som identifierats som kritiska i enlighet med direktiv (EU) 2022/2557.

11. Kommissionen får anta genomförandeakter som närmare anger typen av information i och formatet och förfarandet för underrättelser som lämnas i enlighet med punkt 1 i denna artikel och med artikel 30 samt för underrättelser som lämnas i enlighet med punkt 2 i den här artikeln.

Senast den 17 oktober 2024 ska kommissionen, med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer eller av plattformar för sociala nätverkstjänster, anta genomförandeakter som närmare anger i vilka fall en incident ska anses vara betydande enligt punkt 3. Kommissionen får anta sådana genomförandeakter med avseende på andra väsentliga och viktiga entiteter.

Kommissionen ska utbyta råd och samarbeta med samarbetsgruppen om de utkast till genomförandeakter som avses i första och andra stycket i denna punkt i enlighet med artikel 14.4 e.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 24

Användning av europeiska ordningar för cybersäkerhetscertifiering

1. För att visa att vissa krav enligt artikel 21 är uppfyllda får medlemsstaterna ålägga väsentliga och viktiga entiteter att använda särskilda IKT-produkter, IKT-tjänster och IKT-processer, som har utvecklats av den väsentliga eller viktiga entiteten eller upphandlats från tredje parter, som är certifierade enligt europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 i förordning (EU) 2019/881. Medlemsstaterna ska dessutom uppmuntra väsentliga och viktiga entiteter att använda kvalificerade betrodda tjänster.

2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 38 för att komplettera detta direktiv genom att ange vilka kategorier av väsentliga eller viktiga entiteter som ska vara skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhålla ett certifikat enligt en europeisk ordning för cybersäkerhetscertifiering som har antagits enligt artikel 49 i förordning (EU) 2019/881. Dessa delegerade akter ska antas om det har fastställts att cybersäkerhetsnivån är otillräcklig och ska omfatta en genomförandeperiod.

Innan kommissionen antar sådana delegerade akter ska den göra en konsekvensbedömning och genomföra samråd i enlighet med artikel 56 i förordning (EU) 2019/881.

3. I fall där det inte finns en lämplig europeisk ordning för cybersäkerhetscertifiering med avseende på tillämpningen av punkt 2 i denna artikel kan kommissionen, efter samråd med samarbetsgruppen och europeiska gruppen för cybersäkerhetscertifiering, begära att Enisa utarbetar ett förslag till certifieringsordning enligt artikel 48.2 i förordning (EU) 2019/881.

Artikel 25

Standardisering

1. För att främja en enhetlig tillämpning av artikel 21.1 och 21.2 ska medlemsstaterna, utan att föreskriva eller gynna användning av en viss typ av teknik, uppmuntra användningen av europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem.

2. Enisa ska i samarbete med medlemsstaterna och, när så är lämpligt, efter samråd med relevanta intressenter, utarbeta råd och riktlinjer för de tekniska områden som ska beaktas när det gäller punkt 1 samt för redan befintliga standarder, inklusive nationella standarder, som skulle göra det möjligt att täcka dessa områden.

KAPITEL V

JURISDIKTION OCH REGISTRERING

Artikel 26

Jurisdiktion och territorialitet

1. Entiteter som omfattas av detta direktivs tillämpningsområde ska anses omfattas av jurisdiktionen i den medlemsstat där de är etablerade, utom när det gäller följande:

a) Tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, som ska anses omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster.

b) Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster, vilka ska anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen i enlighet med punkt 2.

c) Offentliga förvaltningsentiteter, som ska anses omfattas av jurisdiktionen i den medlemsstat som inrättade dem.

2. Vid tillämpning av detta direktiv ska en entitet som avses i punkt 1 b anses ha sitt huvudsakliga etableringsställe i unionen i den medlemsstat där besluten om riskhanteringsåtgärder för cybersäkerhet i huvudsak fattas. Om en sådan medlemsstat inte kan fastställas eller om sådana beslut inte fattas i unionen ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där cybersäkerhetsoperationer utförs. Om en sådan medlemsstat inte kan fastställas ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där den berörda entiteten har det etableringsställe som har flest anställda i unionen.

3. Om en entitet som avses i punkt 1 b inte är etablerad i unionen, men erbjuder tjänster inom unionen, ska den utse en företrädare i unionen. Företrädaren ska vara etablerad i en av de medlemsstater där tjänsterna erbjuds. Entiteten ska anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad. Om det inte finns en utsedd företrädare i unionen enligt denna punkt får varje medlemsstat där entiteten tillhandahåller tjänster vidta rättsliga åtgärder mot entiteten för överträdelsen av detta direktiv.

4. Det faktum att en entitet som avses i punkt 1 b utsett en företrädare ska inte påverka eventuella rättsliga åtgärder mot entiteten i sig.

5. De medlemsstater som har mottagit en begäran om ömsesidigt bistånd med avseende på en entitet som avses i punkt 1 b får, inom ramen för den begäran, vidta lämpliga tillsyns- och efterlevnadskontrollåtgärder med avseende på den berörda entitet som tillhandahåller tjänster eller som har ett nätverks- och informationssystem inom deras territorium.

Artikel 27

Register över entiteter

1. Enisa ska skapa och upprätthålla ett register över leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leveransleverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av internetbaserade marknadsplatser online, internetbaserade sökmotorer och plattformar för sociala nätverkstjänster, på grundval av den information som mottagits från de gemensamma kontaktpunkterna i enlighet med punkt 4. Enisa ska på begäran ge de behöriga myndigheterna tillgång till detta register, samtidigt som skydd av informationens konfidentialitet säkerställs i tillämpliga fall.

2. Medlemsstaterna ska ålägga de entiteter som avses i punkt 1 att lämna följande uppgifter till de behöriga myndigheterna senast den 17 januari 2025:

a) Entitetens namn.

b) Den relevanta sektorn och delsektorn samt typen av entitet enligt bilaga I eller II i tillämpliga fall.

c) Adressen till entitetens huvudsakliga etableringsställe och andra rättsligt giltiga etableringsställen i unionen eller, om entiteten inte är etablerad i unionen, till dess företrädare som utsetts i enlighet med artikel 26.3.

d) Aktuella kontaktuppgifter, inklusive e-postadresser och telefonnummer till entiteten och, i tillämpliga fall, till dess företrädare som utsetts i enlighet med artikel 26.3.

e) De medlemsstater där entiteten tillhandahåller tjänster.

f) Entitetens IP-adressintervall.

3. Medlemsstaterna ska säkerställa att de entiteter som avses i punkt 1 underrättar den behöriga myndigheten om alla ändringar av de uppgifter som de lämnat enligt punkt 2 utan dröjsmål och under alla omständigheter inom tre månader från dagen för ändringen.

4. När den gemensamma kontaktpunkten i den berörda medlemsstaten mottagit den information som avses i punkterna 2 och 3, med undantag för den information som avses i punkt 2 f, ska den utan dröjsmål vidarebefordra den informationen till Enisa.

5. Den information som avses i punkterna 2 och 3 i denna artikel ska, i tillämpliga fall, lämnas genom den nationella mekanism som avses i artikel 3.4 fjärde stycket.

Artikel 28

Databas över domännamnsregistreringsuppgifter

1. För att bidra till domännamnssystemets säkerhet, stabilitet och motståndskraft ska medlemsstaterna ålägga registreringsenheter för toppdomäner och de enheter som tillhandahåller domännamnsregistreringstjänster att samla in och upprätthålla korrekta och fullständiga registreringsuppgifter för domännamn i en särskild databas med tillbörlig aktsamhet i enlighet med unionens dataskyddslagstiftning när det gäller personuppgifter.

2. För tillämpningen av punkt 1 ska medlemsstaterna föreskriva att databasen med registreringsuppgifter för domännamn innehåller nödvändig information för att identifiera och kontakta innehavarna av domännamnen och de kontaktpunkter som administrerar domännamnen under toppdomänerna. Denna information ska omfatta följande:

a) Domännamn.

b) Registreringsdatum.

c) Registrantens namn, e-postadress och telefonnummer.

d) E-postadress och telefonnummer till den kontaktpunkt som administrerar domännamnet om dessa inte är desamma som för registranten.

3. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att ha strategier och förfaranden, inbegripet kontrollförfaranden, för att säkerställa att de databaser som avses i punkt 1 innehåller korrekt och fullständig information. Medlemsstaterna ska föreskriva att sådana strategier och förfaranden offentliggörs.

4. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål efter registreringen av ett domännamn offentliggöra registreringsuppgifter för domännamn som inte är personuppgifter.

5. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att ge åtkomst till specifika registreringsuppgifter för domännamn på lagliga och vederbörligen motiverade begäranden från legitima åtkomstsökande, i enlighet med unionens dataskyddslagstiftning. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål och under alla omständigheter inom 72 timmar från mottagandet besvarar en begäran om åtkomst. Medlemsstaterna ska föreskriva att strategier och förfaranden för utlämning av sådana uppgifter offentliggörs.

6. Fullgörandet av de skyldigheter som fastställs i punkterna 1–5 får inte leda till dubblerad insamling av registreringsuppgifter för domännamn. I detta syfte ska medlemsstaterna ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att samarbeta med varandra.

KAPITEL VI

INFORMATIONSUTBYTE

Artikel 29

Arrangemang för informationsutbyte om cybersäkerhet

1. Medlemsstaterna ska säkerställa att entiteter som omfattas av tillämpningsområdet för detta direktiv och, i relevanta fall, andra relevanta entiteter som inte omfattas av detta direktivs tillämpningsområde på frivillig basis har möjlighet att utbyta relevant information om cybersäkerhet sinsemellan, inbegripet information om cyberhot, tillbud, sårbarheter, tekniker och förfaranden, angreppsindikatorer, fientlig taktik, specifik information om fientliga aktörer, cybersäkerhetsvarningar och rekommendationer avseende konfigurationsverktyg för cybersäkerhet för att upptäcka cyberattacker, om sådant informationsutbyte

a) syftar till att förebygga, upptäcka, reagera på eller återhämta sig från incidenter eller begränsa deras inverkan,

b) höjer cybersäkerhetsnivån, särskilt genom att öka medvetenheten om cyberhot, begränsa eller hindra sådana hots förmåga att sprida sig, stödja en rad defensiva förmågor, avhjälpande av sårbarheter och delgivning av information om sårbarheter, metoder för att upptäcka och förebygga hot, strategier för begränsning av hot eller reaktions- och återhämtningsfaser, eller genom att främja forskningssamverkan om cyberhot bland offentliga och privata entiteter.

2. Medlemsstaterna ska säkerställa att informationsutbytet sker inom grupper av väsentliga och viktiga entiteter, och i relevanta fall, deras leverantörer eller tjänsteleverantörer. Sådant utbyte ska genomföras med hjälp av arrangemang för informationsutbyte om cybersäkerhet med hänsyn till den potentiellt känsliga karaktären hos den information som utbyts.

3. Medlemsstaterna ska underlätta inrättandet av de arrangemang för informationsutbyte om cybersäkerhet som avses i punkt 2 i denna artikel. Sådana arrangemang får ange operativa aspekter, inbegripet användning av särskilda IKT-plattformar och automatiseringsverktyg, innehållet i och villkoren för de arrangemangen för informationsutbyte. Medlemsstaterna får, i samband med fastställandet av närmare bestämmelser om offentliga myndigheters deltagande i sådana arrangemang, införa villkor för den information som tillgängliggörs av behöriga myndigheter eller CSIRT-enheter. Medlemsstaterna ska erbjuda stöd för tillämpningen av sådana arrangemang i enlighet med de riktlinjer som avses i artikel 7.2 h.

4. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter underrättar de behöriga myndigheterna om sitt deltagande i de arrangemang för informationsutbyte om cybersäkerhet som avses i punkt 2, när de ingår sådana arrangemang eller, om de utträder ur sådana arrangemang, när utträdet får verkan.

5. Enisa ska tillhandahålla stöd för inrättandet av de arrangemang för informationsutbyte om cybersäkerhet som avses i punkt 2 genom att utbyta bästa praxis och erbjuda vägledning.

Artikel 30

Frivillig underrättelse om relevant information

1. Medlemsstaterna ska säkerställa att underrättelser, utöver den underrättelseskyldighet som föreskrivs i artikel 23, kan lämnas in till CSIRT-enheterna eller, i tillämpliga fall, de behöriga myndigheterna, på frivillig basis av

a) väsentliga och viktiga entiteter med avseende på incidenter, cyberhot och tillbud,

b) andra entiteter än de som avses i led a, oberoende av om de omfattas av detta direktiv, vad gäller om betydande incidenter, cyberhot och tillbud.

2. Medlemsstaterna ska behandla de underrättelser som avses i punkt 1 i denna artikel i enlighet med det förfarande som anges i artikel 23. Medlemsstaterna får ge behandling av obligatoriska underrättelser företräde framför behandling av frivilliga underrättelser.

CSIRT-enheterna, och i tillämpliga fall, de behöriga myndigheterna ska vid behov informera de gemensamma kontaktpunkterna om underrättelser som mottagits i enlighet med denna artikel, och samtidigt säkerställa att informationen från den underrättande entiteten förblir konfidentiell och skyddas på lämpligt sätt. Utan att det påverkar förebyggande, utredning, avslöjande och lagföring av brott får frivillig rapportering inte leda till att den underrättande entiteten åläggs ytterligare skyldigheter som den inte skulle ha blivit föremål för om den inte hade lämnat in underrättelsen.

KAPITEL VII

TILLSYN OCH EFTERLEVNADSKONTROLL

Artikel 31

Allmänna aspekter på tillsyn och efterlevnadskontroll

1. Medlemsstaterna ska säkerställa att deras behöriga myndigheter på ett ändamålsenligt sätt övervakar och vidtar de åtgärder som krävs för att säkerställa att detta direktiv efterlevs.

2. Medlemsstaterna får tillåta sina behöriga myndigheter att prioritera tillsyn. Denna prioritering ska baseras på en riskbaserad metod. När de behöriga myndigheterna utövar sina tillsynsuppgifter enligt artiklarna 32 och 33 får de i detta syfte fastställa tillsynsmetoder som gör det möjligt att prioritera sådana uppgifter enligt en riskbaserad metod.

3. De behöriga myndigheterna ska ha ett nära samarbete med tillsynsmyndigheterna enligt förordning (EU) 2016/679 när de behandlar incidenter som medför personuppgiftsincidenter, utan att det påverkar tillsynsmyndigheternas befogenheter och uppgifter enligt den förordningen.

4. Utan att det påverkar de nationella rättsliga och institutionella ramarna ska medlemsstaterna säkerställa att de behöriga myndigheterna, vid tillsynen av de offentliga förvaltningsentiteternas efterlevnad av detta direktiv och införandet av efterlevnadskontrollåtgärder vid överträdelser av detta direktiv, har lämpliga befogenheter att utföra dessa uppgifter och är operativt oberoende i förhållande till de offentliga förvaltningsentiteter som övervakas. Medlemsstaterna får besluta att införa lämpliga, proportionella och effektiva tillsyns- och efterlevnadskontrollåtgärder med avseende på dessa entiteter i enlighet med de nationella rättsliga och institutionella ramarna.

Artikel 32

Tillsyns- och efterlevnadskontrollåtgärder i fråga om väsentliga entiteter

1. Medlemsstaterna ska säkerställa att de tillsyns- eller efterlevnadskontrollåtgärder som åläggs väsentliga entiteter angående de skyldigheter som anges i detta direktiv är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

2. Medlemsstaterna ska säkerställa att behöriga myndigheter, när de utövar sina tillsynsuppgifter avseende väsentliga entiteter, har befogenhet att åtminstone underställa dessa entiteter

a) inspektioner på plats och distansbaserad tillsyn, inklusive slumpvisa kontroller som utförs av utbildad personal,

b) regelbundna och riktade säkerhetsrevisioner som utförs av ett oberoende organ eller en behörig myndighet,

c) ad hoc-revisioner, inbegripet när detta är motiverat på grund av en betydande incident eller av en väsentlig entitets överträdelse av detta direktiv,

d) säkerhetsskanningar på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier, vid behov i samarbete med den berörda entiteten,

e) begäranden om sådan information som behövs för att bedöma de riskhanteringsåtgärder för cybersäkerhet som antagits av den berörda entiteten, inbegripet dokumenterade cybersäkerhetsstrategier, samt fullgörandet av skyldigheten att lämna information till de behöriga myndigheterna i enlighet med artikel 27,

f) begäranden om tillgång till uppgifter, handlingar och information som behövs för att de ska kunna utföra sina tillsynsuppgifter,

g) begäranden om bevis på genomförandet av cybersäkerhetsstrategier, t.ex. resultaten av säkerhetsrevisioner som utförts av en kvalificerad revisor och respektive underliggande bevis.

De riktade säkerhetsrevisioner som avses i första stycket led b ska baseras på riskbedömningar som utförs av den behöriga myndigheten eller den granskade entiteten, eller på annan tillgänglig riskrelaterad information.

Resultaten av alla riktade säkerhetsrevisioner ska göras tillgängliga för den behöriga myndigheten. Kostnaderna för sådana riktade säkerhetsrevisioner som utförs av ett oberoende organ ska betalas av den granskade entiteten, utom i vederbörligen motiverade fall när den behöriga myndigheten beslutar något annat.

3. När de behöriga myndigheterna utövar sina befogenheter enligt punkt 2 e, f eller g ska de ange syftet med en begäran och specificera den begärda informationen.

4. Medlemsstaterna ska säkerställa att deras behöriga myndigheter, när de utövar sina befogenheter med avseende på efterlevnadskontroll gentemot väsentliga entiteter, åtminstone har befogenhet att

a) utfärda varningar om berörda entiteters överträdelser av detta direktiv,

b) anta bindande instruktioner, också om vilka åtgärder som krävs för att förebygga eller avhjälpa en incident, samt tidsgränser för genomförandet av sådana åtgärder och för rapporteringen om deras genomförande, eller ett föreläggande om att de berörda entiteterna ska avhjälpa konstaterade brister eller överträdelser av detta direktiv,

c) ålägga de berörda entiteterna att upphöra med beteenden som utgör en överträdelse av detta direktiv och att avstå från att upprepa sådana beteenden,

d) ålägga de berörda entiteterna att säkerställa att deras riskhanteringsåtgärder för cybersäkerhet överensstämmer med artikel 21 eller att fullgöra de rapporteringsskyldigheter som fastställs i artikel 23, på ett specificerat sätt och inom en angiven tidsperiod,

e) ålägga de berörda entiteterna att informera de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller utför verksamheter som potentiellt kan beröras av ett betydande cyberhot om hotets karaktär och om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa fysiska eller juridiska personer kan vidta som svar på hotet,

f) ålägga de berörda entiteterna att inom en rimlig tidsfrist genomföra de rekommendationer som lämnats till följd av en säkerhetsrevision,

g) utse en övervakningsansvarig med väldefinierade uppgifter för en fastställd tidsperiod för att övervaka att de berörda entiteterna efterlever artiklarna 21 och 23,

h) ålägga de berörda entiteterna att offentliggöra aspekter av överträdelser av detta direktiv på ett specificerat sätt,

i) påföra eller begära att relevanta organ eller domstolar i enlighet med nationell rätt påför administrativa sanktionsavgifter enligt artikel 34 utöver någon av de åtgärder som avses i leden a–h i denna punkt.

5. Om efterlevnadskontrollåtgärder som antas enligt punkt 4 a–d och f är ineffektiva ska medlemsstaterna säkerställa att deras behöriga myndigheter har befogenhet att fastställa en tidsfrist inom vilken en väsentlig entitet ska vidta nödvändiga åtgärder för att avhjälpa bristerna eller uppfylla dessa myndigheters krav. Om de begärda åtgärderna inte vidtas inom den fastställda tidsfristen ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenhet att

a) tillfälligt upphäva eller begära att ett certifierings- eller auktorisationsorgan, eller en domstol, i enlighet med nationell rätt, tillfälligt upphäver en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls eller verksamheter som utövas av den väsentliga entiteten,

b) begära att relevanta organ eller domstolar, i enlighet med nationell rätt, inför ett tillfälligt förbud för varje fysisk person som på nivån för verkställande direktör eller juridiskt ombud har ledningsansvar i den väsentliga entiteten att utöva ledningsfunktioner i den entiteten.

Tillfälliga upphävanden eller förbud i enlighet med denna punkt ska tillämpas endast till dess att den berörda entiteten vidtar nödvändiga åtgärder för att avhjälpa bristerna eller uppfylla de krav från den behöriga myndigheten som gav upphov till sådana efterlevnadskontrollåtgärder. Sådana tillfälliga upphävanden eller förbud får komma i fråga endast om lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och stadgan iakttas, inbegripet rätten till ett effektivt rättsmedel och en rättvis rättegång, oskuldspresumtion och rätten till försvar.

De efterlevnadskontrollåtgärder som föreskrivs i denna punkt är inte tillämpliga på sådana offentliga förvaltningsentiteter som omfattas av detta direktiv.

6. Medlemsstaterna ska säkerställa att varje fysisk person som ansvarar för eller agerar som juridiskt ombud för en väsentlig entitet har befogenhet att säkerställa att entiteten efterlever detta direktiv, på grundval av en befogenhet att företräda entiteten, att fatta beslut på dess vägnar eller att utöva kontroll över entiteten. Medlemsstaterna ska säkerställa att dessa fysiska personer kan hållas ansvariga för överträdelser av sitt uppdrag att säkerställa att detta direktiv efterlevs.

När det gäller offentliga förvaltningsentiteter påverkar inte denna punkt nationell rätt avseende det ansvar som åligger statligt anställda och valda eller utnämnda tjänstepersoner.

7. När de behöriga myndigheterna tillämpar efterlevnadskontrollåtgärder som avses i punkt 4 eller 5 ska de iaktta rätten till försvar och ta hänsyn till omständigheterna i varje enskilt fall och som ett minimum ta vederbörlig hänsyn till följande:

a) Överträdelsens allvar och betydelsen av de bestämmelser som har överträtts, med beaktande av att bland annat följande alltid ska anses vara en allvarlig överträdelse:

   i) Upprepade överträdelser.

   ii) Underlåtenhet att underrätta om eller avhjälpa betydande incidenter.

   iii) Underlåtenhet att avhjälpa brister enligt bindande instruktioner från behöriga myndigheter.

   iv) Hindrande av revisioner eller övervakningsverksamhet som den behöriga myndigheten beordrat efter det att en överträdelse konstaterats.

   v) Tillhandahållande av falsk eller grovt felaktig information i fråga om riskhanteringsåtgärder för cybersäkerhet eller rapporteringsskyldigheter enligt artiklarna 21 och 23.

b) Överträdelsens varaktighet.

c) Eventuella tidigare relevanta överträdelser från den berörda entitetens sida.

d) Den materiella eller immateriella skada som uppstått, inbegripet finansiella eller ekonomiska förluster, effekter på andra tjänster och det antal användare som berörs.

e) Uppsåt eller oaktsamhet från den som har gjort sig skyldig till överträdelsen.

f) De åtgärder som entiteten har vidtagit för att förhindra eller begränsa den materiella eller immateriella skadan.

g) Efterlevnad av godkända uppförandekoder eller godkända certifieringsmekanismer.

h) I vilken utsträckning de fysiska eller juridiska personer som hålls ansvariga samarbetar med de behöriga myndigheterna.

8. De behöriga myndigheterna ska utförligt motivera sina efterlevnadskontrollåtgärder. Innan sådana åtgärder antas ska de behöriga myndigheterna underrätta de berörda entiteterna om sina preliminära slutsatser. De ska också ge dessa entiteter en rimlig tidsfrist för att lämna synpunkter, utom i vederbörligen motiverade fall där omedelbara åtgärder för att förhindra eller reagera på incidenter annars skulle hindras.

9. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv informerar de relevanta behöriga myndigheterna inom samma medlemsstat i enlighet med direktiv (EU) 2022/2557 när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll för att säkerställa att en entitet som identifierats som en kritisk entitet i enlighet med direktiv (EU) 2022/2557 efterlever detta direktiv. När så är lämpligt får behöriga myndigheter enligt direktiv (EU) 2022/2557 begära att behöriga myndigheter enligt detta direktiv utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll gentemot en entitet som identifieras som en kritisk entitet i enlighet med direktiv (EU) 2022/2557.

10. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv samarbetar med de relevanta behöriga myndigheterna i den berörda medlemsstaten enligt förordning (EU) 2022/2554. Medlemsstaterna ska särskilt säkerställa att deras behöriga myndigheter enligt detta direktiv informerar det tillsynsforum som inrättats enligt artikel 32.1 i förordning (EU) 2022/2554 när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll för att säkerställa att en väsentlig entitet som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster enligt artikel 31 i förordning (EU) 2022/2554 efterlever detta direktiv.

Artikel 33

Tillsyns- och efterlevnadskontrollåtgärder i fråga om viktiga entiteter

1. När medlemsstaterna får bevis, indikationer på eller information om att en viktig entitet påstås underlåta att fullgöra detta direktiv, särskilt artiklarna 21 och 23, ska de säkerställa att de behöriga myndigheterna vid behov vidtar åtgärder i form av tillsynsåtgärder i efterhand. Medlemsstaterna ska säkerställa att dessa åtgärder är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

2. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de utövar sina tillsynsuppgifter avseende viktiga entiteter, har befogenhet att åtminstone underställa dessa entiteter

a) inspektioner på plats och distansbaserad tillsyn i efterhand, som utförs av utbildad personal,

b) riktade säkerhetsrevisioner utförda av ett oberoende organ eller en behörig myndighet,

c) säkerhetsskanningar på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier, vid behov i samarbete med den berörda entiteten,

d) begäranden om information som behövs för att i efterhand bedöma de riskhanteringsåtgärder för cybersäkerhet som antagits av den berörda entiteten, inbegripet dokumenterade cybersäkerhetsstrategier, samt fullgörandet av skyldigheten att lämna information till de behöriga myndigheterna i enlighet med artikel 27,

e) begäranden om tillgång till uppgifter, handlingar och information som behövs för att utföra sina tillsynsuppgifter,

f) begäranden om bevis på genomförandet av cybersäkerhetsstrategier, t.ex. resultaten av säkerhetsrevisioner som utförts av en kvalificerad revisor och respektive underliggande bevis.

De riktade säkerhetsrevisioner som avses i första stycket led b ska baseras på riskbedömningar som utförs av den behöriga myndigheten eller den granskade entiteten, eller på annan tillgänglig riskrelaterad information.

Resultaten av alla riktade säkerhetsrevisioner ska göras tillgängliga för den behöriga myndigheten. Kostnaderna för sådana riktade säkerhetsrevisioner som utförs av ett oberoende organ ska betalas av den granskade entiteten, utom i vederbörligen motiverade fall när den behöriga myndigheten beslutar något annat.

3. När de behöriga myndigheterna utövar sina befogenheter enligt punkt 2 d, e eller f ska de ange syftet med en begäran och specificera den begärda informationen.

4. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de utövar sina befogenheter med avseende på efterlevnadskontroll gentemot viktiga entiteter åtminstone har befogenhet att

a) utfärda varningar om de berörda entiteternas överträdelser av detta direktiv,

b) anta bindande instruktioner eller ett föreläggande om att de berörda entiteterna ska avhjälpa konstaterade brister eller överträdelser av detta direktiv,

c) ålägga de berörda entiteterna att upphöra med beteenden som utgör en överträdelse av detta direktiv och att avstå från att upprepa sådana beteenden,

d) ålägga de berörda entiteterna att säkerställa att deras riskhanteringsåtgärder för cybersäkerhet överensstämmer med artikel 21 eller att fullgöra de rapporteringsskyldigheter som fastställs i artikel 23, på ett specificerat sätt och inom en angiven tidsperiod,

e) ålägga de berörda entiteterna att informera de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller utför verksamheter som potentiellt kan beröras av ett betydande cyberhot om hotets karaktär och om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa fysiska eller juridiska personer kan vidta som svar på hotet,

f) ålägga de berörda entiteterna att inom en rimlig tidsfrist genomföra de rekommendationer som lämnats till följd av en säkerhetsrevision,

g) ålägga de berörda entiteterna att offentliggöra aspekter av överträdelser av detta direktiv på ett specificerat sätt,

h) påföra eller begära att relevanta organ eller domstolar i enlighet med nationell rätt påför administrativa sanktionsavgifter enligt artikel 34 utöver någon av de åtgärder som avses i leden a–g i denna punkt.

5. Artikel 32.6, 32.7 och 32.8 ska i tillämpliga delar tillämpas på de tillsyns- och efterlevnadskontrollåtgärder som föreskrivs i denna artikel för viktiga entiteter.

6. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv samarbetar med de relevanta behöriga myndigheterna i den berörda medlemsstaten i enlighet med förordning (EU) 2022/2554. Medlemsstaterna ska särskilt säkerställa att deras behöriga myndigheter enligt detta direktiv informerar det tillsynsforum som inrättats enligt artikel 32.1 i förordning (EU) 2022/2554 när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll för att säkerställa att en viktig entitet som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster i enlighet med artikel 31 i förordning (EU) 2022/2554 efterlever detta direktiv.

Artikel 34

Allmänna villkor för påförande av administrativa sanktionsavgifter för väsentliga och viktiga entiteter

1. Medlemsstaterna ska säkerställa att de administrativa sanktionsavgifter som påförs väsentliga och viktiga entiteter enligt denna artikel för överträdelser av detta direktiv är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

2. Administrativa sanktionsavgifter ska påföras utöver någon av de åtgärder som avses i artikel 32.4 a–h, artikel 32.5 och artikel 33.4 a–g.

3. När beslut fattas om huruvida administrativa sanktionsavgifter ska påföras och om avgiftsbeloppet i varje enskilt fall, ska vederbörlig hänsyn tas till åtminstone de faktorer som anges i artikel 32.7.

4. Medlemsstaterna ska säkerställa att väsentliga entiteter som överträder artikel 21 eller 23, i enlighet med punkterna 2 och 3 i den här artikeln påförs administrativa sanktionsavgifter på högst 10 000 000 EUR eller högst 2 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den väsentliga entiteten tillhör, beroende på vilken siffra som är högst.

5. Medlemsstaterna ska säkerställa att viktiga entiteter som överträder artikel 21 eller 23, i enlighet med punkterna 2 och 3 i den här artikeln påförs administrativa sanktionsavgifter på högst 7 000 000 EUR eller högst 1,4 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den viktiga entiteten tillhör, beroende på vilken siffra som är högst.

6. Medlemsstaterna får föreskriva befogenhet att förelägga viten för att tvinga en väsentlig eller viktig entitet att upphöra med en överträdelse av detta direktiv i enlighet med ett föregående beslut av den behöriga myndigheten.

7. Utan att det påverkar behöriga myndigheters befogenheter enligt artiklarna 32 och 33 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga förvaltningsentiteter som omfattas av de skyldigheter som fastställs i detta direktiv.

8. Om administrativa sanktionsavgifter inte föreskrivs i en medlemsstats rättssystem ska den medlemsstaten säkerställa att denna artikel tillämpas på ett sådant sätt att förfarandet inleds av den behöriga myndigheten och sanktionsavgifterna sedan påförs av behöriga nationella domstolar, varvid det säkerställs att dessa rättsmedel är effektiva och har samma verkan som de administrativa sanktionsavgifter som påförs av de behöriga myndigheterna. De påförda sanktionsavgifterna ska i alla händelser vara effektiva, proportionella och avskräckande. Medlemsstaten ska underrätta kommissionen om bestämmelserna i de lagar som den antar i enlighet med denna punkt senast den 17 oktober 2024 och, utan dröjsmål, om eventuella senare ändringslagstiftning eller ändringar som berör dem.

Artikel 35

Överträdelser som innebär personuppgiftsincidenter

1. Om de behöriga myndigheterna under tillsyn eller efterlevnadskontroll får kännedom om att en väsentlig eller viktig entitets överträdelse av de skyldigheter som fastställs i artiklarna 21 och 23 i detta direktiv kan innebära en personuppgiftsincident, enligt definitionen i artikel 4.12 i förordning (EU) 2016/679, som ska anmälas i enlighet med artikel 33 i den förordningen, ska de utan onödigt dröjsmål informera de tillsynsmyndigheter som avses i artikel 55 eller 56 i den förordningen.

2. Om de tillsynsmyndigheter som avses i artikel 55 eller 56 i förordning (EU) 2016/679 påför administrativa sanktionsavgifter enligt artikel 58.2 i) i den förordningen ska de behöriga myndigheterna inte påföra administrativa sanktionsavgifter enligt artikel 34 i detta direktiv för en överträdelse som avses i punkt 1 i den här artikeln som följer av samma beteende som det som den administrativa sanktionsavgiften avsåg enligt artikel 58.2 i) i förordning (EU) 2016/679. De behöriga myndigheterna får emellertid tillämpa de efterlevnadskontrollåtgärder som föreskrivs i artikel 32.4 a–h, artikel 32.5 och artikel 33.4 a–g i detta direktiv.

3. Om den tillsynsmyndighet som är behörig enligt förordning (EU) 2016/679 är etablerad i en annan medlemsstat än den behöriga myndigheten, ska den behöriga myndigheten informera den tillsynsmyndighet som är etablerad i dess egen medlemsstat om det potentiella dataintrång som avses i punkt 1.

Artikel 36

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella åtgärder som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast den 17 januari 2025 samt utan dröjsmål eventuella ändringar som berör dem.

Artikel 37

Ömsesidigt bistånd

1. Om en entitet tillhandahåller tjänster i mer än en medlemsstat eller tillhandahåller tjänster i en eller flera medlemsstater och dess nätverks- och informationssystem är belägna i en eller flera andra medlemsstater ska de behöriga myndigheterna i de berörda medlemsstaterna vid behov samarbeta med och bistå varandra. Detta samarbete ska åtminstone omfatta följande:

a) Att de behöriga myndigheter som tillämpar tillsyns- eller efterlevnadskontrollåtgärder i en medlemsstat via den gemensamma kontaktpunkten informerar och samråder med de behöriga myndigheterna i övriga berörda medlemsstater om de tillsyns- och efterlevnadskontrollåtgärder som vidtagits.

b) Att en behörig myndighet får begära att en annan behörig myndighet vidtar tillsyns- eller efterlevnadskontrollåtgärder.

c) Att en behörig myndighet, efter att ha mottagit en motiverad begäran från en annan behörig myndighet, ska tillhandahålla ömsesidigt bistånd till den andra behöriga myndigheten i proportion till sina egna resurser så att tillsyns- eller efterlevnadskontrollåtgärderna kan genomföras på ett ändamålsenligt, effektivt och konsekvent sätt.

Det ömsesidiga bistånd som avses i första stycket led c får omfatta begäranden om information och tillsynsåtgärder, inbegripet begäranden om att utföra inspektioner på plats, distansbaserad tillsyn eller riktade säkerhetsrevisioner. En behörig myndighet till vilken en begäran om bistånd riktas får inte avslå begäran om det inte fastställs att myndigheten antingen inte är behörig att tillhandahålla det begärda biståndet, att det begärda biståndet inte står i proportion till den behöriga myndighetens tillsynsuppgifter eller att begäran avser information eller omfattar verksamhet som, om den lämnas ut eller utförs, skulle strida mot den medlemsstatens väsentliga nationella säkerhetsintressen, allmänna säkerhet eller försvar. Innan den behöriga myndigheten avslår en sådan begäran ska den samråda med övriga berörda behöriga myndigheter samt, på begäran av en av de berörda medlemsstaterna, med kommissionen och Enisa.

2. När så är lämpligt får behöriga myndigheter från olika medlemsstater i samförstånd genomföra de gemensamma tillsynsåtgärderna.

KAPITEL VIII

DELEGERADE AKTER OCH GENOMFÖRANDEAKTER

Artikel 38

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 24.2 ska ges till kommissionen för en period på fem år från och med den 16 januari 2023 .

3. Den delegering av befogenhet som avses i artikel 24.2 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artikel 24.2 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 39

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

3. Om kommitténs yttrande ska inhämtas genom skriftligt förfarande, ska det förfarandet avslutas utan resultat om kommitténs ordförande, inom tidsfristen för att avge yttrandet, så beslutar eller en kommittéledamot så begär.

KAPITEL IX

SLUTBESTÄMMELSER

Artikel 40

Översyn

Senast den 17 oktober 2027 och därefter var 36:e månad ska kommissionen se över hur detta direktiv fungerar och rapportera resultatet till Europaparlamentet och rådet. Rapporten ska särskilt bedöma relevansen av de berörda enheternas storlek och sektorer, delsektorer och typer när det gäller den entitet som avses i bilagorna I och II för ekonomins och samhällets funktion när det gäller cybersäkerhet. För detta ändamål och för att ytterligare främja det strategiska och operativa samarbetet ska kommissionen beakta rapporterna från samarbetsgruppen och CSIRT-nätverket om de erfarenheter som förvärvats på strategisk och operativ nivå. Rapporten ska vid behov åtföljas av ett lagstiftningsförslag.

Artikel 41

Införlivande

1. Medlemsstaterna ska senast den 17 oktober 2024 anta och offentliggöra de bestämmelser som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta.

De ska tillämpa dessa bestämmelser från och med den 18 oktober 2024.

2. När en medlemsstat antar de bestämmelser som avses i punkt 1 ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

Artikel 42

Ändring av förordning (EU) nr 910/2014

I förordning (EU) nr 910/2014 ska artikel 19 utgå med verkan från och med den 18 oktober 2024.

Artikel 43

Ändring av direktiv (EU) 2018/1972

I direktiv (EU) 2018/1972 ska artiklarna 40 och 41 utgå med verkan från och med den 18 oktober 2024.

Artikel 44

Upphävande

Direktiv (EU) 2016/1148 ska upphöra att gälla med verkan från och med den 18 oktober 2024.

Hänvisningar till det upphävda direktivet ska anses som hänvisningar till det här direktivet och ska läsas i enlighet med jämförelsetabellen i bilaga III.

Artikel 45

Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 46

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Strasbourg den 14 december 2022.

På Europaparlamentets vägnar	*På rådets vägnar*
R. METSOLA	M. BEK
Ordförande	*Ordförande*

BILAGA I

HÖGKRITISKA SEKTORER

Sektor	Delsektor	Typ av entitet
1. Energi	a) Elektricitet	— Elföretag enligt definitionen i artikel 2.57 i Europaparlamentets och rådets direktiv (EU) 2019/944 (1)som bedriver *leverans* enligt definitionen i artikel 2.12 i det direktivet
		— Systemansvariga för distributionssystem enligt definitionen i artikel 2.29 i direktiv (EU) 2019/944
		— Systemansvariga för överföringssystem enligt definitionen i artikel 2.35 i direktiv (EU) 2019/944
		— Producenter enligt definitionen i artikel 2.38 i direktiv (EU) 2019/944
		— Nominerade elmarknadsoperatörer enligt definitionen i artikel 2.8 i Europaparlamentets och rådets förordning (EU) 2019/943 (2) — Marknadsaktörer enligt definitionen i artikel 2.25 i förordning (EU) 2019/943 och som tillhandahåller aggregering, efterfrågeflexibilitet eller energilagringstjänster enligt definitionen i artikel 2.18, 2.20 och 2.59 i direktiv (EU) 2019/944 — Laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt och som tillhandahåller en laddningstjänst till slutanvändare, även när detta utförs på uppdrag av en leverantör av mobilitetstjänster och i dess namn
	b) Fjärrvärme eller fjärrkyla	— Operatörer av fjärrvärme eller fjärrkyla enligt definitionen i artikel 2.19 i Europaparlamentets och rådets direktiv (EU) 2018/2001 (3)
	c) Olja	— Operatörer av oljeledningar
		— Operatörer av anläggningar för oljeproduktion, raffinaderier, bearbetningsanläggningar och anläggningar för lagring och överföring av olja
		— Centrala lagringsenheter enligt definitionen i artikel 2 f i rådets direktiv 2009/119/EG (4)
	d) Gas	— Gashandelsföretag eller gashandlare enligt definitionen i artikel 2.8 i Europaparlamentets och rådets direktiv 2009/73/EG (5)
		— Systemansvariga för distributionssystemet enligt definitionen i artikel 2.6 i direktiv 2009/73/EG
		— Systemansvariga för överföringssystemet enligt definitionen i artikel 2.4 i direktiv 2009/73/EG
		— Systemansvariga för lagringssystemet enligt definitionen i artikel 2.10 i direktiv 2009/73/EG
		— Systemansvariga för en LNG-anläggning enligt definitionen i artikel 2.12 i direktiv 2009/73/EG
		— Naturgasföretag enligt definitionen i artikel 2.1 i direktiv 2009/73/EG
		— Operatörer av raffinaderier och bearbetningsanläggningar för naturgas
	e) Vätgas	— Operatörer av anläggningar för produktion, lagring och överföring av vätgas

Sektor	Delsektor	Typ av enhet
2. Transporter	a) Lufttransport	— Lufttrafikföretag enligt definitionen i artikel 3.4 i förordning (EG) nr 300/2008 och som används för kommersiella syften
		— Flygplatsens ledningsenheter enligt definitionen i artikel 2.2 i Europaparlamentets och rådets direktiv 2009/12/EG (*), flygplatser enligt definitionen i artikel 2.1 i det direktivet, inbegripet de huvudflygplatser som förtecknas i avsnitt 2 i bilaga II till Europaparlamentets och rådets förordning (EU) nr 1315/2013 (†), och enheter som driver närliggande anläggningar inom flygplatser
		— Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänst enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 549/2004 (‡)
	b) Järnvägstransport	— Infrastrukturförvaltare enligt definitionen i artikel 3.2 i Europaparlamentets och rådets direktiv 2012/34/EU (§)
		— Järnvägsföretag enligt definitionen i artikel 3.1 i direktiv 2012/34/EU, inbegripet tjänsteleverantörer enligt definitionen i artikel 3.12 i det direktivet
	c) Sjöfart	— Transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster, enligt definitionerna för sjötransport i bilaga I till Europaparlamentets och rådets förordning (EG) nr 725/2004 (**), exklusive de enskilda fartyg som drivs av dessa företag
		— Ledningsenheter för hamnar enligt definitionen i artikel 3.1 i Europaparlamentets och rådets direktiv 2005/65/EG (††), inbegripet deras hamnanläggningar enligt definitionen i artikel 2.11 i förordning (EG) nr 725/2004, och enheter som sköter anläggningar och utrustning i hamnar
		— Operatörer av sjötrafikinformationstjänst (VTS) enligt definitionen i artikel 3 o i Europaparlamentets och rådets direktiv 2002/59/EG (‡‡)
	d) Vägtransport	— Vägmyndigheter enligt definitionen i artikel 2.12 i kommissionens delegerade förordning (EU) 2015/962 (§§) med ansvar för trafikstyrning, med undantag för offentliga enheter för vilka trafikstyrning eller driften av intelligenta transportsystem är en icke väsentlig del av deras allmänna verksamhet
		— Operatörer av intelligenta transportsystem enligt definitionen i artikel 4.1 i Europaparlamentets och rådets direktiv 2010/40/EU (¶¶)
3. Bankverksamhet		Kreditinstitut enligt definitionen i artikel 4.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013 (***)
4. Finansmarknads-infrastruktur		— Operatörer av handelsplatser enligt definitionen i artikel 4.24 i Europaparlamentets och rådets direktiv 2014/65/EU (†††)
		— Centrala motparter enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 648/2012 (‡‡‡)

Sektor	Delsektor	Typ av entitet
5. Hälso- och sjukvårdssektorn		— Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU ([18])
		— EU-referenslaboratorier som avses i artikel 15 i Europaparlamentets och rådets förordning (EU) 20222/2371 ([19])
		— Entiteter som bedriver forskning och utveckling avseende läkemedel enligt definitionen i artikel 1.2 i Europaparlamentets och rådets direktiv 2001/83/EG ([20]) — Entiteter som tillverkar farmaceutiska basprodukter och läkemedel som avses i avsnitt C huvudgrupp 21 i Nace Rev. 2 — Entiteter som tillverkar medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan (förteckning över kritiska medicintekniska produkter vid ett hot mot folkhälsan) i den mening som avses i artikel 22 i Europaparlamentets och rådets förordning (EU) 2022/123 ([21])
6. Dricksvatten		Leverantörer och distributörer av dricksvatten enligt definitionen i artikel 2.1 a i Europaparlamentets och rådets direktiv (EU) 2020/2184 ([22]) undantaget distributörer för vilka distribution av dricksvatten utgör en icke väsentlig del av deras allmänna verksamhet, som består i distribution av andra förnödenheter och varor
7. Avloppsvatten		Företag som samlar ihop, släpper ut och renar avloppsvatten från tätbebyggelse, hushållsspillvatten eller industrispillvatten enligt definitionen i artikel 2.1–2.3 i rådets direktiv 91/271/EEG ([23]), undantaget företag som samlar ihop, släpper ut eller renar avloppsvatten från tätbebyggelse, hushållsspillvatten eller industrispillvatten som en icke väsentlig del av sin allmänna verksamhet
8. Digital infrastruktur		— Leverantörer av internetknutpunkter
		— Leverantörer av DNS-tjänster, med undantag för operatörer av rotnamnsservrar
		— Registreringsenheter för toppdomäner
		— Leverantörer av molntjänster
		— Leverantörer av datacentraltjänster
		— Leverantörer av nätverk för leverans av innehåll
		— Tillhandahållare av betrodda tjänster
		— Tillhandahållare av allmänna elektroniska kommunikationsnät
		— Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster
9. Förvaltning av IKT-tjänster (mellan företag)		— Leverantörer av hanterade tjänster — Leverantörer av hanterade säkerhetstjänster

Sektor	Delsektor	Typ av enhet
10. Offentlig förvaltning		— Offentliga förvaltningsenheter hos nationella regeringar såsom de definieras av en medlemsstat i enlighet med nationell rätt
		— Offentliga förvaltningsenheter på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt
11. Rymden		Operatörer av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter och som stöder tillhandahållandet av rymdbaserade tjänster, undantaget tillhandahållare av allmänna elektroniska kommunikationsnät

(1) Europaparlamentets och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU (EUT L 158, 14.6.2019, s. 125).
(2) Europaparlamentets och rådets förordning (EU) 2019/943 av den 5 juni 2019 om den inre marknaden för el (EUT L 158, 14.6.2019, s. 54).
(3) Europaparlamentets och rådets direktiv (EU) 2018/2001 av den 11 december 2018 om främjande av användningen av energi från förnybara energikällor (EUT L 328, 21.12.2018, s. 82).
(4) Rådets direktiv 2009/119/EG av den 14 september 2009 om skyldighet för medlemsstaterna att inneha minimilager av råolja och/eller petroleumprodukter (EUT L 265, 9.10.2009, s. 9).
(5) Europaparlamentets och rådets direktiv 2009/73/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för naturgas och om upphävande av direktiv 2003/55/EG (EUT L 211, 14.8.2009, s. 94).
(6) Europaparlamentets och rådets direktiv 2009/12/EG av den 11 mars 2009 om flygplatsavgifter (EUT L 70, 14.3.2009, s. 11).
(7) Europaparlamentets och rådets förordning (EU) nr 1315/2013 av den 11 december 2013 om unionens riktlinjer för utbyggnad av det transeuropeiska transportnätet och om upphävande av beslut nr 661/2010/EU (EUT L 348, 20.12.2013, s. 1).
(8) Europaparlamentets och rådets förordning (EG) nr 549/2004 av den 10 mars 2004 om ramen för inrättande av det gemensamma europeiska luftrummet ("ramförordning") (EUT L 96, 31.3.2004, s. 1).
(9) Europaparlamentets och rådets direktiv 2012/34/EU av den 21 november 2012 om inrättande av ett gemensamt europeiskt järnvägsområde (EUT L 343, 14.12.2012, s. 32).
(10) Europaparlamentets och rådets förordning (EG) nr 725/2004 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar (EUT L 129, 29.4.2004, s. 6).
(11) Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd (EUT L 310, 25.11.2005, s. 28).
(12) Europaparlamentets och rådets direktiv 2002/59/EG av den 27 juni 2002 om inrättande av ett övervaknings- och informationssystem för sjötrafik i gemenskapen och om upphävande av rådets direktiv 93/75/EEG (EUT L 208, 5.8.2002, s. 10).
(13) Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster (EUT L 157, 23.6.2015, s. 21).
(14) Europaparlamentets och rådets direktiv 2010/40/EU av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag (EUT L 207, 6.8.2010, s. 1).
(15) Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och om ändring av förordning (EU) nr 648/2012 (EUT L 176, 27.6.2013, s. 1).
(16) Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).
(17) Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 201, 27.7.2012, s. 1).
(18) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

(19) Europaparlamentets och rådets förordning (EU) 2022/2371 av den 23 november 2022 om allvarliga gränsöverskridande hot mot människors hälsa och om upphävande av beslut nr 1082/2013/EU (EUT L 314, 6.12.2022, s. 26).
(20) Europaparlamentets och rådets direktiv 2001/83/EG av den 6 november 2001 om upprättande av gemenskapsregler för humanläkemedel (EGT L 311, 28.11.2001, s. 67).
(21) Europaparlamentets och rådets förordning (EU) 2022/123 av den 25 januari 2022 om en förstärkt roll för Europeiska läkemedelsmyndigheten vid krisberedskap och krishantering avseende läkemedel och medicintekniska produkter (EUT L 20, 31.1.2022, s. 1).
(22) Europaparlamentets och rådets direktiv (EU) 2020/2184 av den 16 december 2020 om kvaliteten på dricksvatten (EUT L 435, 23.12.2020, s. 1).
(23) Rådets direktiv 91/271/EEG av den 21 maj 1991 om rening av avloppsvatten från tätbebyggelse (EGT L 135, 30.5.1991, s. 40).

BILAGA II

ANDRA KRITISKA SEKTORER

Sektor	Delsektor	Typ av entitet
1. Post- och budtjänster		Tillhandahållare av posttjänster enligt definitionen i artikel 2.1a i direktiv 97/67/EG, inbegripet tillhandahållare av budtjänster
2. Avfallshantering		Verksamhetsutövare som bedriver avfallshantering enligt definitionen i artikel 3.9 i Europaparlamentets och rådets direktiv 2008/98/EG (1), dock undantaget verksamhetsutövare vars huvudsakliga näringsverksamhet inte är av avfallshantering
3. Tillverkning, produktion och distribution av kemikalier		Företag som tillverkar ämnen och distribuerar ämnen eller blandningar som avses i artikel 3.9 och 3.14 i Europaparlamentets och rådets förordning (EG) nr 1907/2006 (2) samt företag som producerar varor enligt definitionen i artikel 3.3 i den förordningen genom att använda ämnen och blandningar
4. Produktion, bearbetning och distribution av livsmedel		Livsmedelsföretag enligt definitionen i artikel 3.2 i Europaparlamentets och rådets förordning (EG) nr 178/2002 (3) som bedriver grossisthandel och industriell produktion och bearbetning
5. Tillverkning	a) Tillverkning av medicintekniska produkter och medicintekniska produkter för *in vitro*-diagnostik	Entiteter som tillverkar medicintekniska produkter enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) 2017/745 (4)nligt definitionen i artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2017/746 (5), med undantag av entiteter som tillverkar sådana medicintekniska produkter som avses i punkt 5 femte strecksatsen i bilaga I i detta direktiv
	b) Tillverkning av datorer, elektronikvaror och optik	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 26 i Nace Rev. 2
	c) Tillverkning av elapparatur	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 27 i Nace Rev. 2
	d) Tillverkning av övriga maskiner	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 28 i Nace Rev. 2
	e) Tillverkning av motorfordon, släpfordon och påhängsvagnar	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 29 i Nace Rev. 2
	f) Tillverkning av andra transportmedel	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 30 i Nace Rev. 2

Sektor	Delsektor	Typ av enhet
6. Digitala leverantörer		— Leverantörer av marknadsplatser online
		— Leverantörer av sökmotorer
		— Leverantörer av plattformar för sociala nätverkstjänster
7. Forskning		Forskningsorganisationer

(1) Europaparlamentets och rådets direktiv 2008/98/EG av den 19 november 2008 om avfall och om upphävande av vissa direktiv (EUT L 312, 22.11.2008, s. 3).

(2) Europaparlamentets och rådets förordning (EG) nr 1907/2006 av den 18 december 2006 om registrering, utvärdering, godkännande och begränsning av kemikalier (Reach), inrättande av en europeisk kemikaliemyndighet, ändring av direktiv 1999/45/EG och upphävande av rådets förordning (EEG) nr 793/93 och kommissionens förordning (EG) nr 1488/94 samt rådets direktiv 76/769/EEG och kommissionens direktiv 91/155/EEG, 93/67/EEG, 93/105/EG och 2000/21/EG (EUT L 396, 30.12.2006, s. 1).

(3) Europaparlamentets och rådets förordning (EG) nr 178/2002 av den 28 januari 2002 om allmänna principer och krav för livsmedelslagstiftning, om inrättande av Europeiska myndigheten för livsmedelssäkerhet och om förfaranden i frågor som gäller livsmedelssäkerhet (EGT L 31, 1.2.2002, s. 1).

(4) Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (EUT L 117, 5.5.2017, s. 1).

(5) Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (EUT L 117, 5.5.2017, s. 176).

BILAGA III

JÄMFÖRELSETABELL

Direktiv (EU) 2016/1148	Detta direktiv
Artikel 1.1	Artikel 1.1
Artikel 1.2	Artikel 1.2
Artikel 1.3	–
Artikel 1.4	Artikel 2.12
Artikel 1.5	Artikel 2.13
Artikel 1.6	Artikel 2.6 och 2.11
Artikel 1.7	Artikel 4
Artikel 2	Artikel 2.14
Artikel 3	Artikel 5
Artikel 4	Artikel 6
Artikel 5	–
Artikel 6	–
Artikel 7.1	Artikel 7.1 och 7.2
Artikel 7.2	Artikel 7.4
Artikel 7.3	Artikel 7.3
Artikel 8.1–8.5	Artikel 8.1–8.5
Artikel 8.6	Artikel 13.4
Artikel 8.7	Artikel 8.6
Artikel 9.1, 9.2 och 9.3	Artikel 10.1, 10.2 och 10.3
Artikel 9.4	Artikel 10.9
Artikel 9.5	Artikel 10.10
Artikel 10.1, 10.2 och 10.3 första stycket	Artikel 13.1, 13.2 och 13.3
Artikel 10.3 andra stycket	Artikel 23.9
Artikel 11.1	Artikel 14.1 och 14.2
Artikel 11.2	Artikel 14.3
Artikel 11.3	Artikel 14.4 första stycket leden a–q och led s och 14.7
Artikel 11.4	Artikel 14.4 första stycket led r och andra stycket
Artikel 11.5	Artikel 14.8
Artikel 12.1–12.5	Artikel 15.1–15.5
Artikel 13	Artikel 17
Artikel 14.1 och 14.2	Artikel 21.1–21.4
Artikel 14.3	Artikel 23.1
Artikel 14.4	Artikel 23.3
Artikel 14.5	Artikel 23.5, 23.6 och 23.8

Direktiv (EU) 2016/1148	Detta direktiv
Artikel 14.6	Artikel 23.7
Artikel 14.7	Artikel 23.11
Artikel 15.1	Artikel 31.1
Artikel 15.2 första stycket a	Artikel 32.2 e
Artikel 15.2 första stycket b	Artikel 32.2 g
Artikel 15.2 andra stycket	Artikel 32.3
Artikel 15.3	Artikel 32.4 b
Artikel 15.4	Artikel 31.3
Artikel 16.1 och 16.2	Artikel 21.1–21.4
Artikel 16.3	Artikel 23.1
Artikel 16.4	Artikel 23.3
Artikel 16.5	–
Artikel 16.6	Artikel 23.6
Artikel 16.7	Artikel 23.7
Artikel 16.8 och 16.9	Artiklarna 21.5 och 23.11
Artikel 16.10	–
Artikel 16.11	Artikel 2.1, 2.2 och 2.3
Artikel 17.1	Artikel 33.1
Artikel 17.2 a	Artikel 32.2 e
Artikel 17.2 b	Artikel 32.4 b
Artikel 17.3	Artikel 37.1 a och b
Artikel 18.1	Artikel 26.1 b och 26.2
Artikel 18.2	Artikel 26.3
Artikel 18.3	Artikel 26.4
Artikel 19	Artikel 25
Artikel 20	Artikel 30
Artikel 21	Artikel 36
Artikel 22	Artikel 39
Artikel 23	Artikel 40
Artikel 24	–
Artikel 25	Artikel 41
Artikel 26	Artikel 45
Artikel 27	Artikel 46
Bilaga I punkt 1	Artikel 11.1
Bilaga I punkt 2 a i–iv	Artikel 11.2 a–d

Direktiv (EU) 2016/1148	Detta direktiv
Bilaga I punkt 2 a v	Artikel 11.2 f
Bilaga I punkt 2 b	Artikel 11.4
Bilaga I punkt 2 c i och ii	Artikel 11.5 a
Bilaga II	Bilaga I
Bilaga III punkterna 1 och 2	Bilaga II punkt 6
Bilaga III punkt 3	Bilaga I punkt 8

Införande av NIS2-direktivet

Kostnadsuppskattningar för myndigheterna

SWECO

Innehållsförteckning

1 Inledning 4
1.1 Om NIS1 och NIS2 direktiven 4
1.2 Om Swecos uppdrag 4
1.2.1 Beskrivning av uppdragets genomförande 5

2 Summering av myndigheternas kostnadsuppskattningar 6

3 Myndigheternas kostnadsuppskattningar för införandet av NIS2 direktivet 8
3.1 MSB:s roll som samordnare av NIS lagen 8
3.2 Myndigheter som idag utövar tillsyn enligt NIS1 direktivet 10
3.2.1 Statens Energimyndigheten 10
3.2.2 Transportstyrelsen 11
3.2.3 Inspektionen för vård och omsorg 12
3.2.4 Livsmedelsverket 13
3.2.5 Post och Telestyrelsen 14
3.3 Tillkommande myndigheter i samband med införandet av NIS2 direktivet 16
3.3.1 Läkemedelsverket 16
3.3.2 Länsstyrelsernas tillsynsuppdrag av säkerhetsskydd 18
3.3.3 Länsstyrelsen Skåne 18
3.3.4 Länsstyrelsen Stockholm 19
3.3.5 Länsstyrelsen Västra Götaland 20
3.3.6 Länsstyrelsen Norrbotten 20

4 Referenser 21
4.1 Skrivet material 21
4.2 Intervjuer 21

1 Inledning

1.1 Om NIS1 och NIS2-direktiven

Digitaliseringen innebär att en allt större andel av samhällets aktiviteter i olika grad är beroende av nätverk och informationssystem. Den digitala utvecklingen medför stora möjligheter som bland annat bättre tjänster och ökad effektivitet, men också risker. Därför är informations och cybersäkerhet i dag en fråga som angår hela samhället. Särskilt höga säkerhetskrav ska ställas när det gäller samhällsviktig verksamhet som, för att upprätthålla nödvändiga samhällsfunktioner, måste fungera under alla förhållanden.

Syftet med NIS direktivet var att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen. Direktivet gäller för leverantörer av samhällsviktiga tjänster inom sju särskilt utpekade sektorer: energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Vidare omfattas leverantörer av vissa digitala tjänster.

Direktivet har genomförts i svensk rätt genom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174), även kallad NIS lagen, och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Därutöver har främst Myndigheten för samhällsskydd och beredskap (MSB) meddelat föreskrifter.

EU har nyligen antagit det så kallade NIS2 direktivet, som ersätter det tidigare NIS direktivet. Syftet med det nya direktivet är att minska fragmenteringen av den inre marknaden genom att föreskriva minimiregler för ett samordnat regelverk. Tillämpningsområdet för regleringen utvidgas till att omfatta aktörer inom fler sektorer än det tidigare NIS direktivet. De tillkommande sektorerna är avloppsvatten, förvaltning av IKT tjänster (mellan företag), offentlig förvaltning, rymden, post och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, tillverkning, digitala leverantörer och forskning. Vidare skärps kraven på aktörer genom minimikrav för åtgärder som ska tillämpas för att hantera risker kopplade till säkerheten i respektive aktörs nätverk och informationssystem. NIS2 börjar gälla i hela EU den 18 oktober 2024. Exakt hur förändringen påverkar lagstiftning och verksamheter i Sverige är ännu inte helt klart. Regeringen har utsett en utredare med uppdrag att ta fram detaljerade förslag. Resultatet av utredningen presenteras senast den 23 februari 2024.

1.2 Om Swecos uppdrag

I november 2023 fick Sweco i uppdrag av utredningen Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft att klargöra de ökade kostnaderna som utredningens förslag om cybersäkerhetsreglering medför för de tio tillsynsmyndigheterna. De tio tillsynsmyndigheterna är: Statens Energimyndighet, Transportstyrelsen, IVO, Läkemedelsverket, Livsmedelsverket, Post och telestyrelsen och länsstyrelserna i Norrbotten, Skåne, Stockholm och Västra Götaland. Swecos uppdrag har en tydlig avgränsning; att klargöra de ökade kostnaderna för de aktuella och tillkommande tillsynsmyndigheterna i samband med införandet av NIS2 direktivet.

Statens Energimyndighet, Transportstyrelsen, IVO, Livsmedelsverket och Post och telestyrelsen är redan tillsynsmyndigheter och har redan snarlika uppgifter. För dessa fem myndigheter är fokus för analysen i vilken utsträckning införandet av NIS2 direktviet

medförde ökade kostnader. Utgångspunkt för analysen utgörs av de budgetmedel dessa fem myndigheter tillfördes till följd av regelverket om informationssäkerhet för samhällsviktiga och digitala tjänster som trädde i kraft 2018. Det möjliga behovet av ökade kostnader bör uppskattas förhållande till de budgetmedlen. Här ska beaktas att dessa myndigheter redan har byggt upp en tillsynsstruktur.

En första fråga är om och i så fall i vilken utsträckning det förändrade tillämpningsområdet, i samband med införandet av NIS2 direktivet, kan komma att påverka dessa fem tillsynsmyndigheternas kostnader. Förändringen för dessa fem myndigheter handlar därför om hur mycket det förhållande att den gällande lagen är begränsad till samhällsviktiga och digitala tjänster medan förslaget till cybersäkerhetslagen som huvudregel omfattar de enskilda verksamhetsutövarna inom sektorn som uppfyller storlekskravet. Vidare kommer nästan hela den offentliga sektorn att omfattas.

En andra fråga rör de fem tillsynsmyndigheter som inte har bedrivit tillsyn enligt NIS, det vill säga fyra länsstyrelser och Läkemedelsverket. För de tillkommande tillsynsmyndigheterna ska de initiala kostnaderna för att starta upp verksamheten och de löpande kostnaderna för att bedriva tillsynsverksamhet klargöras.

För MSB ska det göras en jämförelse mellan nu gällande uppgifter och de som utredningen föreslår. En analys ska göras om utredningens förslag medför ökade kostnader. Här ska också klargöras hur myndighetens arbete finansieras för närvarande, exempelvis om det finns någon finansiering från EU.

Swecos uppdrag förutsätter att de elva berörda myndigheterna bistår med kostnadsunderlag och annan, för frågeställningarna, relevant information.

1.2.1 Beskrivning av uppdragets genomförande

För att klargöra tillsynsmyndigheternas ökade kostnader i och med införandet av NIS2 direktivet genomfördes enskilda intervjuer med de tio tillsynsmyndigheterna och MSB i egenskap av samordningsmyndighet. Inför intervjuerna, som genomfördes digitalt, fick tillsynsmyndigheterna ta del av de intervjufrågor som skulle diskuteras under mötet. En viktig utgångspunkt för genomförandet av intervjuerna var Statskontorets utredning från 2018 där tillsyn enligt NIS direktivet utreddes. Intervjuguiden var strukturerad enligt följande; aktuell tillsynsverksamhets kostnader, uppskattade kostnader för tillkommande verksamhet enligt NIS2, uppdelat i initiala och löpande kostnader. Viktigt att notera är att utökning av verksamhet i och med införandet av NIS2 direktivet tog ett tre årsperspektiv.

För att säkerställa att de uppgifter som lämnades under intervjuerna var i linje med det intervjupersonerna avsåg skickades kostnadsuppskattningarna till intervjupersonerna i efterhand för verifiering. I samtliga intervjuer uppstod dock ett behov av att komplettera insamlat material. Fyra myndigheter inkom med kompletterande uppgifter. För att eventuellt komplettera de uppgifter som uppgavs i intervjuerna gjordes en genomgång av myndigheternas årsredovisningar från år 2022.

Kostnadsuppskattningarna per tillsynsmyndighet skrevs fram som fallstudier. Genom mellanfallsanalys summerades huvudpunkterna från fallstudierna i kapitel 2 med rekommendationer om områden som borde undersökas närmare.

2 Summering av myndigheternas kostnadsuppskattningar

Swecos uppdrag var att klargöra de ökade kostnaderna som införandet av NIS2 direktivet medför för de tio tillsynsmyndigheter (Statens energimyndighet, Transportstyrelsen, IVO, Läkemedelsverket, Livsmedelsverket, Post och telestyrelsen och länsstyrelserna i Norrbotten, Skåne, Stockholm och Västra Götaland) och MSB.

Av dessa är fem myndigheter, dvs. Statens energimyndighet, Transportstyrelsen, IVO, Livsmedelsverket och Post och telestyrelsen redan tillsynsmyndigheter och har redan snarlika uppgifter. För dessa fem myndigheter behöver analyseras om och i så fall vilken utsträckning utredningens förslag medför ökade kostnader.

De myndigheter som idag är tillsynsmyndigheter har utifrån befintlig verksamhet gjort uppskattningar av vad den utökade verksamheten, i och med införandet av NIS2 direktivet, skulle innebära. Dock ska dessa kostnadsuppskattningar behandlas med försiktighet då kostnadsuppskattningarna inte är i paritet med ökningen av tillsynsobjekt. Myndigheterna lyfter även själva att de inte har haft möjlighet att utreda i mer detalj vad utökningen av verksamheten, i och med införandet av NIS2 direktivet, kommer att innebära.

Läkemedelsverket, Länsstyrelsen Stockholm, Länsstyrelsen Norrbotten, Länsstyrelsen Skåne och Länsstyrelsen Västra Götaland har inte utövat tillsyn enligt NIS direktivet innan och för dessa fem myndigheterna är tillsyn enligt NIS2 direktivet ny verksamhet. Kostnadsuppskattningarna från dessa myndigheter ska därför hanteras med största försiktighet. I de fall kostnadsuppskattningar har uppgetts har myndigheterna utgått från aktuell verksamhet, tillsyn av säkerhetsskydd.

Kostnadsuppskattningarna, vilka utgår från en treårsperiod, för att utöka/bredda verksamheten i och med införandet av NIS2 direktivet är dels initiala kostnader, dels löpande kostnader.

Inom ramen för initiala kostnader är det kostnader för rekrytering, utformning av rutiner och arbetssätt, framtagande av föreskrifter, informationsinsatser, juridiskt stöd, fortutbildning samt IT stöd/teknisk utveckling.

Löpande kostnader härrör till årsarbetskrafter för genomförande av tillsyn och juridiskt stöd. I vissa fall har även kostnader för omvärldsbevakning, informationsinsatser och samordning tagits upp av myndigheterna.

I tabellen 1 på nästa sida presenteras de kostnadsuppskattningar som framkommit inom ramen för Swecos uppdrag. I de fall myndigheterna inte har haft möjlighet att uppge kostnader anges det med ingen uppgift (i.u) i tabellen.

Tabell 1. Summering av myndigheternas kostnadsuppskattningar år 1 till år 3

Myndighet	Estimerad kostnad	Kommentar
MSB	131 000 tkr	Avser organisatoriska förmågor och teknisk utveckling
Statens Energimyndighet	11 200 17 200 tkr	Preliminära och bör revideras/kompletteras
Transportstyrelsen	54 770 tkr	Avser åren 2025, 2026 och 2027.
IVO	38 000 tkr	Avser åren 2024, 2025 och 2026
Livsmedelsverket	25 700 26 200 tkr	Preliminära och bör revideras/kompletteras
Post och telestyrelsen	18 000 tkr	Avser endast löpande kostnader. Initiala kostnader för att starta upp den tillkommande verksamheten saknas
Läkemedelsverket	70 000 tkr	Uppskattade kostnader utan hänsyn till vad tillsynen de facto kommer att innebära
Länsstyrelsen Skåne	13 000 tkr	Avser enbart årsarbetskrafter.
Länsstyrelsen Stockholm	23 000 tkr	Avser enbart årsarbetskrafter
Länsstyrelsen Västra Götaland	i.u.	
Länsstyrelsen Norrbotten	i.u	
TOTAL	**384 670 391 170 tkr**	

Avslutningsvis, det går inte nog att understryka att de kostnadsuppskattningar som uppges i denna rapport är bristfälliga och bör beaktas med stor försiktighet. Swecos rekommendation är att kostnadsuppskattningarna från myndigheterna bör kompletteras för att få en tillförlitlig bild av vad införandet av NIS2 direktivet kommer att innebära.

3 Myndigheternas kostnadsuppskattningar för införandet av NIS2-direktivet

3.1 MSB:s roll som samordnare av NIS-lagen

Myndigheten för samhällsskydd och beredskap (MSB) har en samordnande roll för NIS lagen i Sverige. Det innebär bland annat att de tar fram övergripande regler för alla sektorer som omfattas av NIS lagen. Den samordnade rollen kommer MSB fortsatt att ha i och med tillämpningen att NIS2 direktivet från den 18 oktober 2024. MSB ser en ambitionshöjning i och med att myndigheten blir en cyberkrishanteringsmyndighet.

MSB var vid tillfället för Swecos uppdrag inne i en utredande fas där de arbetade på att ta fram kostnadsberäkningar för vad den nya rollen som cyberkrishanteringsmyndighet skulle innebära för myndigheten. I arbetet med att ta fram kostnadsberäkningar såg myndigheten en komplexitet i att det pågår flera parallella utredningar relaterat till införandet av NIS2 och CER vilket försvårade deras interna utredningsarbete.

De uppskattningar som MSB kunde uppge var kostnader för att stärka upp de organisatoriska och tekniska förmågorna (till exempel incidentrapportering, tillsynssamordning och kommunikationsinsatser).

Tabell 2. Kostnadsuppskattningar för att stärka organisatoriska och tekniska förmågor MSB

Personal 15,7 årsarbetskrafter, år 1 3	47 100 tkr
Tillkommande kostnader	65 500 tkr
Totalt	**112 600 tkr**

En annan kostnadspost som MSB uppgav var kostnader för tekniska utveckling där det främst handlade om att utveckla WIS, se tabell 3. Valet att vidareutveckla WIS för att omhänderta behoven i NIS2 i stället för att bygga ut nuvarande tekniska lösning motiveras av myndigheten enligt följande:

Analys av den tekniska miljö som behövs har visat att WIS är det bästa och mest kostnadseffektiva alternativet. Bakgrunden är att WIS är ett bra system/infrastruktur för informationsdelning som många redan idag använder. Det svarar också redan nu upp mot flera delar av det som NIS2 kommer att kräva avseende användarantal, funktionalitet, flexibilitet och säkerhet. Detta innebär att systemet endast förutsätter begränsad utveckling för att kunna användas för all informationsdelning inom ramen för NIS2 (både incidentrapporter och annan kommunikation). WIS har särskilt jämförts i förhållande till den tekniska miljö som idag används för incidentrapportering. Detta system (IRON) bedöms inte kunna ge den flexibilitet, användarvänlighet och enkla skalbarhet som krävs för att motsvara behoven i NIS2."[1]

[1] Skriftlig kommunikation den 11 jan 2024.

Tabell 3. Kostnadsuppskattningar för teknisk utveckling MSB

Personal: 6,4 årsarbetskrafter	6 400 tkr
Tillkommande kostnader	12 000 tkr
Totalt	**18 400 tkr**

Det är viktigt att notera att kostnadsuppskattningarna som presenteras ovan är preliminära och kan komma att revideras. MSB bedriver ett utredningsarbete som kommer att resultera i en helhetsbild av de ökade kostnaderna i samband med införandet av NIS2 direktivet. Det är i dagsläget oklart när MSB kan komma att komplettera och revidera kostnadsuppskattningarna.

3.2 Myndigheter som idag utövar tillsyn enligt NIS1-direktivet

3.2.1 Statens Energimyndigheten

Energimyndigheten har idag ansvar för tillsyn av 249 tillsynsobjekt inom Energisektorn. Sedan NIS direktivet trädde i kraft har myndigheten fokuserat på rekrytering, utbildning och kompetensutveckling. Under åren 2020 2022 har Energimyndigheten utfört 138 anmälningstillsyner och för närvarande, i december år 2023, pågår även sex planlagda tillsyner.

I tabell 4 nedan framgår antalet tillsyner som har genomförts vid Energimyndigheten under åren 2020 2022.

Tabell 4. Antal tillsyner under åren 2020 2022.

Tillsynsmyndighet	Antal tillsyner		
	2020	2021	2022
	18	18*	120

*samma 18 tillsyner pågick båda åren 2020 2021

Energimyndigheten ska återkomma med totalkostnader för tillsynen under åren 2020 2022 men utifrån antalet årsarbetskrafter[2], som är den största löpande kostnaden, kan en grov uppskattning göras av Sweco. Utifrån en varierande personalsammansättning om mellan 3 5 årsarbetskrafter årligen uppgår en uppskattad totalkostnad för personal till 3 5 miljoner kronor per år i dagsläget. Energimyndigheten uppger att tillsynsverksamheten för NIS1 i dagsläget är underdimensionerad.

Utredningen föreslår att Energimyndigheten fortsätter sin tillsyn inom energisektorn i enlighet med NIS2 direktivet. Myndighetens ansvar kommer emellertid att utökas genom att inkludera fler leverantörer och nya tematiska områden, såsom fjärrvärme. Det förväntas att 449 479 leverantörer kommer att beröras av NIS2 direktivet, vilket innebär en nästan fördubbling av antalet tillsynsobjekt. Energimyndigheten belyser att energisektorn är dynamisk och att nya aktörer ständigt tillkommer detta innebär att sektorn på sikt kan komma att växa betydligt.

Den utökade tillsynsomfattningen för Energimyndigheten förväntas leda till minst en fördubbling av tillsynsfrekvens och informationsinsatser, vilket i sin tur uppskattas kräva en fördubbling av antalet resurser. Myndigheten identifierar potentiella initiala kostnader som rekrytering och utbildning av personal, arbete med föreskrifter, utformning av nya rutiner och handböcker, kompetensutveckling inom nya områden och handläggarstöd under uppstartsperioden då en anmälningsvåg förväntas från berörda leverantörer. En ökning av incidentrapportering förutspås också, vilket skapar ett behov av att denna process omhändertas och utvecklas. En annan viktig aspekt som myndigheten belyser är skillnaden i kompetensnivå mellan små, mellanstora och stora företag när det gäller NIS2. Små företag har begränsade resurser att avsätta för utbildning och kompetensutveckling inom området till skillnad från större bolag.

[2] Varje årsarbetskraft uppskattas kosta 1 miljon kronor årligen.

Nedan uppgifter ska ses som preliminära och Energimyndigheten har inte bekräftat uppgifterna ska därför hanteras med stor försiktighet.

Tabell 5: Preliminära kostnader för tillsyn enligt NIS2, Energimyndigheten

Initiala kostnader*, tkr		**2 200**
Utformning av rutiner och handböcker		200
Handläggarstöd		2 000
Föreskrifter		
Kompetensutveckling		
Rekrytering och utbildning av ny personal		
Löpande kostnader, tkr, år1 3	**9 000**	**15 000**
Årsarbetskrafter**	9 000	15 000
Total kostnad	**11 200**	**17 200**

*ofullständig kostnadsuppskattning
**årsarbetskrafter inkluderar tillsynsarbete, informationsinsatser, arbete med föreskrifter och kontinuerlig rekrytering

Det är viktigt att notera att kostnadsuppskattningarna som presenteras ovan är preliminära och bör revideras och kompletteras. Det är i dagsläget oklart när Energimyndigheten kan komma att komplettera och revidera kostnadsuppskattningarna.

3.2.2 Transportstyrelsen

Transportstyrelsen har idag ansvar för tillsyn inom transportsektorn. Sedan NIS direktivet trädde i kraft har myndigheten fokuserat på rekrytering, metodutveckling, uppbyggnad av tillsynsverksamhet enligt NIS, vägledning, samverkan och utbildningsinsatser. Idag har myndigheten ansvar för tillsyn av 130 tillsynsobjekt. Som siffrorna visar i tabellerna 6 och 7 nedan har verksamheten expanderat betydligt under det nuvarande året både sett till tillsynsfrekvens och antal årsarbetskrafter.

I tabell 6 nedan framgår antalet tillsyner som har genomförts vid Transportstyrelsen under åren 2020 2023[3].

Tabell 6. Antal tillsyner mellan åren 2020 och 2023, Transportstyrelsen

Tillsynsmyndighet	Antal tillsyner			
	2020	2021	2022	2023*
	0	3	3	44

*avser fram till november

I tabell 7 nedan framgår Transportstyrelsens totala kostnader för tillsynen under åren 2020 2022.

Tabell 7.Total kostnad för tillsyn mellan åren 2020 och 2023, Transportstyrelsen

Tillsynsmyndighet	Total kostnad för tillsyn (tkr)			
	2020	2021	2022	2023*
	2 200	2 200	2 200	5 000

*avser fram till november

Utredningen föreslår att Transportstyrelsen fortsätter sin tillsyn inom transportsektorn och därtill upptar ansvaret för tillsyn inom tillverkningssektorn i enlighet med NIS2 direktivet. Detta medför, tillsammans med det nya storlekskravet och tillkommande trafikområden som

[33] Uppgifter om utförda tillsyner från myndigheten till Sweco skiljer sig från tidigare uppgifter till utredningen.

exempelvis järnväg och sjö, en mångdubbling av antalet tillsynsobjekt. Transportstyrelsen uppskattar att antal berörda leverantörer kommer att öka från 130 till 750.

Med denna utökade tillsynsomfattning förväntas en betydligt högre tillsynsfrekvens och för att möta detta uppskattar Transportstyrelsen ett behov av totalt 15 årsarbetskrafter. Ökningen är ca 10 årsarbetskrafter från nuvarande personalsammansättning. Myndigheten lyfter särskild komplexitet i att rekrytera personal med cybersäkerhetskompetens (särskilt i tekniskt avseende) och ser en internationell kompetensbrist inom detta område.

Transportstyrelsen identifierar potentiella initiala kostnader i och med rekrytering och utbildning av personal, kartläggning och tolkning av regelverk, arbete med föreskrifter, juriststöd, systemstöd och informationsinsatser till leverantörer under uppstartsperioden. De initiala kostnaderna uppskattas till 770 000 kronor.[4] Vid jämförelser med implementeringen av NIS kan man även se ett behov av att ta höjd för engångskostnader som konsultstöd. Myndigheten belyser att i det fall då matchande resurser för den ökade tillsynsomfattningen inte skulle göras tillgänglig blir metodutveckling och effektivisering av arbetsprocesser en betydande initial kostnad eftersom förutsättningar att utföra tillsyn enligt NIS2 inte finns i dagsläget.

Med hänsyn till ovan nämnda aspekter uppskattar Transportstyrelsen en årlig totalkostnad på 18 miljoner kronor för tillsyn enligt NIS2 år 2025, vilket är en ökning på 13 miljoner kronor från år 2023. Om vi utgår från att år 2025 utgör år 1 för kostnader för tillsyn enligt NIS2 blir totala kostnaden för tre år 54 mkr. Transportstyrelsen räknar på en kostnad per årsarbetskraft på mellan 1,1 mkr och 1,28 mkr. Se tabell 8 nedan.

Tabell 8: Preliminära kostnader för tillsyn enligt NIS2, Transportstyrelsen[5]

År	Antal tillsyner	Årsarbete	Kostnad
2020	0	2	2,2 mkr
2021	3	2	2,2 mkr
2022	3	2	2,2 mkr
2023	44	4,5	5 mkr
2024	60	7	9 mkr
2025	150	15	18 mkr

Transportstyrelsen är den myndighet som inkommit med det mest kompletta underlaget. Den kostnadspost som saknas är tillkommande kostnad för teknisk utveckling/systemstöd.

3.2.3 Inspektionen för vård och omsorg

Inspektionen för vård och omsorg (IVO) har idag ansvar för tillsyn inom hälso och sjukvård. Myndigheten uppskattar att denna av tillsyn berör 240 tillsynsobjekt, både privata och kommunala. I tabell 9 nedan framgår antalet tillsyner som har genomförts vid IVO under åren 2020 2022. Den löpande totalkostnaden för tillsynsarbetet uppskattas år 2022 till nästan 8,5 miljoner kronor, vilket framgår av tabell 10 nedan.

Tabell 9. Antal tillsyner mellan åren 2020 och 2022, IVO

Tillsynsmyndighet	Antal tillsyner		
	2020	2021	2022
	21	13	13

[4] Kostnadsuppskattningar som inkom via mejl den 11 december 2023.
[5] Kostnadsuppskattningar som inkom via mail den 11 december 2023.

Tabell 10. Totala kostnader för tillsyn under åren 2020 till 2022, IVO.

Tillsynsmyndighet	Total kostnad för tillsyn (tkr)		
	2020	2021	2022
	6 616 tkr	8 929 tkr	8 476 tkr

Utredningen föreslår att IVO fortsätter sin tillsyn inom hälso och sjukvårdssektorn (vårdgivare) medan Läkemedelsverket upptar ansvar för tillsyn av övriga aktörer inom sektorn i enlighet med NIS2 direktivet. Det nya storlekskravet medför en betydande ökning av antalet tillsynsobjekt. Myndigheten uppskattar att antalet berörda aktörer kommer att öka från nuvarande 240 till 819.

För att möta den utökade tillsynsomfattningen uppskattar myndigheten en ökning av antalet resurser. Myndigheten anger att initiala kostnader kan förväntas för rekrytering och utveckling för systemstöd och identifierar även ökade kostnader för informationsinsatser. Kostnadsuppskattningar för tillsyn utgår från att den är egeninitierad (dvs inte styrs med frekvens i författning). Då Socialstyrelsen har föreskriftsansvar uppskattas inga kostnader inom detta område.

Tabell 11: Preliminära kostnader för tillsyn enligt NIS2, IVO

Initiala kostnader, tkr	**6 000**
År 1, Juridisk bedömning, projektuppdrag, projektledare, arbetsgrupp, omvärldsanalys/benchmarking, kompetensinventering, IT stöd, År 1	3 000
År 1, Informationsinsatser	5 00
År 2, Implementeringskostnad: projektuppdrag, projektledare, rekryteringskostnader, IT stöd.	2 500
Löpande kostnader, tkr	**32 000**
År 1, Tillsyn	10 000
År 2, Tillsyn	11 000
År 3, Tillsyn	11 000
Total kostnad, tkr	**38 000**

3.2.4 Livsmedelsverket

Livsmedelsverket har idag ansvar för tillsyn inom leverans och distribution av dricksvatten. Sedan NIS direktivet trädde i kraft har fokus varit på rekrytering, utformning av rutiner och föreskrifter, samverkan och informationsinsatser till leverantörer. Idag har myndigheten ansvar för tillsyn av 95 100 tillsynsobjekt.

I samband med NIS direktivets införande år 2018 gjorde Livsmedelsverket en initial uppskattning av fem årsarbetskrafter, vilket på grund av kompetensbrist stannade av vid dagens fyra årsarbetskrafter. Med denna personalsammansättning har utfallet för verksamheten uppgått till omkring sju miljoner kronor per år. I tabell 12 nedan framgår antalet tillsyner som har genomförts vid Livsmedelsverket under åren 2020 2022. I tabell 13 presenteras Livsmedelsverkets totala kostnader för tillsyn årligen.

Tabell 12. Antal tillsyner under åren 2020 till 2022, Livsmedelsverket

Tillsynsmyndighet	Antal tillsyner		
	2020	2021	2022
	29	20	28

Tabell 13. Total kostnad för tillsyn under åren 2020 till 2022, Livsmedelsverket

Tillsynsmyndighet	Total kostnad för tillsyn (tkr)		
	2020	2021	2022
	7 000	7 000	7 000

Utredningen föreslår att Livsmedelsverket fortsätter sin tillsyn inom dricksvattenssektorn och därtill upptar ansvaret för tillsyn inom sektorerna avloppsvatten och livsmedel i enlighet med NIS2 direktivet. Detta medför vissa helt nya tematiska områden för tillsynen och innebär, tillsammans med det nya storlekskravet, en mångdubbling av antalet tillsynsobjekt. Livsmedelsverket uppskattar att antal berörda leverantörer kommer att öka från 95 100 till 525 675.

För att möta den utökade tillsynsomfattningen uppskattar myndigheten ett behov av totalt 8 årsarbetskrafter, vilket innebär en fördubbling av antalet resurser jämfört med nuläget. Livsmedelsverket identifierar tillsynsfrekvens, informationsinsatser till leverantörer, omvärldsbevakning, samordning, IT förvaltning, resor och expertisstöd (juriststöd, konsultstöd etc) som områden för löpande kostnader, varav flertalet eller alla kommer att expandera i och med införandet av NIS2. Därtill kommer det att finnas behov av rekrytering och utbildning av personal som medför initiala kostnader tillsammans med tolkning av lagstiftning och konsultstöd. Myndigheten ser även ett behov av att utveckla det nuvarande systemet för reaktiv tillsyn.

Tabell 14: Preliminära kostnader för tillsyn enligt NIS2, Livsmedelsverket

Initiala kostnader*, tkr	**500 1 000**
Rekrytering och utbildning av personal	
Tolkning av lagstiftning	
Konsultstöd	500 1 000
Systemstöd/Utveckling av system	
Löpande kostnader, tkr, år 1 3	**25 200**
Årsarbetskrafter**	24 000
Juriststöd	1 200
Total kostnad	**25 700 26 200**

*ofullständig kostnadsuppskattning
**årsarbetskrafter inkluderar informationsinsatser, tillsynsarbete, IT förvaltning, föreskrifter, omvärldsbevakning och samordning

Det är viktigt att notera att kostnadsuppskattningarna som presenteras ovan är preliminära och bör revideras och kompletteras. Det är i dagsläget oklart när Livsmedelsverket kan komma att komplettera och revidera kostnadsuppskattningarna.

3.2.5 Post och Telestyrelsen

Post och telestyrelsen (PTS) har idag ansvar för tillsyn inom digital infrastruktur. Sedan NIS direktivet trädde i kraft har myndighetens arbete involverat bland annat informationsinsatser till leverantörer, föreskrifter, tillsynsarbete, samverkan och incidentrapportering. Fram till november år 2023 har 39 tillsyner utförts. Myndigheten uppskattar att de har ett 60 tal tillsynsobjekt varav enbart 8 är anmälningsskyldiga. Tillsynsarbete (enligt LEK) är idag finansierat via anmälningsavgifter. Post och telestyrelsen återkommer om totalkostnad per år för tillsynsarbetet.

Utredningen föreslår att PTS fortsätter sin tillsyn inom digital infrastruktur och därtill upptar ansvaret för tillsyn inom sektorerna digitala leverantörer, förvaltning av IKT tjänster, post

och budtjänster och rymden i enlighet med NIS2 direktivet. Detta medför vissa helt nya tematiska områden för tillsynen och innebär, tillsammans med det nya storlekskravet, en ökning av antalet tillsynsobjekt. PTS har under hösten låtit genomföra en marknadsanalys för att ta reda på hur många nya aktörer NIS2 kommer att innebära för PTS. Enligt denna analys kommer antalet tillsynsobjekt att öka till ca 1100 med NIS2[6]. Det finns en hel del osäkerhet i dessa siffror eftersom definitionerna inte är helt tydliga samt att alla aktörer inte nödvändigtvis har huvudsakligt etableringsställe i Sverige och därför kan komma att regleras från ett annat EU land.[7]

Efter ikraftträdande av NIS2 kommer PTS av allt att döma att ansvara för betydligt fler tillsynsobjekt, samt ha tillsynsansvar över fler sektorer än idag. Det innebär ett väsentligt utökat område för att bedriva både planlagd och händelsestyrd tillsyn. Det kommer bland annat att krävas fler resurser för att kunna bedriva händelsestyrd tillsyn, tex efter inträffade incidenter.[8] För att möta den utökade tillsynsomfattningen uppskattar myndigheten ett behov av ytterligare sex årsarbetskrafter utöver de 20 årsarbetskrafter som idag arbetar inom området.

PTS bedömer att för att kunna stärka myndighetens arbete på detta område behövs både juridisk och teknisk kompetens samt cybersäkerhetskompetens. Myndigheten gör även bedömningen att då många av de tillkommande aktörerna och sektorerna är nya för PTS ur ett tillsynsperspektiv så behöver myndigheten också bygga upp en kunskapsbas och bygga kompetens internt för att kunna granska tex regelefterlevnad på ett effektivt sätt. Dessutom är PTS en ny tillsynsmyndighet för många av de nya aktörerna, vilket kan medföra behov av extra informationsarbete. PTS vet av erfarenhet att det är mer tidskrävande att bedriva tillsyn över tillsynsovana aktörer.

Då verksamheten hos PTS behöver växa tillkommer också kostnader i att rekrytera och kompetensutveckla nya medarbetare. Ny reglering med för PTS nya sektorer och med nya aktörer innebär också att både nya och befintliga medarbetare behöver kompetensutvecklas inom dessa sektorer.

Det tillsynsarbete som PTS bedriver inom området säkerhet i nät och tjänster finansieras idag av avgifter från anmälda aktörer. Enligt lagen (2022:482) om elektronisk kommunikation (LEK) måste alla som avser att tillhandahålla vissa elektroniska kommunikationsnät och kommunikationstjänster göra en anmälan till PTS innan de påbörjar verksamheten. Anmälda aktörer ska även betala vissa avgifter. En del av dessa avgifter utgörs av årlig avgift för tillsyn enligt LEK och tas alltså ut av de anmälningspliktiga operatörer som PTS har tillsyn över. Avgifterna baseras på operatörernas storlek på omsättning, och det är regeringen som beslutar om avgiftsnivåer för anmälningsplikten och nummer genom bestämmelser i finansieringsförordningen. Avgifterna sätts utifrån principen om full kostnadstäckning.[9]

Nuvarande NIS och kommande NIS2/CER reglering kommer att finansieras via förvaltningsanslaget. Eftersom vissa delar av LEK kommer att flyttas över till NIS2 regleringen kommer även kostnaden för dessa delar att behöva flyttas över till förvaltningsförslaget. Av nuvarande bemanning är det 8 årsarbetskrafter som kommer behöva byta finansiering från avgifter till förvaltningsanslag.[10]

PTS identifierar potentiella initiala kostnader som arbete med föreskrifter, förberedande arbete med analyser, rekrytering och utbildning av personal, utarbetning av rutiner, tolkning av regelverk, harmoniseringsarbete och samverkan. Myndigheten ser att frekvensen av incidentrapportering kommer att öka samtidigt behovet av informationsinsatser till

[6] Tillsyn enligt LEK kommer att gå in under tillsyn enligt NIS2
[7] Komplettering via mail den 22 december 2023
[8] Komplettering via mail den 22 december 2023
[9] Komplettering via mail den 12 januari 2024
[10] Komplettering via mail den 12 januari 2024

leverantörer växer och den djuplodade tillsynen blir mer tidskrävande. De belyser behovet av förändrade och nya verktyg för hantering av incidenter, anmälan enligt NIS2 samt register för anmälda aktörer. Arbetsbelastningen förväntas öka även med avseende på att alla berörda leverantörer ska anmäla sig i och med införandet av NIS2 direktivet.

En annan viktig aspekt som PTS belyser är att det är en tidskrävande initial process att sätta sig in i och lära sig nya sektorer, tematiska områden och regleringar.

Tabell 15: Preliminära kostnader för tillsyn enligt NIS2, PTS

Initiala kostnader*, tkr	
Rekrytering och utbildning av personal	
Föreskrifter	
Tolkning av regelverk	
Förberedande arbete med analyser	
Utarbetning av nya rutiner	
Harmoniseringsarbete och samverkan	
Systemstöd/Utveckling av system	
Informationsinsatser	
Löpande kostnader, tkr, år 1 3	**18 000**
Årsarbetskrafter**	18 000
Total kostnad	**18 000**

*ofullständig kostnadsuppskattning
**årsarbetskrafter inkluderar informationsinsatser, tillsynsarbete, omvärldsbevakning och samordning

Det är viktigt att notera att kostnadsuppskattningarna som presenteras ovan är preliminära och bör revideras och kompletteras. Det är i dagsläget oklart när Post och telestyrelsen kan komma att komplettera och revidera kostnadsuppskattningarna.

3.3 Tillkommande myndigheter i samband med införandet av NIS2-direktivet

3.3.1 Läkemedelsverket

Läkemedelsverkets tillsynsuppdrag spänner över ett stort område som omfattar produkter och system inom läkemedel, medicintekniska produkter, narkotika/narkotikaprekursorer, kosmetiska produkter och tatueringsfärger. Dessa styrs av olika regelverk på nationell och europeisk nivå.[11]

I och med införandet av NIS2 kommer myndigheten får ansvar för hälso och sjukvårdssektorn, övrigt och tillverkning. Myndigheten uppgav att detta är helt nya tillsynsområden och att de idag inte har de kompetenser som krävs för att genomföra tillsyn enligt NIS2 direktivet. Myndigheten beskrev även att de behöver kunskap om vad NIS2 innebär för att på bästa sätt förstå hur tillsynsverksamheten ska organiseras. Myndigheten behöver även utreda vad tillsynen kommer att bestå av och hur många tillsynsobjekt som är aktuella. Läkemedelsverket för en dialog med myndigheten IVO i syfte att ta fram kostnadsberäkningar för den nya tillsynsverksamheten.

[11] Läkemedelsverkets årsredovisning 2022

I tabell 16 framgår vilka kostnadsposter som diskuterades under intervjun och som Läkemedelsverket inkom med kompletterande underlag[12] om.

[12] Komplettering inkom den 10 januari 2024 via mejl.

Tabell 16: Preliminära kostnader för tillsyn enligt NIS2, Läkemedelsverket

	tkr
Initiala kostnader	10 000
Rekrytering av personal	
Uppstart av verksamhet (organisation och processer)	
Utveckling/inköp av IT system	
Löpande kostnader, år 1 3	60 000
Årsarbetskrafter	
Informationsinsatser	
Föreskriftsarbete	
Juridiskt stöd	
Total kostnad	**70 000**

Läkemedelsverket betonar att kostnadsuppskattningarna är preliminära och kommer att behöva kompletteras/revideras.

3.3.2 Länsstyrelsernas tillsynsuppdrag av säkerhetsskydd

Länsstyrelserna i Norrbotten, Skåne, Stockholm och Västra Götaland ansvarar för tillsynen av säkerhetsskydd. Ansvaret innebär tillsyn över:

- kommuner och regioner
- enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet och som inte står under tillsyn av andra tillsynsmyndigheter
- myndigheter som saknar utpekad tillsynsmyndighet och har sin placering inom länsstyrelsernas utpekade geografiska tillsynsområden.[13]

I tillsynsuppdraget ingår att

- genomföra samråd vid vissa säkerhetsskyddsavtal och överlåtelser.
- inleda ett samråd vid vissa säkerhetsskyddsavtal och överlåtelser, om verksamhetsutövaren inte gjort det.
- besluta om placering av befattningar i säkerhetsklass 2 och 3 när det gäller anställning eller annat deltagande i verksamhet hos enskilda verksamhetsutövare som står under vår tillsyn.
- besluta om förelägganden, sanktionsavgifter och i vissa fall förbud.
- ge vägledning om säkerhetsskydd.[14]

Länsstyrelserna i Norrbotten, Skåne, Stockholm och Västra Götaland ska få tillsynsansvar enligt NIS2 direktivet för avfallshantering, forskning, offentlig förvaltning, tillverkning och tillverkning, produktion och distribution av kemikalier.

3.3.3 Länsstyrelsen Skåne

Länsstyrelsen Skåne har tillsynsansvar för Kalmar, Blekinge, Kronoberg samt Skånes län. Enheten som arbetar med tillsynen bildades för två år sedan och de uppgifter som anges

[13] https://www.lansstyrelsen.se/skane/samhalle/sakerhet-och-beredskap/tillsyn-av-sakerhetsskydd.html

[14] https://www.lansstyrelsen.se/skane/samhalle/sakerhet-och-beredskap/tillsyn-av-sakerhetsskydd.html

gällande breddning av verksamheten till att även omfatta NIS2 direktivet bygger på erfarenheterna av att etablera verksamheten enligt tillsyn av säkerhetsskydd. Idag arbetar åtta personer på enheten och tre årsarbetskrafter arbetar med tillsyn enligt säkerhetsskydd.

Vid en breddning av verksamheten till att omfatta tillsyn enligt NIS2 direktivet uppskattar Länsstyrelsen Skåne att uppstartsfasen kommer att kräva en årsarbetskraft[15] för att samordna uppstarten av NIS2. Under uppstartsfasen avser man även med att rekrytera handläggare till gruppen som ska arbeta med NIS2. NIS2 och CER kommer att ingå i det pågående arbetet med säkerhetsskyddet. Detta innebär att det kommer ske prioriteringar med de resurser vi har.

Löpande kostnader för att arbeta med tillsyn uppskattas till fyra årsarbetskrafter fördelade på sex till åtta personer. Vidare framhålls att det är kommuner och andra myndigheter som styr och dimensionerar tillsynsverksamheten. Proaktiva insatser är det som myndigheten behöver dimensionera för, reaktiva händer är mindre resurskrävande.

Informationsinsatser kommer att bli mer resurskrävande i ett initialt skede men myndigheten kommer att hantera detta genom omprioriteringar av resurser. Kostnaderna i tabell 17 ska ses som preliminära och kan komma att revideras.

Tabell 17: Preliminära kostnader för tillsyn enligt NIS2, Länsstyrelsen Skåne

	tkr
Initiala kostnader	**1 000**
Samordnare, en årsarbetskraft	1 000
Löpande kostnader, år 1 3	**12 000**
Inspektörer/handläggare, fyra årsarbetskrafter	12 000
Total kostnad	**13 000**

3.3.4 Länsstyrelsen Stockholm

Länsstyrelsen Stockholm har tillsynsansvar för Södermanland, Västmanland, Dalarna, Värmland, Gävleborg, Uppsala, Örebro, Gotland samt Stockholms län. Kostnadsuppskattningar för införandet av NIS2 direktivet jämförs med befintlig verksamhet som bedrivs för tillsyn enligt säkerhetsskydd. För närvarande arbetar tre årsarbetskrafter inom avdelningen och antalet tillsynsobjekt uppskattas till 180 aktörer.

I och med införandet av NIS2 direktivet kommer myndigheten att behöva förvärva kompetens inom en ny form av tillsyn. Rekrytering och utbildning av personal identifieras som den största löpande kostnaden och en grov uppskattning görs till ett behov av minst sex årsarbetskrafter samt en årsarbetskraft för juridiskt stöd. Länsstyrelsen ser även behov av att utveckla nya system och ha ett kontinuerligt systemstöd. De lyfter kompetensbrist inom NIS och cybersäkerhet, både hos leverantörer och tillsynsmyndigheter, som en viktig fråga i och med införandet av det nya direktivet och belyser även att omvärldsbevakning kommer att bli betydligt mer tidskrävande framöver.

Tabell 18: Preliminära kostnader för tillsyn enligt NIS2, Länsstyrelsen Stockholm

	tkr
Initiala kostnader	**1 250**
Informatör, en årsarbetskraft	1 250
Löpande kostnader år 1 3	**21 750**
Inspektörer/handläggare, fem årsarbetskrafter	18 000

[15] Kostnad för en årsarbetskraft uppskattas till en miljon kronor om året.

Juridiskt stöd	3 750
Total kostnad	**23 000**

Länsstyrelsen Stockholm uppgav kostnadsuppskattningar för tillkommande årsarbetskrafter men bör komplettera med tillkommande kostnader för informationsinsatser, föreskriftsarbete och teknisk utveckling.

3.3.5 Länsstyrelsen Västra Götaland

Länsstyrelsen Västra Götaland har tillsynsansvar för Halland, Östergötland, Jönköping samt Västra Götalands län.

I dagsläget är verksamheten bemannad med tre handläggare, en administratör och en jurist på 60%. Antal tillsynsobjekt är 110, dock är det flera verksamhetsutövare som antas vara okända. Enheten har genomfört nio tillsyner inom säkerhetsskydd hittills. Målet är att genomföra 26 tillsyner årligen.

Myndigheten har inte tagit fram kostnadsberäkningar för införandet av NIS2 direktivet. För att kunna genomföra en utredning av denna magnitud efterfrågar myndigheten ett regeringsuppdrag eller liknande där det efterfrågas att myndigheten inkommer med kostnadsberäkningar.

Tabell 19: Preliminära kostnader för tillsyn enligt NIS2, Länsstyrelsen Västra Götaland

	tkr
Initiala kostnader	
Löpande kostnader	
Total kostnad	

Länsstyrelsen Västra Götaland kunde vid tidpunkten för Swecos uppdrag inte ange kostnadsuppskattningar för verksamheten tillsyn enligt NIS2 direktivet. Myndigheten efterfrågade ett regeringsuppdrag dör att kunna ta fram kostnadsuppskattningar.

3.3.6 Länsstyrelsen Norrbotten

Länsstyrelsen Norrbotten har tillsynsansvar för säkerhetsskydd för Västerbotten, Jämtland, Västernorrland samt Norrbottens län. Myndigheten inkom med uppskattningar på antalet tillkommande tillsynsobjekt i och med införandet av NIS2 direktivet. Dock ställde myndigheten inte upp på en intervju trots påminnelser.

Tabell 20: Preliminära kostnader för tillsyn enligt NIS2, Länsstyrelsen Skåne

	tkr
Initiala kostnader	
Löpande kostnader	
Total kostnad	

Länsstyrelsen Norrbotten behöver inkomma med uppgifter gällande kostnader, både initiala och löpande kostnader, för tillsyn enligt NIS2 direktivet.

4 Referenser

4.1 Skrivet material

Energimyndigheten, årsredovisning 2022

IVO, årsredovisning 2022

Kommittédirektiv. Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft Beslut vid regeringssammanträde den 23 februari 2023

Livsmedelsverket. Årsredovisning 2022

Läkemedelsverket, årsredovisning 2022

Länsstyrelsen Norrbotten, årsredovisning 2022

Länsstyrelsen Skåne, årsredovisning 2022

Länsstyrelsen Stockholm, årsredovisning 2022

Länsstyrelsen Västra Götaland, årsredovisning 2022

MSB, årsredovisning 2022

Post och telestyrelsen, årsredovisning 2022

Statskontoret (2018). Tillsyn enligt NIS direktivet kostnader och finansiering. 2018:7.

Transportstyrelsen, årsredovisning 2022

4.2 Intervjuer

Kan kompletteras efter överenskommelse.

Jämförelsetabell

Artikel i NIS2-direktivet	Svensk rätt[1]
1	1 kap. 1 §
2.1	1 kap. 3 och 4 §§
2.2	1 kap. 7 och 8 §§
2.3	-
2.4	1 kap. 7 §
2.5	1 kap. 3 och 4 §§
2.6	1 kap. 14 §
2.7	1 kap. 11 och 12 §§
2.8	1 kap. 13 §
2.9	1 kap. 13 §
2.10	1 kap. 10 §
2.11	1 kap. 14 §
2.12	-
2.13	-
2.14	-
3.1 och 3.2	2 kap. 1 §
3.3	14 § förordningen
3.4	2 kap. 2 §
3.5	25 § förordningen
3.6	-
4.1 och 4.2	1 kap. 9 §
4.3	-
5	-
6	1 kap. 2 §
7	-
8.1	4 kap. 1 § och 8 § förordningen
8.2	4 kap. 2 §
8.3	20 § förordningen

[1] Om inget annat anges avses utredningens förslag till cybersäkerhetslag. Med förordningen avses utredningens förslag till cybersäkerhetsförordning.

Artikel i NIS2-direktivet	Svensk rätt[1]
8.4	21 § förordningen
8.5	-
8.6	-
9.1	31 § förordningen
9.2	-
9.3	-
9.4	-
9.5	-
10.1	27 § förordningen
10.2	-
10.3	28 § förordningen
10.4	29 § förordningen
10.5	-
10.6	29 § förordningen
10.7–10	-
11 och 12.1	28–30 §§ förordningen
12.2	-
13.1	-
13.2	29 § förordningen
13.3–6	-
14	-
15	-
16	-
17	-
18	-
19	-
20.1	5 kap. 8 §
20.2	3 kap. 3 §
21.1–3	3 kap. 1 §
21.4	4 och 5 kap.
22	-
23.1	3 kap. 5–7 §§
23.2	3 kap. 6 §
23.3	3 kap. 4 §
23.4 a	3 kap. 5 §
23.4 b och c	3 kap. 6 §
23.4 d och e	3 kap. 7 §
23.5	29 § förordningen
23.6	23 och 29 §§ förordningen
23.7	29 § förordningen

Artikel i NIS2-direktivet	Svensk rätt[1]
23.8	23 § förordningen
23.9	24 § förordningen
23.10–11	-
24	-
25	-
26.1	1 kap. 4 §
26.1 a	1 kap. 5 §
26.1 b	1 kap. 6 §
26.1 c	1 kap. 3 §
26.2	3 § förordningen
26.3	1 kap. 6 §
26.4	-
26.5	-
27.1	-
27.2	2 kap. 2 §
27.3	2 kap. 2 §
27.4	25 § förordningen
27.5	-
28.1 och 28.2	Förslag till 1, 2 och 6 §§ toppdomänlagen
28.3	-
28.4	-
28.5	Förslag till 6 § toppdomänlagen
28.6	-
29	29 § förordningen
30	-
31.1	4 kap. 2 §
31.2	-
31.3	15 § förordningen
31.4	-
32.1	-
32.2 a och e–g	4 kap. 4–5 §§
32.2 b–c	4 kap. 8 § och 39 § förordningen
32.2 d	4 kap. 9 §
32.3	38 § förordningen
32.4 a	5 kap. 2 §
32.4 b–d och f	5 kap. 6 §
32.4 g	-
32.4 e och h	5 kap. 7 §
32.4 i	5 kap. 12 §
32.5 a	-

Artikel i NIS2-direktivet	Svensk rätt[1]
32.5 b	5 kap. 8 och 9 §§
32.6	-
32.7	5 kap. 3–5 och 16 §§
32.8	-
32.9	-
32.10	16 § förordningen
33.1	4 kap. 3 §
33.2 a och d–f	4 kap. 4–5 §§
33.2 b–c	4 kap. 8 § och 39 § förordningen
33.2 d	4 kap. 9 §
33.3	38 § förordningen
33.4 a	5 kap. 2 §
33.4 b–d och f	5 kap. 6 §
33.4 e och g	5 kap. 7 §
33.4 h	5 kap. 12 §
33.5	5 kap. 3–5 och 16 §§
33.6	16 § förordningen
34.1	5 kap. 16 §
34.2	5 kap. 2 och 12 §§
34.3	5 kap. 3–5 och 16 §§
34.4–5	5 kap. 13–15 §§
34.6	5 kap. 6 §
34.7	5 kap. 12–15 §
34.8	-
35.1	15 § förordningen
35.2	5 kap. 17 §
35.3	15 § förordningen
36	5 kap. 6–9 och 13–15 §§
37	17–18 §§ förordningen
38	-
39	-
40	-
41	Bestämmelserna om ikraftträdande i författningsförslagen
42	-
43	-
44	-
45	-
46	-

Statens offentliga utredningar 2024

Kronologisk förteckning

1. Ett starkare skydd för offentliganställda mot våld, hot och trakasserier. Ju.
2. Ett samordnat vaccinationsarbete – för effektivare hantering av kommande vacciner. Del 1 och 2. S.
3. Ett starkt judiskt liv för framtida generationer. Nationell strategi för att stärka judiskt liv i Sverige 2025–2034. Ku.
4. Inskränkningarna i upphovsrätten. Ju.
5. Förbättrad ordning och säkerhet vid förvar. Ju.
6. Steg mot stärkt kapacitet. Fi.
7. Ett säkrare och mer tillgängligt fastighetsregister. Ju.
8. Livsmedelsberedskap för en ny tid. LI.
9. Utvecklat samarbete för verksamhetsförlagd utbildning – långsiktiga åtgärder för sjuksköterskeprogrammen. U.
10. Preskription av avlägsnandebeslut och vissa frågor om återreseförbud. Ju.
11. Rätt frågor på regeringens bord – en ändamålsenlig regeringsprövning på miljöområdet. KN.
12. Mål och mening med integration. A.
13. En effektivare kontaktförbudslagstiftning – ett utökat skydd för utsatta personer. Ju.
14. Arbetslivskriminalitet – myndighetssamverkan, en gemensam tipsfunktion, lärdomar från Belgien och gränsöverskridande arbete. A.
15. Nya regler för arbetskraftsinvandring m.m. Ju.
16. Växla yrke som vuxen – en reformerad vuxenutbildning och en ny yrkesskola för vuxna. U.
17. Skolor mot brott. U.
18. Nya regler om cybersäkerhet. Fö.

Statens offentliga utredningar 2024

Systematisk förteckning

Arbetsmarknadsdepartementet

Mål och mening med integration. [12]

Arbetslivskriminalitet – myndighetssamverkan, en gemensam tipsfunktion, lärdomar från Belgien och gränsöverskridande arbete. [14]

Finansdepartementet

Steg mot stärkt kapacitet. [6]

Försvarsdepartementet

Nya regler om cybersäkerhet. [18]

Justitiedepartementet

Ett starkare skydd för offentliganställda mot våld, hot och trakasserier. [1]

Inskränkningarna i upphovsrätten. [4]

Förbättrad ordning och säkerhet vid förvar. [5]

Ett säkrare och mer tillgängligt fastighetsregister. [7]

Preskription av avlägsnandebeslut och vissa frågor om återreseförbud. [10]

En effektivare kontaktförbudslagstiftning – ett utökat skydd för utsatta personer. [13]

Nya regler för arbetskraftsinvandring m.m. [15]

Klimat- och näringslivsdepartementet

Rätt frågor på regeringens bord – en ändamålsenlig regeringsprövning på miljöområdet. [11]

Kulturdepartementet

Ett starkt judiskt liv för framtida generationer. Nationell strategi för att stärka judiskt liv i Sverige 2025–2034. [3]

Landsbygds- och infrastrukturdepartementet

Livsmedelsberedskap för en ny tid. [8]

Socialdepartementet

Ett samordnat vaccinationsarbete – för effektivare hantering av kommande vacciner. Del 1 och 2. [2]

Utbildningsdepartementet

Utvecklat samarbete för verksamhetsförlagd utbildning – långsiktiga åtgärder för sjuksköterskeprogrammen. [9]

Växla yrke som vuxen – en reformerad vuxenutbildning och en ny yrkesskola för vuxna. [16]

Skolor mot brott. [17]