Informationssäkerhet för samhällsviktiga och digitala tjänster

Betänkande av
Utredningen om genomförande av NIS-direktivet

Stockholm 2017

STATENS OFFENTLIGA UTREDNINGAR

SOU 2017:36

SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskansliets förvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2017

ISBN 978-91-38-24602-3
ISSN 0375-250X

Till statsrådet Anders Ygeman

Regeringen beslutade den 31 mars 2016 att utse en särskild utredare med uppdrag att föreslå hur Europaparlamentets och rådet 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 ska genomföras i svensk rätt.

Utredarens uppdrag har varit att föreslå hur direktivet ska genomföras i svensk rätt. Detta har innefattat bland annat att föreslå hur direktivets krav på utpekande av myndigheter med ansvar för vissa funktioner ska genomföras, med inriktningen att Myndigheten för samhällsskydd och beredskap ges en samordnande roll på området men att andra myndigheters ansvar för tillsyn inom särskilda sektorer ska fortsätta gälla, hur identifiering av och krav på leverantörer som omfattas av direktivet kan genomföras i ett samlat regelverk med beaktande av gällande bestämmelser, sektorsansvar och vad som är mest effektivt utifrån olika perspektiv, föreslå nödvändiga ändringar i offentlighets- och sekretesslagen (2009:400) för att känslig information i incidentrapporter ska kunna skyddas, och lämna nödvändiga författningsförslag.

Frågan om hur en nationell strategi för säkerhet i nätverk och informationssystem bör utformas har inte omfattats av uppdraget.

Lagmannen i Stockholms tingsrätt Stefan Strömberg förordnades att fr.o.m. den 2 maj 2016 vara särskild utredare.

Förordnade sakkunniga har under hela eller delar av utredningstiden varit rättssakkunnige Dan Leeman (Justitiedepartementet), kanslirådet Henrik Moberg (Socialdepartementet), rättssakkunniga Mia Persson (Försvarsdepartementet) och kanslirådet Jörgen Samuelsson (Näringsdepartementet).

Som experter att biträda utredningen förordnades fr.o.m. den 5 oktober 2016 numera stf. avdelningschefen Mia Arblom (Försvarsmakten), numera avdelningsdirektören Henrik Christiansson (Säkerhetspolisen), numera enhetschefen Linda Ericson (Myndigheten för samhällsskydd och beredskap), juristen Britt-Marie Jönson (Post- och telestyrelsen), informationssäkerhetsexperten Arvid Kjell (Försvarets Radioanstalt) och it-säkerhetschefen Josefine Östfeldt (Polismyndigheten) samt fr.o.m. den 23 november 2016 juristen Markus Lind (Datainspektionen).

Som ledamöter i en till utredningen knuten referensgrupp förordnades fr.o.m. den 5 oktober 2016 säkerhetschefen Per Ekegren (Livsmedelsverket), chefsjuristen Elisabeth Ekstrand (IIS), handläggaren Linda Eriksson (Statens Energimyndighet), säkerhetschefen Stefan Larsson (E-hälsomyndigheten), riskexperten Anders Lindgren (Finansinspektionen), juristen Markus Lind (Datainspektionen), säkerhetschefen Torbjörn Mellblom (Sjöfartsverket), näringspolitiske experten Pär Nygårds (IT-&Telekomföretagen), utredaren Margareta Palmqvist (Socialstyrelsen), verksjuristen Kim Reenaas (Elsäkerhetsverket), enhetschefen Gunilla Roos (Transportstyrelsen), enhetschefen Per-Olof Ström (Trafikverket), förbundsjuristen Jeanna Thorslund (SKL) och enhetschefen Tina Stödberg (Affärsverket svenska kraftnät). Jeanna Thorslund entledigades den 26 oktober 2016 och samma dag förordnades i stället sektionschefen Jörgen Sandström (SKL). Tina Stödberg entledigades den 28 oktober 2016 och samma dag förordnades i stället it-säkerhetssamordnaren Satu Hallikainen (Affärsverket svenska kraftnät). Markus Lind entledigades den 23 november 2016 för att i stället förordnas som expert.

Som sekreterare anställdes den 2 maj 2016 byrådirektören Annette Norman och den 1 augusti 2016 numera rådmannen Malin Stensbäck.

Utredningen överlämnar härmed betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster* (SOU 2017:36). 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. Utredningens uppdrag är med detta slutfört.

Stockholm i april 2017

Stefan Strömberg

/ Annette Norman
Malin Stensbäck

Innehåll

Bilagor

Sammanfattning

Bakgrund

I juli 2016 antog Europaparlamentet och rådet NIS-direktivet[1]. Direktivet fastställer åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen, i syfte att förbättra den inre marknadens funktion.

Direktivet innebär bland annat skyldigheter för vissa leverantörer av samhällsviktiga tjänster och vissa leverantörer av digitala tjänster att vidta säkerhetsåtgärder för att hantera risker samt förebygga och hantera incidenter i nätverk och informationssystem som de är beroende av för att tillhandahålla tjänsterna. Leverantörerna ska också rapportera incidenter som har en betydande respektive avsevärd inverkan på kontinuiteten i tjänsten.

För att en leverantör ska anses vara en sådan leverantör av samhällsviktiga tjänster som omfattas av direktivet krävs att leverantören bedriver verksamhet inom någon av de i direktivet särskilt utpekade enheterna. Enheterna finns inom sju angivna sektorer. Sektorerna omfattar energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Dessutom krävs att den tjänst som tillhandahålls är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Medlemsstaterna är skyldiga att dels upprätta en förteckning över de tjänster på medlemsstatens territorium som är viktiga för att

[1] 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.

upprätthålla kritisk samhällelig eller ekonomisk verksamhet, dels identifiera de leverantörer som tillhandahåller sådana tjänster.

De leverantörer av digitala tjänster som omfattas av direktivet är sådana som tillhandahåller internetbaserade marknadsplatser, internetbaserade sökmotorer eller molntjänster. Dessa leverantörer ska inte identifieras på det sätt som gäller för leverantörer av samhällsviktiga tjänster och omfattas av direktivet utan att någon bedömning ska göras av om de är samhällsviktiga eller inte.

Medlemsstaterna ska enligt direktivet utse myndigheter med särskilda uppgifter på området, till exempel tillsynsmyndigheter, nationella kontaktpunkter och enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter). Medlemsstaterna ska också säkerställa att tillsynsmyndigheterna har befogenheter och medel för att kontrollera att leverantörerna uppfyller sina skyldigheter samt fastställa regler om sanktioner för överträdelse av de nationella bestämmelserna som antagits enligt direktivet.

Direktivet innehåller vidare en skyldighet för varje medlemsstat att anta en nationell strategi för säkerhet i nätverk och informationssystem.

Medlemsstaterna ska senast den 9 maj 2018 anta och offentliggöra de bestämmelser i lagar och andra författningar som är nödvändiga för att följa direktivet. Bestämmelserna ska tillämpas från och med den 10 maj 2018.

Utredningens uppdrag

Utredningens uppdrag har varit att föreslå hur NIS-direktivet ska genomföras i svensk rätt. Detta har innefattat bland annat att föreslå hur direktivets krav på utpekande av myndigheter med ansvar för vissa funktioner ska genomföras, hur identifiering av och krav på leverantörer som omfattas av direktivet kan genomföras i ett samlat regelverk med beaktande av gällande bestämmelser, sektorsansvar och vad som är mest effektivt utifrån olika perspektiv, föreslå nödvändiga ändringar i offentlighets- och sekretesslagen (2009:400) för att känslig information i incidentrapporter ska kunna skyddas, och lämna nödvändiga författningsförslag.

Frågan om hur en nationell strategi för säkerhet i nätverk och informationssystem bör utformas har inte omfattats av uppdraget.

Utredningens förslag

Ett samlat regelverk – en ny lag och en ny förordning

Utredningen föreslår en ny lag och en ny förordning som till utformning och innehåll ligger nära NIS-direktivet. Regelverket ska tillämpas endast på sådana leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster som omfattas av direktivet. I den utsträckning det finns bestämmelser om säkerhetskrav eller incidentrapporteringskrav på de aktuella leverantörerna i annan lag som minst motsvarar bestämmelserna i den föreslagna lagen ska emellertid de bestämmelserna tillämpas. Om sådana krav finns i bindande EU-rättsakter (lex specialis) ska den föreslagna lagen inte tillämpas alls.

Vissa företag och leverantörer är uttryckligen undantagna från direktivets tillämpningsområde. Dessa omfattas följaktligen inte heller av den föreslagna lagen. Detta innebär att regelverket inte ska tillämpas på företag som omfattas av kraven i artiklarna 13a och 13b i direktiv 2002/21/EG, dvs. tillhandahållare av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst. I NIS-direktivet anges dock internetknutpunkter uttryckligen som en sådan enhet som ska regleras enligt direktivet. Tillhandahållare av internetknutpunkter omfattas därför av den föreslagna lagen trots att de enligt svensk rätt anses som sådana företag som omfattas av artiklarna 13a och 13b.

Regelverket ska inte heller tillämpas på leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 i förordning (EU) nr 910/2014 (eIDAS).

Även verksamhet som är av betydelse för Sveriges säkerhet är undantagen från tillämpningsområdet. Detta innebär till exempel att verksamhet som omfattas av säkerhetsskyddslagen inte omfattas. Incidenter som inträffar i sådan verksamhet ska därmed inte rapporteras enligt bestämmelserna i den föreslagna lagen, utan även fortsättningsvis rapporteras enligt 10 a § säkerhetsskyddsförordningen (1996:633).

Föreskrifter med förteckning över samhällsviktiga tjänster

För att leverantörer av samhällsviktiga tjänster ska kunna identifieras ska Myndigheten för samhällsskydd och beredskap meddela föreskrifter (förteckning) om vilka tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet (samhällsviktiga tjänster) för varje sektor som omfattas av NIS-direktivet.

Identifiering av leverantörer av samhällsviktiga tjänster

Det är i likhet med vad som gäller enligt säkerhetsskyddslagstiftningen verksamhetsutövaren som är ansvarig för att avgöra om denne omfattas av lagen. I detta syfte ska den som är ansvarig för en verksamhet som tillhandahåller en samhällsviktig tjänst som finns upptagen i de föreskrifter (förteckning) som Myndigheten för samhällsskydd och beredskap ska meddela, undersöka om tillhandahållandet av tjänsten är beroende av nätverk eller informationssystem och om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Undersökningen ska dokumenteras. För att avgöra om en störning är betydande ska verksamhetsutövaren beakta vissa särskilda faktorer, bland annat det antal användare som är beroende av den aktuella tjänsten. Tillsynsmyndigheten får meddela föreskrifter om vilka sektorspecifika och sektoröverskridande faktorer som ska beaktas vid bedömningen av om en incident skulle medföra en betydande störning.

Säkerhetskrav och incidentrapportering

Såväl leverantörer av samhällsviktiga tjänster som leverantörer av digitala tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i deras nätverk och informationssystem. De ska också vidta lämpliga åtgärder för att förebygga och minimiera den inverkan som incidenter som påverkar säkerheten i deras nätverk och informationssystem har på de tjänster som tillhandahålls. Syftet med sistnämnda åtgärder är att säkerställa kontinuiteten i tjänsterna.

Leverantörer av digitala tjänster ska själva utarbeta åtgärder för att hantera risker. De ska i det arbetet beakta vissa i lagen angivna faktorer. Leverantörer av samhällsviktiga tjänster ska i stället göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder. I analysen, som ska dokumenteras och uppdateras årligen, ska en åtgärdsplan ingå. Tillsynsmyndigheten får också meddela föreskrifter om utformingen av säkerhetsåtgärderna. Leverantörer av samhällsviktiga tjänster ska också bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Både leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster ska utan onödigt dröjsmål rapportera incidenter till CSIRT-enheten (se nedan) vid Myndigheten för samhällsskydd och beredskap. Leverantörer av samhällsviktiga tjänster ska rapportera incidenter som har en betydande inverkan på kontinuiteten i tjänsten, medan leverantörer av digitala tjänster ska rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av tjänsten. I lagen anges ett antal faktorer som framför allt ska beaktas vid bedömningen av om incidenten har en sådan inverkan att den ska rapporteras.

Tillsynsmyndigheten får meddela närmare föreskrifter om faktorer som ska beaktas vid bedömningen av om en incident har betydande inverkan. Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om rapportering av incidenter och om förutsättningarna för frivillig incidentrapportering.

Tillsyn

För varje sektor och för de digitala tjänster som omfattas av lagen ska en tillsynsmyndighet ansvara för att övervaka att regelverket följs. Följande myndigheter föreslås vara tillsynsmyndigheter.

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	Tillsynsmyndighet
Digitala tjänster	Post- och telestyrelsen

Vid tillsyn ska leverantören tillhandahålla tillsynsmyndigheten den information som behövs för en bedömning av säkerheten i leverantörens nätverk och informationssystem. Leverantörer av samhällsviktiga tjänster är skyldiga att tillhandahålla även bevis för att säkerhetsprinciper har genomförts effektivt.

Beträffande leverantörer av digitala tjänster får tillsynsåtgärder vidtas bara i efterhand, när tillsynsmyndigheten har fått kännedom om att leverantören inte uppfyller säkerhetskraven eller kravet att incidentrapportera.

Tillsynsmyndigheten ska försöka få en leverantör som inte följer regelverket att rätta sig. Tillsynsmyndigheten får meddela föreläggganden, dels i syfte att få tillgång till viss information som behövs för tillsynen, dels för att få leverantören att följa regelverket. Ett föreläggande får förenas med vite.

Myndigheten för samhällsskydd och beredskap ska inom ramen för sitt nuvarande uppdrag ha en samlad bild av NIS-direktivets genomförande och tillämpning i Sverige genom att leda ett samarbetsforum där samtliga tillsynsmyndigheter ska ingå samt ta emot tillsynsmyndighetens bedömning av brister i nätverk och informationssystem. I bedömningen bör ingå brister som upptäcks vid tillsyn men även svårigheter vid tillämpning och tolkning av regelverket. Myndigheten för samhällsskydd och beredskap ska vidare tillhandahålla tillsynsmyndigheterna det metodstöd för tillsyn som behövs för en effektiv tillsyn enligt det föreslagna regelverket.

Sanktionsavgift

Tillsynsmyndigheten ska besluta att sanktionsavgift ska tas ut av den som underlåter att incidentrapportera eller att vidta säkerhetsåtgärder. Vid bedömningen av avgiftens storlek ska tillsynsmyndigheten ta särskild hänsyn till skada eller risk för skada som uppstått till följd av överträdelsen, om leverantören tidigare har begått en överträdelse samt de kostnader som leverantören har undvikit till följd av överträdelsen. Sanktionsavgiften får under vissa förhållanden efterges helt eller delvis.

Nationell kontaktpunkt, samarbetsgrupp och CSIRT-enhet

För att underlätta gränsöverskridande samarbete och för att möjliggöra ett effektivt genomförande av NIS-direktivet ska det i varje medlemsstat finnas en *nationell gemensam kontaktpunkt*. Den nationella kontaktpunkten ska ansvara för samordningen av frågor angående nätverk och informationssystem och för gränsöverskridande samarbete på unionsnivå. Den nationella kontaktpunkten ska också lämna en sammanfattande rapport om antalet ingivna incidentrapporter och om de rapporterade incidenternas art till samarbetsgruppen.

Samarbetsgruppen syftar till att stödja och underlätta strategiskt samarbete mellan medlemsstaterna vad gäller säkerhet i nätverk och informationssystem. Gruppen ska bland annat utbyta bästa praxis i olika avseenden. Utöver företrädare för medlemsstaterna består gruppen av representanter från kommissionen och från Europeiska unionens byrå för nät- och informationssäkerhet (Enisa).

I varje medlemsstat ska det enligt NIS-direktivet också finnas en eller flera *enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter)*. CSIRT-enheten ska bland annat övervaka incidenter på nationell nivå och tillhandahålla tidiga varningar m.m. till relevanta aktörer om risker och incidenter. CSIRT-enheten ska också delta i ett CSIRT-nätverk inom unionen.

Utredningens förslag innebär att Myndigheten för samhällsskydd och beredskap ska vara både nationell kontaktpunkt och CSIRT-enhet samt representera Sverige i samarbetsgruppen. Myndigheten för samhällsskydd och beredskap har redan i dag ett sådant uppdrag samt den struktur och kompetens som krävs för detta.

Sekretess

Befintliga bestämmelser om sekretess omfattar uppgifter som ska rapporteras och delas med anledning av incidenter samt tillhandahållas i samband med tillsyn. Det har inte framkommit några exempel på att den nuvarande regleringen är otillräcklig. Det finns därmed inte skäl att införa starkare sekretess för uppgifter som lämnas inom ramen för incidentrapporteringen.

Till följd av tillsynen kan tillsynsmyndigheterna emellertid få del av känsliga uppgifter om enskilds affärs- eller driftförhållande. För att sistnämnda uppgifter ska kunna skyddas behöver sekretessförordningen ändras så att sekretess för sådana uppgifter gäller i verksamhet som består i tillsyn enligt det föreslagna regelverket.

Konsekvenser

NIS-direktivets genomförande kommer initialt att innebära kostnader för de föreslagna tillsynsmyndigheterna. Kostnaderna kan till viss del, i vart fall på lång sikt, finansieras genom de samhällsekonomiska vinster som en hög gemensam nivå av säkerhet i nätverk och informationssystem medför.

Utredningen föreslår att tillsynsmyndigheteras uppdrag enligt förslagen, i vart fall inledningsvis, ska vara anslagsfinansierade och fördelas på de utgiftsområden som respektive sektor tillhör. När det gäller kostnader för löpande tillsyn samt för kompetensförsörjning föreslår utredningen att Statskontoret ges i uppdrag att lämna ett förslag på genomförande och finansiering.

Ikraftträdande

Regelverket föreslås träda i kraft den 10 maj 2018, vilket är det datum som medlemsstaterna enligt NIS-direktivet ska tillämpa direktivets bestämmelser. För att lagen ska kunna tillämpas i enlighet med direktivet den dagen föreslår utredningen att vissa myndigheter dessförinnan ges i uppdrag att påbörja arbetet med myndighetsföreskrifter samt att vidta andra behövliga förberedelseåtgärder.

1 Författningsförslag

1.1 Förslag till lag (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster

Härigenom föreskrivs[1] följande.

Inledande bestämmelse

1 § Denna lag syftar till att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom den Europeiska unionen, för att förbättra den inre marknadens funktion.

Genom denna lag genomförs 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 (NIS-direktivet), utom vad gäller Sveriges skyldighet att anta en nationell strategi för säkerhet i nätverk och informationssystem.

Lagens tillämpningsområde

2 § Denna lag gäller

a) leverantörer av samhällsviktiga tjänster enligt definitionen i 7 § 3 som är etablerade på svenskt territorium.

b) leverantörer av digitala tjänster enligt definitionerna i 7 § 4 och 5 som har sitt huvudsakliga etableringsställe i Sverige eller har utsett

[1] Jfr 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, i den ursprungliga lydelsen.

en företrädare som är etablerad här, dock inte mikroföretag eller små företag enligt definitionen i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.

Undantag från lagens tillämpningsområde

Elektronisk kommunikation

3 § Lagen gäller inte för företag som omfattas av kraven i artiklarna 13a och 13b i Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv), i lydelsen enligt Europaparlamentets och rådets direktiv 2009/140/EG, utom företag som tillhandahåller internetknutpunkter.

Betrodda tjänster

4 § Lagen gäller inte för leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 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, i den ursprungliga lydelsen.

Avvikande bestämmelser i EU-rättsakter eller i annan författning

5 § Finns bestämmelser i bindande EU-rättsakter om krav på att leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster ska säkerställa säkerheten i sina nätverk och informationssystem eller rapportera incidenter så ska denna lag inte tillämpas förutsatt att verkan av kraven minst motsvarar verkan av skyldigheterna i denna lag.

Finns sådana bestämmelser i annan författning ska de bestämmelserna tillämpas om kraven minst motsvarar verkan av skyldigheterna i denna lag.

Sveriges säkerhet

6 § Bestämmelserna i denna lag ska inte tillämpas på verksamhet som är av betydelse för Sveriges säkerhet.

Definitioner i lagen

7 § I denna lag avses med

1. nätverk och informationssystem:

a) ett elektroniskt kommunikationsnät enligt artikel 2 a i direktiv 2002/21/EG, i lydelsen enligt direktiv 2009/140/EG,

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 leden a och b för att de ska kunna drivas, användas, skyddas och underhållas,

2. *säkerhet i nätverk och informationssystem:* nätverk och informationssystems förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via dessa nätverk och informationssystem,

3. *leverantör av samhällsviktiga tjänster:* en enhet av en typ som avses i bilaga 2 till NIS-direktivet och som tillhandhåller en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, tillhandhållandet av tjänsten är beroende av nätverk och informationssystem och en incident skulle medföra en betydande störning av tillhandahållandet av tjänsten,

4. *digital tjänst*: en tjänst i den mening som avses i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster, i den ursprungliga lydelsen, av en typ som anges i bilaga 3 till NIS-direktivet,

5. *leverantör av digital tjänst:* en juridisk person som tillhandahåller en digital tjänst,

6. *incident:* en händelse med en faktisk negativ inverkan på säkerheten i nätverk eller informationssystem,

7. *incidenthantering:* alla förfaranden som stöder upptäckt, analys och begränsning av en incident och åtgärder mot en incident,

8. *risk:* en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i nätverk eller informationssystem,

9. *företrädare:* en i unionen etablerad fysisk eller juridisk person som uttryckligen har utsetts att agera för en leverantör av digitala tjänster som inte är etablerad i unionen, till vilken en behörig nationell myndighet eller en CSIRT-enhet kan vända sig, i stället för till leverantören av digitala tjänster, i frågor som gäller de skyldigheter som leverantören av digitala tjänster har enligt denna lag,

10. *standard:* en standard i den mening som avses i artikel 2.1 i 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, i den ursprungliga lydelsen

11. *specifikation:* en teknisk specifikation i den mening som avses i artikel 2.4 i förordning (EU) nr 1025/2012, i den ursprungliga lydelsen,

12. *internetknutpunkt (IXP):* en nätfacilitet som möjliggör sammankoppling av mer än två oberoende autonoma system, främst i syfte att underlätta utbytet av internettrafik. En IXP tillhandahåller sammankoppling enbart för autonoma system och kräver inte att den internettrafik som passerar mellan två deltagande autonoma system passerar genom ett tredje autonomt system och ändrar inte heller trafiken eller påverkar den på något annat sätt,

13. *domännamnssystem (DNS):* ett hierarkiskt, distribuerat namngivningssystem i ett nätverk som hanterar domännamnsförfrågningar,

14. *leverantör av DNS-tjänst:* en enhet som tillhandahåller DNS-tjänster på internet,

15. *registreringsenhet för toppdomäner:* en enhet som administrerar och förvaltar registreringen av internetdomännamn under en specifik toppdomän,

16. *internetbaserad marknadsplats:* en digital tjänst som gör det möjligt för konsumenter eller näringsidkare enligt definitionen i

artikel 4.1 a respektive 4.1 b i Europaparlamentets och rådets direktiv 2013/11/EU av den 21 maj 2013 om alternativ tvistlösning vid konsumenttvister och om ändring av förordning (EG) nr 2006/2004 och direktiv 2009/22/EG (direktivet om alternativ tvistlösning), i den ursprungliga lydelsen, att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare antingen på webbplatsen för den internetbaserade marknadsplatsen eller på en webbplats tillhörande en näringsidkare där datatjänster som tillhandahålls av en internetbaserad marknadsplats används,

17. *internetbaserad sökmotor:* en digital tjänst som gör det möjligt för användare att göra sökningar på i princip alla webbplatser eller webbplatser på ett visst språk på grundval av en förfrågan om vilket ämne som helst i form av ett nyckelord, en fras eller annan inmatning och som returnerar länkar som innehåller information om det begärda innehållet,

18. *molntjänst:* en digital tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser,

19. *NIS-direktivet:* 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, i den ursprungliga lydelsen

20. *säkerhetsprinciper:* styrande dokument, till exempel föreskrifter och interna riktlinjer,

21. *CSIRT-enhet:* enhet för it-säkerhetsincidenter (Computer Security Incident Response Team)

Identifiering av leverantörer av samhällsviktiga tjänster

8 § Den som är ansvarig för en verksamhet som tillhandahåller en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet (samhällsviktig tjänst) ska undersöka om tillhandahållandet av tjänsten är beroende av nätverk eller informationssystem och om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

Följande sektoröverskridande faktorer ska beaktas när leverantören fastställer om en störning är betydande.

1. Det antal användare som är beroende av den tjänst som den berörda enheten tillhandahåller.

2. Hur beroende andra sektorer enligt bilaga 2 till NIS-direktivet är av den tjänst som enheten tillhandahåller.

3. Vilken inverkan incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet eller allmän säkerhet, uttryckt i grad och varaktighet.

4. Enhetens marknadsandel.

5. Hur stort geografiskt område som skulle kunna påverkas av en incident.

6. Enhetens betydelse för upprätthållandet av en tillräcklig tjänstenivå, med beaktande av tillgången till alternativa sätt för att tillhandahålla tjänsten.

När det är lämpligt ska även sektorspecifika faktorer beaktas.

Tillhandahålls tjänsten även i andra länder i den Europeiska unionen ska den nationella kontaktpunkten samråda med motsvarande funktion i andra berörda länder innan beslut om identifiering fattas.

Undersökningen ska dokumenteras.

Utseende av företrädare för leverantör av digitala tjänster

9 § En leverantör av digitala tjänster som erbjuder digitala tjänster i Sverige men som inte har sitt huvudsakliga etableringsställe inom Europeiska unionen ska utse en företrädare i något av de länder i unionen där tjänsterna erbjuds.

Säkerhetsåtgärder

Leverantörer av samhällsviktiga tjänster

10 § Leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

11 § Leverantörer av samhällsviktiga tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder i sin verksamhet. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till den föreliggande risken.

12 § Leverantörer av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga och minimera verkningarna av incidenter som påverkar säkerheten i nätverk och informationssystem som används för att tillhandahålla sådana samhällsviktiga tjänster, i syfte att säkerställa kontinuiteten i dessa tjänster.

13 § Leverantörer av samhällsviktiga tjänster ska göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder enligt 11 och 12 §§. I analysen ska ingå en åtgärdsplan. Analysen ska dokumenteras och uppdateras årligen.

Leverantörer av digitala tjänster

14 § Leverantörer av digitala tjänster ska utarbeta och vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder när de tillhandahåller internetbaserade marknadsplatser, internetbaserade sökmotorer eller molntjänster inom unionen. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till den föreliggande risken, varvid hänsyn ska tas till

1. säkerheten i system och anläggningar,
2. incidenthantering,
3. hantering av driftskontinuitet,
4. övervakning, revision och testning och
5. efterlevnad av internationella standarder.

15 § Leverantörer av digitala tjänster ska vidta åtgärder för att förebygga och minimera den inverkan som incidenter som påverkar säkerheten i deras nätverk och informationssystem har på internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster som erbjuds inom unionen, i syfte att säkerställa kontinuiteten i dessa tjänster.

Incidentrapportering

Leverantörer av samhällsviktiga tjänster

16 § Leverantörer av samhällsviktiga tjänster ska utan onödigt dröjsmål rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller. Rapporteringen ska göras till CSIRT-enheten.

Rapporterna ska innehålla information som gör det möjligt för CSIRT-enheten att fastställa incidentens eventuella gränsöverskridande verkningar.

Rapportering ska inte medföra ökat ansvar för den rapporterande parten.

17 § För att fastställa om en incident har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten ska hänsyn framför allt tas till följande faktorer.

1. Det antal användare som påverkas av störningen av den samhällsviktiga tjänsten.
2. Hur länge incidenten varar.
3. Hur stort geografiskt område som påverkas av incidenten.

18 § Är en leverantör av samhällsviktiga tjänster beroende av en tredjepartsleverantör av digitala tjänster för tillhandahållandet av en tjänst som är viktig för att upprätthålla kritisk samhällelig och ekonomisk verksamhet, ska leverantören av samhällsviktiga tjänster rapportera varje betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten till följd av en incident som påverkar leverantören av digitala tjänster.

Leverantörer av digitala tjänster

19 § Leverantörer av digitala tjänster ska utan onödigt dröjsmål rapportera alla incidenter som har en avsevärd inverkan på tillhandahållandet av en internetbaserad marknadsplats, internetbaserad sökmotor eller molntjänst som de erbjuder inom unionen. Rapporteringen ska göras till CSIRT-enheten.

Rapporterna ska innehålla information som gör det möjligt för CSIRT-enheten att fastställa vilken betydelse eventuell gränsöverskridande inverkan har.

Rapportering ska inte medföra ökat ansvar för den rapporterande parten.

20 § För att fastställa om en incident har en avsevärd inverkan ska hänsyn framför allt tas till följande faktorer.

1. Det antal användare som påverkas av incidenten, framför allt användare som är beroende av tjänsten för att kunna tillhandahålla sina egna tjänster.
2. Hur länge incidenten varar.
3. Hur stort geografiskt område som påverkas av incidenten.
4. I vilken utsträckning incidenten stör tjänstens funktion.
5. I vilken utsträckning incidenten inverkar på den ekonomiska och samhälleliga verksamheten.

Skyldigheten att rapportera en incident ska endast gälla om leverantören av digitala tjänster har tillgång till den information som behövs för att bedöma en incidents inverkan mot bakgrund av de faktorer som avses i första stycket.

Förpliktande att informera allmänheten om en incident

21 § Efter samråd med den berörda leverantören av digitala tjänster får CSIRT-enheten, om det är lämpligt, förplikta leverantören att informera allmänheten om enskilda incidenter. En förutsättning för ett sådant förpliktande är att allmänheten behöver känna till incidenten för att det ska vara möjligt att förhindra en incident eller åtgärda en pågående incident eller om incidentens avslöjande på annat sätt omfattas av allmänintresset.

Tillsyn

22 § Den myndighet som regeringen bestämmer ska vara nationell behörig myndighet.

Den nationella behöriga myndigheten ska utöva tillsyn över att denna lag och föreskrifter som meddelats i anslutning till lagen följs (tillsynsmyndighet).

23 § Tillsynsmyndigheten har rätt att i den utsträckning det behövs för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av denna lag bedrivs.

24 § Tillsynsmyndigheten får förelägga den som står under tillsyn att tillhandahålla information i enlighet med 26 och 27 §§.

Ett föreläggande får förenas med vite.

25 § Tillsynsmyndigheten har rätt att få verkställighet hos Kronofogdemyndigheten av beslut som avser åtgärder enligt denna lag. Då gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet eller avhysning.

Leverantörer av samhällsviktiga tjänster

26 § Vid tillsyn ska en leverantör av samhällsviktiga tjänster tillhandahålla tillsynsmyndigheten

1. den information som är nödvändig för att bedöma säkerheten i leverantörens nätverk och informationssystem, inbegripet dokumenterade säkerhetsprinciper,
2. bevis för ett effektivt genomförande av säkerhetsprinciper, såsom resultaten av en säkerhetsrevision utförd av tillsynsmyndigheten eller en auktoriserad revisor och, i det senare fallet, att ge tillsynsmyndigheten tillgång till resultaten, inklusive de underliggande bevisen, och
3. annan information som behövs vid bedömningen av om leverantören uppfyller sina skyldigheter.

När tillsynsmyndigheten begär sådan information eller bevis ska den uppge syftet med begäran och precisera vilken information som krävs.

Leverantörer av digitala tjänster

27 § Vid tillsyn ska en leverantör av digitala tjänster tillhandahålla tillsynsmyndigheten den information som behövs för en bedömning av säkerheten i leverantörernas nätverk och informationssystem, inbegripet dokumenterade säkerhetsprinciper.

28 § Tillsynsåtgärder beträffande leverantörer av digitala tjänster får vidtas endast när tillsynsmyndigheten har fått kännedom om att leverantören inte uppfyller kraven i 14, 15 eller 16 §§.

Sanktioner och ingripanden

Underrättelse m.m.

29 § Om tillsynsmyndigheten finner skäl att misstänka att en leverantör av samhällsviktiga tjänster inte följer lagen eller föreskrifter som har meddelats i anslutning till lagen, ska myndigheten underrätta leverantören om detta förhållande och ge denne möjlighet att yttra sig inom skälig tid.

30 § Om tillsynsmyndigheten konstaterar att en leverantör av samhällsviktiga tjänster eller en leverantör av digitala tjänster inte följer lagen eller föreskrifter som har meddelats i anslutning till lagen, ska tillsynsmyndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse.

Föreläggande m.m.

31 § Tillsynsmyndigheten får meddela de förelägganden som behövs för att leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster ska uppfylla de säkerhetskrav och krav på incidentrapportering som följer av denna lag och av föreskrifter som har meddelats i anslutning till lagen.

Ett föreläggande får förenas med vite.

Sanktionsavgift

32 § Tillsynsmyndigheten ska besluta att sanktionsavgift ska tas ut av den som

1. underlåter att vidta säkerhetsåtgärder enligt 11, 12, 14 eller 15 §§ eller
2. underlåter att incidentrapportera enligt 16 eller 19 §§.

Avgiften tillfaller staten.

33 § Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

34 § När sanktionsavgiftens storlek bestäms ska hänsyn tas till samtliga relevanta omständigheter. Särskild hänsyn ska tas till den skada eller risk för skada som uppstått till följd av regelöverträdelsen, om leverantören tidigare har begått en överträdelse samt de kostnader som leverantören undvikit till följd av överträdelsen.

35 § Sanktionsavgiften får efterges helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

36 § Tillsynsmyndigheten får inte ingripa med sanktionsavgift om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

37 § Ett beslut om sanktionsavgift ska vara skriftligt och innehålla skälen för beslutet.

Innan tillsynsmyndigheten beslutar om sanktionsavgift ska den som beslutet kommer att riktas mot ges tillfälle att yttra sig.

38 § Sanktionsavgift får inte beslutas om den som anspråket riktas mot inte har getts tillfälle att yttra sig inom två år efter överträdelsen.

39 § Sanktionsavgiften ska betalas till tillsynsmyndigheten inom trettio dagar efter det att beslutet om sanktionsavgiften fått laga kraft eller den längre tid som anges i beslutet.

40 § Ett beslut om sanktionsavgift får verkställas utan föregående dom eller utslag om avgiften inte har betalts inom den tid som anges i 39 §.

41 § Om sanktionsavgiften inte betalas inom den tid som anges i 39 §, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning.

42 § En beslutad sanktionsavgift faller bort om beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Gemensam nationell kontaktpunkt

43 § Den myndighet som regeringen bestämmer ska vara gemensam nationell kontaktpunkt.

Enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet)

44 § Den myndighet som regeringen bestämmer ska vara CSIRT-enhet.

Bemyndigande

45 § Regeringen eller den myndighet som regeringen bestämmer får, beträffande leverantörer av samhällsviktiga tjänster, meddela föreskrifter om

1. vilka sektorspecifika och sektoröverskridande faktorer som ska beaktas för att fastställa om en incident medför en betydande störning vid identifiering av leverantörer av samhällsviktiga tjänster enligt 8 §,
2. ett systematiskt och riskbaserat informationssäkerhetsarbete enligt 10 §, och
3. vilka faktorer som ska användas för att avgöra om en incident har en betydande inverkan på kontinuiteten i en samhällsviktig tjänst enligt 17 § och därför medför krav på rapportering.

Föreskrifter

Leverantörer av samhällsviktiga tjänster

46 § Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen, beträffande leverantörer av samhällsviktiga tjänster, meddela föreskrifter om

1. vilka tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet (samhällsviktiga tjänster),
2. utformningen av säkerhetsåtgärder som avses i 11 och 12 §§,
3. rapportering av incidenter som avses i 16 §, och
4. förutsättningarna för frivillig rapportering av incidenter.

Leverantörer av digitala tjänster

47 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen, beträffande leverantörer av digitala tjänster, meddela föreskrifter om
1. rapportering av incidenter som avses i 19 § och
2. förutsättningarna för frivillig rapportering av incidenter.

Överklagande m.m.

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

49 § En myndighets beslut enligt denna lag eller enligt föreskrifter som meddelats i anslutning till lagen får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

Kammarrättens avgörande i ett mål enligt denna lag får inte överklagas.

Denna lag träder i kraft den 10 maj 2018.

1.2 Förslag till förordning (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster

Regeringen föreskriver följande.

Inledande bestämmelser

1 § Denna förordning har samma syfte som lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster och genomför tillsammans med lagen 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 (NIS-direktivet), utom vad gäller Sveriges skyldighet att anta en nationell strategi för säkerhet i nätverk och informationssystem.

2 § De definitioner som anges i 7 § i lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster har samma innebörd i denna förordning.

Identifiering av leverantörer av samhällsviktiga tjänster

3 § Myndigheten för samhällsskydd och beredskap ska företräda Sverige i bilaterala och multilaterala samråd när en samhällsviktig tjänst tillhandahålls i ett eller flera andra länder i den Europeiska unionen enligt 8 § fjärde stycket lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster.

Tillsynsmyndigheten ska ges tillfälle att yttra sig före samråd och vid behov lämna stöd till Myndigheten för samhällsskydd och beredskap.

Säkerhetsåtgärder

4 § Vid utformningen av säkerhetsåtgärder bör leverantörer av samhällsviktiga tjänster beakta europeiska eller internationellt accepterade standarder och specifikationer.

Tillsynsmyndigheter

5 § Följande myndigheter är tillsynsmyndigheter enligt lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster.

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	**Tillsynsmyndighet**
Digitala tjänster	Post- och telestyrelsen

6 § Tillsynsmyndigheten ska

1. samarbeta med Datainspektionen när den handlägger incidenter som medfört personuppgiftsincidenter och innan ett åtgärdsföreläggande meddelas,
2. lämna stöd till representanten i samarbetsgruppen,
3. lämna vägledning till leverantörer av samhällsviktiga tjänster vid tillämpningen av lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster och av denna förordning,
4. lämna upplysning till leverantörer av samhällsviktiga tjänster vid bedömningen av om annan lag eller bindande EU-rättsakt ska

tillämpas i stället för lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster, och

5. samarbeta med och bistå tillsynsmyndigheter i andra länder i Europeiska unionen när det gäller tillsynen över leverantörer av digitala tjänster. Detta bistånd och samarbete får omfatta informationsutbyte mellan de berörda behöriga myndigheterna och begäranden om att tillsynsåtgärder enligt lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster ska vidtas.

Gemensam nationell kontaktpunkt

7 § Myndigheten för samhällsskydd och beredskap är gemensam nationell kontaktpunkt.

Myndigheten för samhällsskydd och beredskap ska för Sveriges del fullgöra de uppgifter som åligger den nationella kontaktpunkten enligt artiklarna 8 och 14.5 tredje stycket i NIS-direktivet, i den ursprungliga lydelsen.

Myndigheten för samhällsskydd och beredskap ska årligen lämna en sammanfattande rapport till den samarbetsgrupp den inrättats enligt NIS-direktivet om de incidentrapporter som mottagits. Av rapporten ska framgå antalet mottagna incidentrapporter, incidenternas art och vidtagna säkerhetsåtgärder.

CSIRT-enhet

8 § Myndigheten för samhällsskydd och beredskap är CSIRT-enhet.

Myndigheten för samhällsskydd och beredskap ska uppfylla kraven och för Sveriges del fullgöra de uppgifter som åligger CSIRT-enheten enligt bilaga 1 till NIS-direktivet, i den ursprungliga lydelsen.

Myndigheten för samhällsskydd och beredskap

1. ska ta emot de incidentrapporter som lämnas enligt 16 och 19 §§ lagen (2008:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster,

2. ska informera andra berörda länder i Europeiska unionen om en incident som rapporterats av en leverantör av samhällsviktiga

tjänster har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i det landet,

3. ska, om det är lämpligt, informera andra länder i Europeiska unionen som påverkats av en incident som rapporterats av en leverantör av digitala tjänster,

4. får informera allmänheten om enskilda incidenter efter samråd med den rapporterande leverantören,

5. ska när det är möjligt överlämna relevant information som kan bidra till en effektiv hantering av incidenten och det förebyggande arbetet till den rapporterande leverantören av samhällsviktiga tjänster,

6. ska skyndsamt uppmana leverantörer att anmäla incidenter som har sin grund i en brottslig gärning till polisen, och

7. ska skyndsamt överlämna de incidentrapporter som lämnats enligt 16 och 19 §§ lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga och digitala tjänster till den tillsynsmyndighet som enligt 5 § denna förordning utövar tillsyn över den rapporterande leverantören.

Myndigheten för samhällsskydd och beredskap

9 § Myndigheten för samhällsskydd och beredskap ska lämna råd och stöd till tillsynsmyndigheterna vid utarbetandet av myndighetsföreskrifter.

Bemyndiganden

10 § Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om

1. ett systematiskt och riskbaserat informationssäkerhetsarbete enligt 10 § lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster,

2. vilka tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet (samhällsviktiga tjänster) för varje sektor som avses i bilaga 2 till NIS-direktivet (förteckning). Föreskriften ska uppdaterast minst vartannat år,

3. rapportering av incidenter, och

4. förutsättningarna för frivillig rapportering av incidenter.

Tillsynsmyndigheterna ska ges tillfälle att yttra sig innan föreskrifter meddelas.

11 § Tillsynsmyndigheten får, för sin sektor, meddela närmare föreskrifter om

1. utformningen av säkerhetsåtgärder enligt 11 och 12 §§ lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster,

2. sektorspecifika och sektoröverskridande faktorer för att fastställa om en incident medför en betydande störning vid identifieringen av leverantörer av samhällsviktiga tjänster, och

3. vilka faktorer som ska användas för att avgöra om en incident har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten och därför medför krav på rapportering.

Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig innan föreskrifter meddelas.

Denna förordning träder i kraft den 10 maj 2018.

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

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

Denna förordning träder i kraft den 10 maj 2018.

Bilaga[2]

Verksamheten består i	Särskilda begränsningar i sekretessen
151. tillsyn enligt lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster	

[2] Senaste lydelse 2017:118.

2 Utredningens uppdrag och arbete

2.1 Bakgrund

I juli 2016 antog Europaparlamentet och rådet direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet). Direktivet innehåller bl.a. skyldigheter för varje medlemsstat att anta en nationell strategi för säkerhet i nätverk och informationssystem och att utse myndigheter med särskilda uppgifter på detta område. Medlemsstaterna är enligt direktivet också skyldiga att identifiera operatörer som bedriver samhällsviktig verksamhet inom sju sektorer och som är beroende av nätverk och informationssystem. Medlemsstaterna ska senast den 9 maj 2018 anta och offentliggöra de bestämmelser i lagar och andra författningar som är nödvändiga för att genomföra direktivet. Dessa bestämmelser ska tillämpas från och med den 10 maj 2018. Direktivet finns som bilaga 2.

2.2 Utredningens uppdrag

Regeringen beslutade den 31 mars 2016 att utse en särskild utredare med uppdrag att föreslå hur NIS-direktivet ska genomföras i svensk rätt. I uppdraget ingår bl.a. att

- föreslå hur direktivets krav på utpekande av myndigheter med ansvar för vissa funktioner ska genomföras, med inriktningen att Myndigheten för samhällsskydd och beredskap ges en samordnande roll på området men att andra myndigheters ansvar för tillsyn inom särskilda sektorer ska fortsätta att gälla,

- föreslå hur identifiering av och krav på aktörer som omfattas av direktivet kan genomföras i ett samlat regelverk med beaktande av gällande bestämmelser, sektorsansvar och vad som är mest effektivt utifrån olika perspektiv,
- föreslå nödvändiga ändringar i offentlighets- och sekretesslagen (2009:400) för att känslig information i incidentrapporter ska kunna skyddas, och
- lämna nödvändiga författningsförslag.

Frågan om hur en nationell strategi för säkerhet i nätverk och informationssystem bör utformas ingår inte i uppdraget.

Utredningens direktiv finns i sin helhet som bilaga 1.

Uppdraget ska redovisas senast den 1 maj 2017.

2.3 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 sju protokollförda möten med expert- och sakkunniggruppen, varav ett i internatform. Därutöver har ett protokollfört möte hållits med endast de sakkunniga. Utredningen har också haft enskilda möten med deltagarna i referensgruppen. Vid mötet med Elsäkerhetsverket konstaterades att verket inte berörs av NIS-direktivet. Utredningen och Elsäkerhetsverkets representant enades då om att Elsäkerhetsverket fortsättningsvis inte behövde vara representerat i referensgruppen. Elsäkerhetsverket har därför inte närvarat vid de två protokollförda möten som utredningen haft med referensgruppen i sin helhet. Utredningen har också sammanträffat med en representant från Energimarknadsinspektionen, med företrädare för Inspektionen för vård och omsorg samt med representanter för Riksrevisionen. Utredningen har vidare informerat sig om Läkemedelsverkets uppdrag när det gäller informationssäkerhet för medicintekniska produkter.

Utredningen har med hjälp främst av deltagarna i referensgruppen gjort en övergripande inventering av gällande rätt på det område som NIS-direktivet reglerar. Inventeringen finns tillgänglig i ärende dnr Komm2017/00542-1.

Utredningen har löpande hållit Regeringskansliet informerat om arbetet.

Utredningen har informerat sig om arbetet med betänkandena *Informations- och cybersäkerhet i Sverige* (SOU 2015:23), *En ny säkerhetsskyddslag* (SOU 2015:25), *En trygg dricksvattenförsörjning* (SOU 2016:32), om utredningen angående frågan om åtgärder för att öka Polismyndighetens tillgång till information om it-brottslighet (Ds 2016:22), om Integritetskommitténs arbete (Ju 2014:09) och om Regeringskansliets arbete med en Strategi för informations- och cybersäkerhet.

2.4 Betänkandets disposition och läsanvisning

Betänkandet inleds med en övergripande sammanfattning av innehållet i NIS-direktivet (kapitel 3). Därefter följer en beskrivning av de typer av enheter som finns angivna i bilaga 2 till NIS-direktivet. Enheterna kan beskrivas som de verksamheter som – om de tillhandahåller samhällsviktiga tjänster vars tillhandahållande är beroende av nätverk och informationssystem – omfattas av direktivet. (kapitel 4). I kapitel 5 anges utgångspunkterna för genomförandet av direktivet. Utredningen kommer där till slutsatsen att NIS-direktivet bör genomföras i en ny lag och en ny förordning. I kapitlet behandlas också den föreslagna lagens tillämpningsområde. I kapitel 6 behandlas sedan begreppet samhällsviktiga tjänster. Kapitlen därefter behandlar frågor om säkerhetskrav och incidentrapportering för leverantörer av samhällsviktiga tjänster (kapitel 7), tillsyn (kapitel 8) samt ingripanden och sanktioner (kapitel 9). I kapitel 10 behandlas de leverantörer av digitala tjänster som anges i bilaga 3 till NIS-direktivet. Dessa leverantörer omfattas av direktivet även om de inte är samhällsviktiga och regleras på ett mindre ingripande sätt än leverantörer av samhällsviktiga tjänster. I kapitel 11 redogörs för utredningens slutsats att Myndigheten för samhällsskydd och beredskap ska anförtros rollen som nationell kontaktpunkt och CSIRT-enhet samt vara Sveriges representant i samarbetsgruppen enligt NIS-direktivet. Där finns också en beskrivning av Myndigheten för samhällsskydd och beredskaps uppdrag och verksamhet. I kapitel 12 behandlas frågor om sekretess. Kapitel 13 innehåller utredningens konsekvensanalys. Ikraftträdandet behandlas i kapitel 14. I det kapitlet föreslår utred-

ningen att regeringen ska ge ett antal myndigheter i uppdrag att bland annat påbörja arbete med myndighetsföreskrifter inför lagens ikraftträdande. Slutligen följer en författningskommentar till de lämnade författningsförslagen (kapitel 15).

Kommittédirektiven finns i sin helhet i bilaga 1. I bilaga 2 finns NIS-direktivet. Bilaga 3 innehåller en parallelluppställning över direktivets artiklar och de bestämmelser i gällande rätt eller i utredningens författningsförslag som genomför varje artikel.

3 NIS-direktivet

Europaparlamentet och Europeiska rådet antog den 6 juli 2016 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). Direktivet ska vara genomfört i svensk rätt den 9 maj 2018.

Detta kapitel innehåller en övergripande beskrivning av de bestämmelser i direktivet som är av störst betydelse för genomförandet i svensk rätt. Mer detaljerade redogörelser för bestämmelserna finns i anslutning till de avsnitt som behandlar de specifika frågorna. Direktivet i sin helhet finns i bilaga 2.

3.1 Bakgrund och syfte

Syftet med NIS-direktivet är att förbättra den inre marknadens funktion genom att skapa tillit och förtroende och fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen (artikel 1.1 och skäl 31). I skälen till direktivet anges följande.

Nätverk och informationssystem och nätverks- och informationstjänster spelar en viktig roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och i synnerhet för den inre marknadens funktion. Säkerhetsincidenter, som blir allt mer omfattande och vanliga och får allt större inverkan, utgör ett allvarligt hot mot nätverkens och informationssystemens funktion. Dessa system kan också bli mål för avsiktligt sabotage i syfte att skada dem eller förorsaka driftsavbrott. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande ekonomiska förluster, undergräva användarnas förtroende och medföra allvarliga konsekvenser för unionens eko-

nomi. Nätverk och informationssystem, i synnerhet internet, spelar en viktig roll genom att underlätta den gränsöverskridande rörligheten för varor, tjänster och personer. På grund av denna transnationella natur kan allvarliga störningar av dessa system, vare sig de är avsiktliga eller oavsiktliga och oberoende av var de förekommer, påverka enskilda medlemsstater och unionen som helhet. Säkerheten i nätverk och informationssystem är därför avgörande för att den inre marknaden ska fungera väl. (skäl 1–3)

För att främja diskussioner och utbyten av bästa praxis mellan medlemsstaterna, inbegripet utarbetandet av principer för ett samarbete vid it-relaterade kriser, bör en samarbetsgrupp inrättas. Samarbetsgruppen ska stödja och underlätta strategiskt samarbete mellan medlemsstaterna vad gäller säkerhet i nätverk och informationssystem. Den ska bestå av företrädare för medlemsstaterna, kommissionen och Europeiska unionens byrå för nät- och informationssäkerhet (Enisa). För att gruppen ska vara effektiv och inkluderande är det viktigt att alla medlemsstater har en minimikapacitet och en strategi som säkerställer en hög nivå på säkerheten i nätverk och informationssystem på det egna territoriet. Dessutom bör säkerhets- och rapporteringskrav gälla för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, för att främja en riskhanteringskultur och säkerställa att de allvarligaste incidenterna rapporteras. (skäl 4)

Medlemsstaternas befintliga kapacitet räcker inte för att säkerställa en hög nivå på säkerheten i nätverk och informationssystem i unionen. Medlemsstaterna har mycket olika beredskapsnivåer, vilket har lett till skilda tillvägagångssätt i unionen. Resultatet blir olika skyddsnivåer för konsumenter och företag, vilket undergräver den allmänna nivån på säkerheten i nätverk och informationssystem i unionen. Avsaknaden av gemensamma krav för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster gör det i sin tur omöjligt att inrätta en övergripande och effektiv mekanism för samarbete på unionsnivå. Effektiva åtgärder för att lösa problemen vad gäller säkerhet i nätverk och informationssystem förutsätter därför ett övergripande angreppssätt på unionsnivå, som omfattar en gemensam miniminivå för kapacitetsuppbyggnad och planering, utbyte av information, samarbete och gemensamma säkerhetskrav för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. (skäl 5–6)

3.2 Medlemsstaternas skyldigheter enligt direktivet

Direktivet fastställer åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen, i syfte att förbättra den inre marknadens funktion (artikel 1.1 och 1.2). Åtgärderna innebär att medlemsstaterna ska

- anta en nationell strategi för säkerhet i nätverk och informationssystem (artikel 7),
- införa säkerhets- och incidentrapporteringskrav för leverantörer av samhällsviktiga tjänster och för leverantörer av digitala tjänster (artiklarna 14.1–3 och 16.1–3),
- utse nationella behöriga myndigheter, nationella kontaktpunkter och enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) och reglera samarbetet dem emellan (artiklarna 8.1, 8.3, 9.1 och 10),
- ingå i en samarbetsgrupp för strategiskt samarbete och informationsutbyte (artikel 11) och
- ingå i ett nätverk för enheter för hantering av it-säkerhetsincidenter (CSIRT-nätverk) (artikel 12).

Medlemsstaterna ska också, senast den 9 november 2018,

- identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium, och i det syftet
- upprätta en förteckning över tjänster som är viktiga för att upprätthålla kritisk samhällelig och/eller ekonomisk verksamhet (artikel 5.1, 5.3 och 5.2 a).

När det gäller leverantörer av samhällsviktiga tjänster får medlemsstaterna anta eller behålla bestämmelser som syftar till att uppnå en högre nivå på säkerheten i nätverk och informationssystem än vad direktivet kräver (artikel 3). För leverantörer av digitala tjänster får medlemsstaterna dock inte införa ytterligare säkerhets- eller rapporteringskrav (artikel 16.10).

3.2.1 En nationell strategi

I betänkandet *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten* (SOU 2015:23) föreslås att regeringen ska anta en nationell strategi för statens informations- och cybersäkerhet. Betänkandet har remitterats och bereds för närvarande inom Regeringskansliet. Regeringen avser att prioritera detta arbete och bedömer att strategin bör kunna anpassas för att motsvara direktivets krav på vad en nationell strategi för säkerhet i nätverk och informationssystem ska innehålla. Frågan om hur en sådan strategi bör utformas omfattas enligt kommittédirektiven inte av utredarens uppdrag.

3.2.2 Identifiering av leverantörer av samhällsviktiga tjänster och upprättande av en förteckning över samhällsviktiga tjänster

En leverantör av samhällsviktiga tjänster definieras i direktivet som en offentlig eller privat enhet av en typ som avses i bilaga 2 till direktivet och som uppfyller vissa kriterier. Enheterna finns inom sju sektorer:

- Energi, med delsektorerna elektricitet, olja och gas
- Transporter, med delsektorerna lufttransport, järnvägstransport, sjöfart och vägtransport
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvårdssektorn, med delsektor hälso- och sjukvårdsmiljöer (inklusive sjukhus och privata kliniker)
- Leverans och distribution av dricksvatten
- Digital infrastruktur

Kriterierna innebär att leverantören, för att träffas av direktivets bestämmelser, ska tillhandahålla en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, att tillhandahållandet av tjänsten ska vara beroende av nätverk och informations-

system samt att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. (artiklarna 4.4 och 5.2).

Medlemsstaterna bör enligt direktivet ansvara för att fastställa vilka enheter som uppfyller kriterierna för definitionen av leverantör av samhällsviktiga tjänster. I syfte att säkerställa ett enhetligt tillvägagångssätt bör definitionen av leverantör av samhällsviktiga tjänster tillämpas konsekvent i alla medlemsstater. (skäl 19) Medlemsstaterna ska mot den bakgrunden senast den 9 november 2018 identifiera de enheter som utgör leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium. För att en leverantör ska anses vara etablerad i en medlemsstat krävs att leverantören utför en faktisk och reell verksamhet med hjälp av en stabil struktur. Den rättsliga formen bör inte vara avgörande, oavsett om det är en filial eller ett dotterbolag med juridisk personlighet. (skäl 21)

För att kunna identifiera leverantörerna ska medlemsstaterna upprätta en förteckning över de tjänster som är viktiga för att upprätthålla kritisk samhällelig och/eller ekonomisk verksamhet (artikel 5.1, 5.2 a och 5.3). Syftet med förteckningen är alltså att urskilja de typer av samhällsviktiga *tjänster* inom en viss sektor som det hänvisas till i direktivet och därmed skilja dem från de icke samhällsviktiga tjänster som en enhet med verksamhet inom en viss sektor kan ansvara för. Vid bedömningen av om en enhet tillhandahåller en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, är det alltså tillräckligt att undersöka om enheten tillhandahåller en tjänst som finns upptagen i förteckningen (skäl 20). För att leverantören sedan ska omfattas av direktivets krav gäller därutöver att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

För att en leverantör ska omfattas av direktivets bestämmelser krävs alltså först och främst att leverantören tillhandahåller en tjänst som finns på förteckningen över samhällsviktiga tjänster. Om tjänsten finns på förteckningen ska det i ett andra steg bedömas om leverantörens tillhandahållande av tjänsten är beroende av nätverk och informationssystem och om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

Medlemsstaterna ska minst vartannat år efter den 9 maj 2018 se över och vid behov uppdatera förteckningen (artikel 5.5). Förteckningen ska senast den 9 november 2018 och därefter vartannat år

tillhandahållas kommissionen som ett led i kommissionens arbete med att bedöma genomförandet av direktivet. Även information om antalet leverantörer av samhällsviktiga tjänster i varje sektor som avses i bilaga 2 till direktivet samt en uppgift om deras betydelse för sektorn ska lämnas till kommissionen (artikel 5.7 b–c).

3.2.3 Säkerhets- och incidentrapporteringskrav för leverantörer av samhällsviktiga tjänster och för leverantörer av digitala tjänster

Leverantörer av samhällsviktiga tjänster

Medlemsstaterna ska säkerställa att leverantörer av samhällsviktiga tjänster *vidtar* ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder i sin verksamhet. Leverantörerna ska också åläggas att vidta lämpliga åtgärder för att förebygga och minimera verkningarna av incidenter som påverkar säkerheten i nätverk och informationssystem som används för att tillhandahålla sådana samhällsviktiga tjänster, i syfte att säkerställa kontinuiteten i dessa tjänster. Medlemsstaterna ska också säkerställa att leverantörer av samhällsviktiga tjänster utan onödigt dröjsmål till den behöriga myndigheten eller CSIRT-enheten rapporterar incidenter som har en *betydande inverkan* på *kontinuiteten* i de samhällsviktiga tjänster som de tillhandahåller. För att fastställa om en incident har betydande inverkan ska hänsyn tas till vissa särskilt angivna faktorer.

De samhällsviktiga tjänster som omfattas av direktivet finns inom sju olika sektorer vilka anges i bilaga 2 till direktivet. Sektorerna är energi, transporter, bankverksamhet, finsansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, leverans och distribution av dricksvatten samt digital infrastruktur. Inom sektorerna specificeras olika typer av enheter som bedriver verksamhet inom sektorerna. För att en leverantör ska omfattas av direktivet krävs att leverantören utgör en sådan enhet som anges i direktivet. Enheterna finns beskrivna kapitel 4 i betänkandet.

Leverantörer av digitala tjänster

De digitala tjänster som omfattas av direktivet anges i bilaga 3 till NIS-direktivet. Dessa är

- internetbaserade marknadsplatser
- internetbaserade sökmotorer
- molntjänster

Medlemsstaterna ska säkerställa att leverantörerna av dessa tjänster *utarbetar och vidtar* ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder när de tillhandahåller tjänsterna inom unionen. Medlemsstaterna ska också säkerställa att leverantörer av digitala tjänster vidtar åtgärder för att förebygga och minimera den inverkan som incidenter som påverkar säkerheten i deras nätverk och informationssystem har på de angivna tjänsterna och som erbjuds inom unionen, i syfte att säkerställa kontinuiteten i dessa tjänster. Medlemsstaterna ska därutöver säkerställa att leverantörer av digitala tjänster utan onödigt dröjsmål till den behöriga myndigheten eller CSIRT-enheten rapporterar alla incidenter som har en *avsevärd inverkan* på *tillhandahållandet* av en tjänst som avses i bilaga 3 till NIS-direktivet och som de erbjuder inom unionen. För att fastställa om en incident har avsevärd inverkan ska hänsyn tas till vissa särskilt angivna faktorer. Kommissionen ska senast den 9 augusti 2017 anta genomförandeakter för att specificera faktorerna.

En leverantör av digitala tjänster ska omfattas av jurisdiktionen i den medlemsstat där leverantören har sitt huvudsakliga etableringsställe. En leverantör av digitala tjänster ska anses ha sitt huvudsakliga etableringsställe i en medlemsstat om den har sitt huvudkontor i denna medlemsstat. En leverantör av digitala tjänster som inte är etablerad i unionen men som erbjuder sådana tjänster som avses i bilaga 3 till direktivet inom unionen ska utse en företrädare i unionen. Företrädaren ska vara etablerad i en av de medlemsstater där tjänsterna erbjuds. Leverantören av digitala tjänster ska anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad. (artikel 18.1–2)

3.2.4 Tillsyn och sanktioner

Nationella behöriga myndigheter (artikel 8.1)

Varje medlemsstat ska utse en eller flera nationella behöriga myndigheter för säkerhet i nätverk och informationssystem, åtminstone för de sektorer och de tjänster som avses i bilaga 2 och 3 till direktivet. De behöriga myndigheterna ska övervaka tillämpningen av direktivet på nationell nivå.

Leverantörer av samhällsviktiga tjänster (artikel 15.1–3)

Medlemsstaterna ska säkerställa att de behöriga myndigheterna har de befogenheter och medel som de behöver för att bedöma om leverantörerna av samhällsviktiga tjänster uppfyller säkerhetskraven och kravet att incidentrapportera. De behöriga myndigheterna ska också ha de befogenheter och medel som krävs för att ålägga leverantörerna att tillhandahålla den information som är nödvändig för att bedöma säkerheten i leverantörernas nätverk och informationssystem och bevis för ett effektivt genomförande av säkerhetsprinciper. Den behöriga myndigheten ska ha rätt att utfärda bindande anvisningar till leverantörerna om hur de ska avhjälpa de identifierade bristerna.

Leverantörer av digitala tjänster (artikel 17.1–3)

När det gäller leverantörer av digitala tjänster ska medlemsstaterna säkerställa att de behöriga myndigheterna vid behov vidtar åtgärder genom tillsynsåtgärder *i efterhand*, när de har mottagit bevis på att en leverantör av digitala tjänster inte uppfyller direktivets krav. De behöriga myndigheterna ska ha de befogenheter och medel som krävs för att ålägga leverantörerna att tillhandahålla den information som behövs för en bedömning av säkerheten i deras nätverk och informationssystem, och för att ålägga leverantörerna att åtgärda varje underlåtenhet att uppfylla direktivets krav.

Om en leverantör av digitala tjänster har sitt huvudsakliga etableringsställe eller en företrädare i en medlemsstat, men dess nätverk eller informationssystem är belägna i en eller flera andra medlemsstater, ska den behöriga myndigheten där det huvudsakliga etableringsstället eller företrädaren finns och de behöriga myndigheterna

i de andra berörda medlemsstaterna samarbeta och vid behov bistå varandra. Samarbetet får omfatta informationsutbyte mellan de berörda behöriga myndigheterna och begäranden om att leverantörerna ska tillhandahålla den information som behövs för tillsynen samt att de ska åläggas att åtgärda underlåtenhet att uppfylla direktivets krav.

Sanktioner (artikel 21)

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av de nationella bestämmelser som antagits enligt direktivet. Sanktionerna ska vara effektiva, proportionella och avskräckande.

3.2.5 Nationell kontaktpunkt

Varje medlemsstat ska utse en gemensam nationell kontaktpunkt för säkerhet i nätverk och informationssystem. Om en medlemsstat bara utser en behörig myndighet, ska den myndigheten också vara den nationella kontaktpunkten. Den nationella kontaktpunkten ska utöva en sambandsfunktion för att säkerställa gränsöverskridande samarbete mellan medlemsstaternas myndigheter och med de berörda myndigheterna i andra medlemsstater samt med samarbetsgruppen och CSIRT-nätverket.

Medlemsstaterna ska säkerställa att de behöriga myndigheterna eller CSIRT-enheterna informerar de nationella kontaktpunkterna om incidentrapporter som lämnats in i enlighet med direktivet. Den nationella kontaktpunkten ska senast den 9 augusti 2018 och därefter en gång om året lämna en sammanfattande rapport till samarbetsgruppen om de rapporter som mottagits, inklusive antalet mottagna incidentrapporter och de rapporterade incidenternas art, samt om vilka åtgärder som vidtagits (artikel 10.3). Rapporten bör vara anonymiserad, eftersom information om de rapporterande enheternas identitet inte krävs för utbyte av bästa praxis inom samarbetsgruppen (skäl 33).

3.2.6 CSIRT-enheter

Varje medlemsstat ska utse en eller flera enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter). CSIRT-enheterna ska ansvara för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande. De ska uppfylla vissa krav som finns angivna i bilaga 1 till direktivet, bl.a. när det gäller driftskontinuitet. CSIRT-enheterna ska täcka åtminstone de sektorer som avses i direktivets bilaga 2 och de tjänster som avses i bilaga 3 till direktivet. Medlemsstaterna ska säkerställa att CSIRT-enheterna har de resurser som de behöver för att effektivt utföra sina uppgifter enligt punkt 2 i bilaga 1 till direktivet. Medlemsstaterna ska också säkerställa att deras CSIRT-enheter samarbetar på ett ändamålsenligt, effektivt och säkert sätt i det CSIRT-nätverk som avses i artikel 12. CSIRT-enheterna ska också ha tillgång till lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur på nationell nivå. 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 NIS-direktivet (skäl 34).

3.2.7 Samarbete på nationell nivå

Om den behöriga myndigheten, den nationella kontaktpunkten och CSIRT-enheten i en medlemsstat är separata, ska de samarbeta när det gäller fullgörandet av skyldigheterna enligt direktivet. De incidentrapporter som lämnas in i enlighet med direktivet ska tas emot av antingen de behöriga myndigheterna eller CSIRT-enheterna. Om en medlemsstat beslutar att CSIRT-enheterna inte ska ta emot rapporter ska CSIRT-enheterna, i den mån det är nödvändigt för att de ska kunna utföra sina uppgifter, beviljas tillgång till uppgifter om incidenter som rapporterats. Medlemsstaterna ska säkerställa att de behöriga myndigheterna eller CSIRT-enheterna informerar de nationella kontaktpunkterna om incidentrapporter som lämnats in.

3.2.8 En samarbetsgrupp för strategiskt samarbete och informationsutbyte

Genom direktivet inrättas en samarbetsgrupp för att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna och skapa förtroende och tillit. Samarbetsgruppen består av företrädare för medlemsstaterna, kommissionen och European Union Agency for Network and Information Security (Enisa). De närmare uppgifterna för samarbetsgruppen anges i artikel 11.3. Samarbetsgruppen ska bl.a. tillhandahålla strategisk vägledning för verksamheten i CSIRT-nätverket (se nedan), utbyta bästa praxis om informationsutbyte angående incidentrapporteringen, med Enisas bistånd utbyta bästa praxis för medlemsstaternas identifiering av leverantörer av samhällsviktiga tjänster samt diskutera metoder för rapportering av incidentrapporter.

3.2.9 Ett nätverk för enheter för hantering av it-säkerhetsincidenter (CSIRT-nätverk)

Genom direktivet inrättas ett nätverk för nationella CSIRT-kontakter för att bidra till utvecklingen av förtroende och tillit mellan medlemsstaterna och för att främja snabbt och effektivt operativt samarbete. CSIRT-nätverket ska bestå av företrädare för medlemsstaternas CSIRT-enheter och Cert-EU (incidenthanteringsorganisationen för EU:s institutioner, organ och kontor). Kommissionen ska delta i CSIRT-nätverket som observatör. Enisa ska tillhandahålla sekretariat och aktivt stödja samarbetet mellan CSIRT-enheterna. CSIRT-nätverkets närmare uppgifter anges i artikel 12.3. Nätverket ska bl.a. utbyta information om CSIRT-enheternas tjänster, verksamhet och samarbetskapacitet, på frivillig grund utbyta och tillgängliggöra icke-konfidentiella uppgifter om enskilda incidenter, på begäran av en företrädare för en medlemsstats CSIRT-enhet diskutera och om möjligt utarbeta en samordnad åtgärd till följd av en incident som har upptäckts inom den medlemsstatens jurisdiktion, samt diskutera, utforska och identifiera ytterligare former av operativt samarbete.

3.3 Undantag från NIS-direktivets tillämpningsområde

Företag som omfattas av kraven i artiklarna 13a och 13b i direktiv 2002/21/EG – tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster

Säkerhets- och rapporteringskraven enligt NIS-direktivet ska enligt artikel 1.3 inte tillämpas på företag som omfattas av kraven i artiklarna 13a och 13b i Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektivet).

Artikel 13a i ramdirektivet ställer krav på tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster att bl.a. vidta lämpliga tekniska och organisatoriska åtgärder för att på ett tillfredsställande sätt skydda säkerheten för sina nät eller tjänster. Artikel 13b innehåller bestämmelser om tillämpning och genomförande. Bland annat anges att de nationella regleringsmyndigheterna ska ha befogenheter att utfärda bindande instruktioner samt att kräva att tillhandahållare av nät och tjänster tillhandahåller viss information och på egen bekostnad underkasta sig säkerhetsgranskningar.

Artiklarna har genomförts i svensk rätt genom 5 kap. 6 b och c §§ lagen (2003:389) om elektronisk kommunikation (LEK).

Av 5 kap. 6 b § LEK framgår bl.a. att den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet. De åtgärder som vidtas ska vara ägnade att skapa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för störningar och avbrott.

I 5 kap. 6 c § LEK anges bl.a. att den som tillhandahåller ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst utan onödigt dröjsmål till tillsynsmyndigheten ska rapportera störningar eller avbrott av betydande omfattning. Post- och telestyrelsen (PTS) är tillsynsmyndighet och mottagare av incidentrapporter enligt denna reglering.

Leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 i förordningen (EU) nr 910/2014

Säkerhets- och rapporteringskraven enligt NIS-direktivet ska enligt artikel 1.3 inte tillämpas på leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 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 (eIDAS-förordningen).

Med betrodda tjänster avses elektroniska underskrifter och stämplar, validering och bevarande av elektroniska underskrifter och stämplar, tjänster för rekommenderad elektronisk leverans och utfärdande av certifikat för autentisering av webbplatser.

Bestämmelserna i artikel 19 i eIDAS-förordningen innebär att alla tillhandahållare av betrodda tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som de tillhandahåller. Tillhandahållarna ska också underrätta tillsynsorganet om alla säkerhetsincidenter eller integritetsförluster som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls eller de personuppgifter som ingår i denna. PTS är tillsynsmyndighet för betrodda tjänster och mottagare av underrättelser om säkerhetsincidenter och integritetsförluster.[1]

Direktiv 2008/114/EG (ECI-direktivet)

NIS-direktivet påverkar enligt artikel 1.4 inte tillämpningen av 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 (ECI-direktivet).

ECI-direktivet omfattar sektorerna energi och transport. Enligt direktivet ska medlemsstaterna inom de sektorerna identifiera och genom klassificering utse europeisk kritisk infrastruktur och bedöma behovet av att stärka skyddet av den. Med europeisk kritisk infrastruktur avses kritisk infrastruktur vars driftsstörning eller för-

[1] Lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

störelse skulle få betydande konsekvenser för minst två medlemsstater. Sverige har hittills inte pekat ut någon europeisk kritisk infrastruktur på sitt territorium.

Direktiv 2011/93/EU

NIS-direktivet påverkar enligt artikel 1.4 inte tillämpningen av 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. Det direktivets syfte är att fastställa minimiregler för brottsrekvisit och påföljder när det gäller sexuella övergrepp mot och sexuell exploatering av barn, barnpornografi och kontaktsökning med barn för sexuella ändamål. Syftet är vidare att stärka åtgärderna för att förebygga sådana brott och förbättra skyddet för dess offer.

Direktiv 2013/40/EU

NIS-direktivet påverkar enligt artikel 1.4 inte tillämpningen av 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. Det direktivets mål är att närma medlemsstaternas strafflagstiftning till varandra när det gäller angrepp mot informationssystem genom att fastställa minimiregler för brottsrekvisit och påföljder. Syftet är också att främja förebyggandet av sådana brott och förbättra samarbetet mellan rättsliga och andra behöriga myndigheter.

Åtgärder till skydd för den nationella säkerheten m.m.

Direktivet påverkar inte medlemsstaternas åtgärder för att skydda sina väsentliga statliga funktioner, särskilt för att skydda den nationella säkerheten, inklusive åtgärder för skydd av information vars avslöjande medlemsstaterna anser strida mot sina väsentliga säkerhetsintressen, och för att upprätthålla lag och ordning, särskilt för att möjliggöra utredning, upptäckt och lagföring av brott (artikel 1.6).

Sektorspecifik reglering/lex specialis

Om det i en sektorspecifik unionsrättsakt föreskrivs krav på att leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster antingen ska säkerställa säkerheten i sina nätverk och informationssystem eller rapportera incidenter, ska enligt artikel 1.7 bestämmelserna i den sektorspecifika unionsrättsakten tillämpas, förutsatt att verkan av kraven i fråga minst motsvarar verkan av skyldigheterna i NIS-direktivet. Medlemsstaterna bör då tillämpa bestämmelserna i sådana sektorspecifika unionsrättsakter, inklusive sådana som rör jurisdiktion, och bör inte genomföra identifieringsförfarandet för leverantörer av samhällsviktiga tjänster enligt definitionen i NIS-direktivet (skäl 9).

I *sjöfartssektorn* omfattar säkerhetskraven för rederier, fartyg, hamnanläggningar, hamnar och sjötrafikinformationstjänster enligt unionsrättsakter all verksamhet, inbegripet radio- och telekommunikationssystem, datorsystem och nätverk. De obligatoriska förfarandena inbegriper rapportering av alla incidenter och bör därför anses utgöra lex specialis, i den mån dessa krav är åtminstone likvärdiga med motsvarande bestämmelser i NIS- direktivet (skäl 10).

Regleringen och tillsynen inom *banksektorn och sektorn för finansmarknadsinfrastrukturer* har i hög grad harmoniserats på unionsnivå, genom användning av unionens primärrätt och sekundärrätt och standarder som utvecklats tillsammans med de europeiska tillsynsmyndigheterna. Inom bankunionen säkerställs tillämpningen och tillsynen av dessa krav genom den gemensamma tillsynsmekanismen. För Sverige, som inte ingår i bankunionen, säkerställs detta av Finansinspektionen. Inom tillsynspraxis på andra områden inom regleringen av finanssektorn säkerställer Europeiska systemet för finansiell tillsyn också en hög grad av enhetlighet och konvergens. Även Europeiska värdepappers- och marknadsmyndigheten utövar direkt tillsyn över vissa enheter, nämligen kreditvärderingsinstitut och transaktionsregister (skäl 12).

Operativ risk utgör en viktig del av reglering och tillsyn inom banksektorn och sektorn för finansmarknadsinfrastrukturer. Den omfattar all verksamhet, inbegripet nätverks och informationssystems säkerhet, integritet och motståndskraft. Kraven på dessa system, som ofta är mer långtgående än de som föreskrivs i NIS-direktivet, fastställs i ett antal unionsrättsakter. Krav på rapporte-

ring av incidenter utgör vidare en del av normal tillsynspraxis inom finanssektorn och ingår ofta i tillsynshandböcker. (skäl 13)

3.4 Personuppgifter

Behandling av personuppgifter enligt NIS-direktivet ska ske i enlighet med Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om behandling av det fria flödet av sådana uppgifter (dataskyddsdirektivet). Dataskyddsdirektivet har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204) (PUL). Den 27 april 2016 beslutade EU om en förordning med en ny generell reglering för personuppgiftsbehandling inom EU – Europaparlamentets och rådets förordning (EU) 2016/679 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). Förordningen kommer att ersätta det nuvarande dataskyddsdirektivet. Den är direkt tillämplig i medlemsstaterna men både förutsätter och möjliggör kompletterande nationella bestämmelser av olika slag. Dataskyddsförordningen kommer att utgöra grunden för generell personuppgiftsbehandling inom EU, vilket innebär att bl.a. PUL måste upphävas. En särskild utredare har fått i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som förordning ger anledning till (dir. 2016:15). Ett delbetänkande, *Brottsdatalag* (SOU 2017:29), överlämnades den 5 april 2017. Uppdraget ska slutredovisas senast den 12 maj 2017.

Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF innehåller regler om skydd av personuppgifter när behöriga myndigheter behandlar sådana uppgifter vid brottsbekämpning, brottmålshantering eller straffverkställighet. Direktivet ålägger medlemsstaterna att bl.a. föreskriva effektiva, proportionella och avskräckande sanktioner för överträdelser av bestämmelser som antas enligt direktivet. Regeringen har i

mars 2016 tillsatt en utredning som ska föreslå hur direktivet ska genomföras i svensk rätt[2]. Uppdraget ska slutredovisas senast den 30 september 2017.

Behandling av personuppgifter som utförs av unionens institutioner och organ enligt direktivet ska ske i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (artikel 2.2).

[2] Utredningen om 2016 års dataskyddsdirektiv, Ju 2016:06, dir. 2016:21.

4 Beskrivning av enheterna

4.1 Inledning

Utredningen har träffat företrädare för samtliga sektorer och gjort en övergripande inventering av nuvarande reglering när det gäller informationssäkerhet, incidentrapportering och tillsyn samt i vilken utsträckning sektorn, delsektorn och enheten gör risk- och sårbarhetsanalyser, se ärende dnr Komm2017/00542-1. Inventeringen har med hänsyn till den tid som utredningen haft till sitt förfogande inte kunnat göras fullständig.

Deltagarna i referensgruppen samt företrädare för Inspektionen för vård och omsorg Datainspektionen, Läkemedelsverket och Energimarknadsinspektionen har bidragit med underlag till inventeringen. Samtliga myndigheter och organisationer har beretts tillfälle att lämna synpunkter på utredningens beskrivning av respektive sektor. För några sektorer har referensgruppen också kunnat ge en ungefärlig bild av hur många leverantörer som skulle kunna anses tillhandahålla en samhällsviktig tjänst enligt NIS-direktivet.

Utredningens bedömning är att den inventering som gjorts är tillräcklig för att få den övergripanden bilden av hur reglering, tillsyn m.m. ser ut inom respektive sektor för att kunna genomföra NIS-direktivet i svensk rätt.

Bestämmelser om säkerhetsåtgärder i nätverk och informationssystem, risk- och säkerhetsanalyser och incidentrapportering finns redan i flera av de sektorer som omfattas av NIS-direktivet, både i nationella bestämmelser och i EU-rättsakter. Regleringen är emellertid inte heltäckande och i några fall är syftet med säkerhetsåtgärderna och incidentrapporteringen ett annat än syftet i NIS-direktivet.

Utgångspunkten för bedömningen av vilka samhällsviktiga tjänster och digitala tjänster som omfattas av den nya lagen är de typer av enheter som anges i bilaga 2 till NIS-direktivet.

Följande enheter omfattas av NIS-direktivet inom respektive sektor i Sverige.

4.2 Energi

Elektricitet

• *Elföretag* enligt definitionen i artikel 2.35 i 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 som bedriver ”leverans eller handel” enligt definitionen i artikel 2.19 i det direktivet.

Med elföretag avses varje fysisk eller juridisk person, med undantag för slutförbrukare, som bedriver åtminstone en av följande verksamheter: produktion, överföring, distribution, leverans eller inköp av el och som ansvarar för kommersiella och tekniska arbetsuppgifter eller underhåll i samband med dessa verksamheter

Med leverans eller handel avses försäljning, inbegripet återförsäljning, av el till kunder.

Elföretag benämns elleverantörer och det finns cirka 200 sådana i Sverige (1 kap. 6 § ellagen [1997:857]).

• *Systemansvariga för distributionssystemet* enligt definitionen i artikel 2.6 i 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.

Med systemansvarig för distributionssystemet avses varje fysisk eller juridisk person som ansvarar för drift och underhåll och, vid behov, utbyggnad av distributionssystemet inom ett visst område och, i tillämpliga fall, dess sammanlänkningar till andra system och för att säkerställa att systemet på lång sikt kan uppfylla rimliga krav på distribution av el.

Dessa benämns elnätsföretag och bestämmelser om företag som bedriver nätverksamhet m.m. finns i 1 kap. 4 § och 3 kap. ellagen (1997:857). Det finns ca 160 elnätsföretag i Sverige.

• *Systemansvariga för överföringssystemet* enligt definitionen i artikel 2.4 i 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.

Med systemansvarig för överföringssystemet avses varje fysisk eller juridisk person som ansvarar för drift och underhåll och, vid behov, utbyggnad av överföringssystemet inom ett visst område och, i tillämpliga fall, dess sammanlänkningar till andra system och för att säkerställa att systemet på lång sikt kan uppfylla rimliga krav på överföring av el.

I Sverige är Affärsverket svenska kraftnät, som förvaltar stamnätet, systemansvarig för överföringssystemet (1 kap. 5 b § ellagen [1997:857]). Det bör anmärkas att systemansvarig för överföringssystemet i direktivets mening är någonting annat än systemansvarig myndighet enligt 8 kap. 1 § ellagen (prop. 2010/11:70 s. 57).

Olja

• *Operatörer av oljeledningar*

Det saknas operatörer av oljeledningar i Sverige.

• *Operatörer av oljeproduktion, raffinaderier, bearbetningsanläggningar, lagring och överföring*

I Sverige finns fem raffinaderier och 21 depåer som kan komma att omfattas av NIS-direktivet.

Gas

• *Gashandelsföretag eller gashandlare* enligt definitionen i artikel 2.8 i 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.

Med gashandelsföretag eller gashandlare avses varje fysisk eller juridisk person som bedriver leveransverksamhet.

I Sverige finns cirka tio stycken aktörer som kan omfattas av NIS-direktivet.

• *Systemansvariga för distributionssystemet* enligt definitionen i artikel 2.6 i 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.

Med systemansvarig för distributionssystemet avses varje fysisk eller juridisk person som bedriver distributionsverksamhet och som ansvarar för drift och underhåll och, vid behov, utbyggnad av distributionssystemet inom ett visst område och, i tillämpliga fall, dess sammanlänkningar till andra system och för att säkerställa att systemet på lång sikt kan uppfylla rimliga krav på gasdistribution.

I Sverige finns sex systemansvariga som kan omfattas av NIS-direktivet.

• *Systemansvariga för överföringssystemet* enligt definitionen i artikel 2.4 i 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.

Med systemansvarig för överföringssystemet avses varje fysisk eller juridisk person som bedriver överföringsverksamhet och som ansvarar för drift och underhåll och, vid behov, utbyggnad av överföringssystemet inom ett visst område och, i tillämpliga fall, dess sammanlänkningar till andra system och för att säkerställa att systemet på lång sikt kan uppfylla rimliga krav på gastransporter.

I Sverige är Swedegas AB systemansvarig för överföringssystemet.

• *Systemansvariga för lagringssystemet* enligt definitionen i artikel 2.10 i 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.

Med systemansvarig för lagringssystemet avses varje fysisk eller juridisk person som bedriver lagringsverksamhet och som ansvarar för driften av en lagringsanläggning.

Med lagringsanläggning avses en anläggning som används för lagring av naturgas och som ägs och/eller drivs av ett naturgasföretag, inbegripet den del av en LNG-anläggning[1] som används för lagring men undantaget den del som används för produktionsverksamhet, och undantaget anläggningar som uteslutande är förbehållna systemansvariga för överföringssystemet när de utför sina uppgifter.

I Sverige finns en systemansvarig, Swedegas AB.

• *Systemansvariga för en LNG-anläggning* enligt definitionen i artikel 2.12 i 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.

Med systemansvarig för en LNG-anläggning avses varje fysisk eller juridisk person som ägnar sig åt kondensering av naturgas eller import, lossning och återförgasning av LNG och som ansvarar för driften av en LNG anläggning.

Med LNG-anläggning avses en terminal som används för kondensering av naturgas eller import, lossning och återförgasning av LNG, inklusive stödtjänster och den tillfälliga lagring som krävs för återförgasningsprocessen och efterföljande leverans till överföringssystemet, men undantaget den del av en LNG-anläggning som används för lagring.

Det saknas systemansvariga för LNG-anläggningar i Sverige enligt definitionen i NIS-direktivet. De svenska LNG-anläggningarna är inte kopplade till överföringssystemet.

• *Naturgasföretag* enligt definitionen i artikel 2.1 i 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.

[1] LNG=Liquid Natural Gas, dvs., flytande naturgas.

Med naturgasföretag avses varje fysisk eller juridisk person, med undantag för slutförbrukare, som bedriver åtminstone en av följande verksamheter: produktion, överföring, distribution, leverans, köp eller lagring av naturgas, inbegripet LNG, som ansvarar för kommersiella och tekniska arbetsuppgifter och/eller underhåll i samband med dessa verksamheter.

Naturgasföretag är ett samlingsbegrepp och vissa av enheterna ovan ingår i begreppet vilket innebär att det i dag inte är möjligt att redovisa en exakt siffra på antalet enheter.

- *Operatörer av raffinaderier och bearbetningsanläggningar för naturgas*.

4.3 Transporter

Lufttransport

- *Lufttrafikföretag* enligt definitionen i artikel 3.4 i 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.

Med lufttrafikföretag avse ett lufttransportföretag med giltig operativ licens eller motsvarande.

I dag omfattas 31 stycken flygföretag men definitionen medför att även andra typer av flygverksamhet skulle kunna omfattas.

- *Flygplatsens ledningsenheter* enligt definitionen i artikel 2.2 i Europaparlamentets och rådets direktiv 2009/12/EG av den 11 mars 2009 om flygplatsavgifter, 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 2013 av den 11 december 2013 om unionens riktlinjer för utbyggnad av det transeuropeiska transportnätet och om upphävande av beslut nr 661/2010/EU, och enheter som driver kringliggande installationer vid flygplatser.

Med flygplatsens ledningsenhet avses den enhet som, tillsammans med annan verksamhet eller självständigt, i kraft av nationella lagar och andra författningar eller avtal har i uppdrag att administrera och

förvalta flygplatsens eller flygplatsnätets infrastrukturer och samordna och kontrollera den verksamhet som bedrivs av de olika aktörer som befinner sig på berörd flygplats eller inom berört flygplatsnät.

Med flygplats avses varje markområde som är särskilt inrättat för landning, start och manövrering av luftfartyg, inbegripet de närliggande anläggningar som kan behövas för flygtrafiken och för service till luftfartygen, samt de anläggningar som behövs för de kommersiella luftfartstjänsterna. Enligt avsnitt 2 i bilaga II till 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 är Arlanda huvudflygplats.

Ett antal svenska flygplatser med sina ledningsfunktioner skulle kunna omfattas. Kringliggande installationer bör vara enheter som krävs för att flygplatsen ska kunna hantera den trafik som den är avsedd för men som inte är belägna inom flygplatsens område. Sådana installationer bör vara navigationshjälpmedel, övervakning och kommunikation som används vid in- och utflygning.

• *Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänst* enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 549/2004 av den 10 mars 2004 om ramen för inrättande av det gemensamma europeiska luftrummet (”ramförordning”).

Med flygkontrolltjänst avses en tjänst som tillhandahålls i syfte att förebygga kollisioner mellan luftfartyg, och mellan luftfartyg och ett hinder inom manöverområdet, samt påskynda och bibehålla ett välordnat flygtrafikflöde.

Luftfartsverket, Aviation Capacity Resources (ACR), Arvidsjaurs flygplats (Afab) och Nuac HB är aktörer som omfattas av denna definition.

Järnvägstransport

• *Infrastrukturförvaltare* enligt definitionen i artikel 3.2 i Europaparlamentets och rådets direktiv 2012/34/EU av den 21 november 2012 om inrättande av ett gemensamt europeiskt järnvägsområde.

Med infrastrukturförvaltare avses varje organ eller företag som särskilt ansvarar för att anlägga, förvalta och underhålla järnvägsinfrastruktur, inklusive trafikledning, trafikstyrning och signalering. Infrastrukturförvaltarens uppgifter med avseende på järnvägsnät eller del av ett järnvägsnät får tilldelas olika organ eller företag. Järnvägsinfrastruktur är de anläggningar som finns förtecknade i bilaga I till direktiv 2012/34/EU.

Trafikverket är infrastrukturförvaltare för det statliga järnvägsnätet.

• *Järnvägsföretag* enligt definitionen i artikel 3.1 i direktiv 2012/34/EU, inbegripet tjänsteleverantörer enligt definitionen i artikel 3.12 i direktiv 2012/34/EU av den 21 november 2012 om inrättande av ett gemensamt europeiskt järnvägsområde.

Med järnvägsföretag avses varje offentligt eller privat företag med tillstånd i enlighet med direktiv 2012/34/EU vars huvudsakliga verksamhet består i att tillhandahålla tjänster för transport av gods och/eller passagerare på järnväg med kravet att företaget måste tillhandahålla dragkraft; detta gäller även företag som endast tillhandahåller dragkraft.

Med tjänsteleverantör avses varje offentlig eller privat enhet som ansvarar för förvaltningen av en eller flera anläggningar för tjänster eller sådant tillhandahållande av en eller flera tjänster till järnvägsföretag som avses i punkterna 2–4 i bilaga II i direktiv 2012/34/EU.

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 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar, exklusive de enskilda fartyg som drivs av dessa företag.

Aktörer som omfattas är rederier och operatörer.

• *Ledningsenheter för hamnar* enligt definitionen i artikel 3.1 i Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd, inbegripet deras hamnanläggningar enligt definitionen i artikel 2.11 i förordning (EG) nr 725/2004 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar, och enheter som sköter anläggningar och utrustning i hamnar.

Med hamn avsesett specificerat land- och vattenområde, med gränser som fastställts av den medlemsstat i vilken hamnen befinner sig, vilket består av sådana anläggningar och sådan utrustning som underlättar kommersiella sjöfartstransporter.

Med hamnanläggning avses en plats där samverkan mellan fartyg och hamn äger rum. Detta inkluderar, i tillämpliga fall, områden såsom ankarplatser, väntekajer och insegling från sjösidan.

Sverige har en annan organisation av hamnar än övriga Europa genom att det saknas så kallade hamnmyndigheter (Port authorities).

• *Operatörer av sjötrafikinformationstjänster* enligt definitionen i artikel 3 o i 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.

Med Sjötrafikinformationstjänst (VTS) avses en tjänst för att förbättra sjötrafikens säkerhet och effektivitet och för att skydda miljön och som har förmåga att samverka med trafiken och hantera de trafiksituationer som uppstår inom sjötrafikinformationstjänstens område.

VTS utförs av Sjöfartsverket i nio VTS-områden.

Vägtransport

• *Vägmyndigheter* enligt definitionen i artikel 2.12 i 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 med ansvar för trafikstyrning och trafikledning.

Med vägmyndighet avses offentlig myndighet som ansvarar för planering, kontroll eller förvaltning av vägar som omfattas av dess territoriella behörighet.

Vägmyndigheter är Trafikverket och kommuner.

• *Operatörer av intelligenta transportsystem* enligt definitionen i artikel 4.1 i 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.

Med intelligenta transportsystem eller ITS avses system i vilka informations- och kommunikationsteknik tillämpas på vägtransportområdet, inklusive infrastruktur, fordon och användare, och för trafikledning och mobilitetshantering, samt för gränssnitt mot andra transportslag.

4.4 Bankverksamhet

• *Kreditinstitut* enligt definitionen i artikel 4.1 i 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 (CRR).

Med kreditinstitut avses ett företag vars verksamhet består i att från allmänheten ta emot insättningar eller andra återbetalbara medel och att bevilja krediter för egen räkning.

I svensk lagstiftning motsvarar definitionen begreppet finansieringsrörelse i 4 § lagen (2004:297) om bank- och finansieringsrörelse (LBF).

4.5 Finansmarknadsinfrastruktur

• *Operatörer av handelsplatser* enligt definitionen i artikel 4.24 i 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 (MiFID II).

Med handelsplats avses en reglerad marknad, en multilateral handelsplattform (MTF-plattform) eller en organiserad handelsplattform (OTF-plattform).

En reglerad marknad definieras som ett multilateralt system som drivs och/eller leds av en marknadsoperatör, vilket sammanför eller underlättar sammanförandet av flera tredjeparters köp- och säljintressen i finansiella instrument – inom systemet och i enlighet med dess icke-skönsmässiga regler – så att detta leder till ett kontrakt i fråga om finansiella instrument upptagna till handel enligt dess regler och/eller system, och som är auktoriserat och löpande verksamt och drivs i enlighet med bestämmelserna i avdelning III i MiFID II.

En MTF-plattform definieras som ett multilateralt system som drivs av ett värdepappersföretag eller en marknadsoperatör och som sammanför flera tredjeparters köp- och säljintressen i finansiella instrument – inom systemet och i enlighet med icke-skönsmässiga regler – så att detta leder till ett kontrakt i enlighet med bestämmelserna i avdelning II i MiFID II.

En OTF-plattform definieras som ett multilateralt system som inte är en reglerad marknad eller en MTF-plattform, och inom vilket flera tredjeparters köp- och säljintressen i obligationer, strukturerade finansiella produkter, utsläppsrätter eller derivat kan interagera inom systemet så att detta leder till ett kontrakt i enlighet med bestämmelserna i avdelning II i MiFID II.

Termen system avser både rent tekniska system tillsammans med handelsregler och system enbart bestående av handelsregler, dvs. utan att det finns något tekniskt handelssystem (skäl 7 i MiFIR).

De företag som i dag har Finansinspektionens tillstånd att driva handelsplattformar i Sverige är Nasdaq Stockholm AB (First North), Nordic Growth Market NGM AB (Nordic MTF) och ATS Finans AB (Aktietorget).

- *Centrala motparter* enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister.

Med central motpart avses en juridisk person som träder emellan motparterna i kontrakt som är föremål för handel på en eller flera finansmarknader och blir köpare till varje säljare och säljare till varje köpare.

4.6 Hälso- och sjukvårdssektorn

Hälso- och sjukvårdsmiljöer (inklusive sjukhus och privata kliniker)

• *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.

Med vårdgivare avses varje fysisk eller juridisk person eller varje annan entitet som lagligen bedriver hälso- och sjukvård på en medlemsstats territorium.

Med hälso- och sjukvård avses hälso- och sjukvårdstjänster som hälso- och sjukvårdspersonal tillhandahåller patienter i syfte att bedöma, bibehålla eller återställa deras hälsotillstånd, inbegripet förskrivning, utlämning och tillhandahållande av läkemedel och medicinska hjälpmedel enligt artikel 3 a.

4.7 Leverans och distribution av dricksvatten

• *Leverantörer och distributörer av dricksvatten* enligt definitionen i artikel 2.1 a rådets direktiv 98/83/EG av den 3 november 1998 om kvaliteten på dricksvatten, dock exklusive distributörer för vilka distribution av dricksvatten endast utgör en del av deras allmänna verksamhet, som består i distribution av andra förnödenheter och varor som inte anses utgöra samhällsviktiga tjänster.

Med dricksvatten avses allt vatten som, antingen i sitt ursprungliga tillstånd eller efter beredning, är avsett för dryck, för matlagning, för beredning av livsmedel eller för andra hushållsändamål, oberoende av dess ursprung och oavsett om det tillhandahålls genom ett distributionsnät, från tankbil/tankbåt, i flaskor eller i behållare.

4.8 Digital infrastruktur

- *Internetknutpunkter (IXP)*

Internetknutpunkter definieras i NIS-direktivet som en nätfacilitet som möjliggör sammankoppling av mer än två oberoende autonoma system, främst i syfte att underlätta utbytet av internettrafik. En internetknutpunkt tillhandhåller sammankoppling enbart för autonoma system och kräver inte att den internettrafik som passerar mellan två deltagande autonoma system passerar genom ett tredje autonomt system och ändrar inte heller trafiken eller påverkar den på något annat sätt (artikel 4.13).

Det finns ett antal tillhandahållare av internetknutpunkter i Sverige, bl.a. Netnod, Sol-ix, STH IX, Norrnod, IXOR och GIX.

- *Leverantörer av DNS-tjänster.*

Med domännamnssystem (DNS) avses enligt NIS-direktivet ett hierarkiskt, distribuerat namngivningssystem i ett nätverk som hanterar domännamnsförfrågningar. Med leverantör av DNS-tjänst avses en enhet som tillhandahåller DNS-tjänster på internet (artikel 4.14 och 4.15).

- *Registreringsenheter för toppdomäner.*

En registreringsenhet för toppdomäner definieras i NIS-direktivet som en enhet som administrerar och förvaltar registreringen av internetdomännamn under en specifik toppdomän (artikel 4.16).

I dag finns en nationell toppdomän för Sverige, .se, samt några toppdomäner, t.ex. toppdomänen .nu.

5 Genomförandet av direktivet

5.1 Allmänna utgångspunkter

5.1.1 Genomförande av EU-direktiv i svensk rätt

Ett EU-direktiv är bindande med avseende på det resultat som ska uppnås men överlåter åt de nationella myndigheterna att bestämma form och tillvägagångssätt för genomförandet (artikel 288 i fördraget om Europeiska unionens funktionssätt). En medlemsstat behöver vid genomförandet inte använda sig av samma terminologi och systematik som i direktivet så länge det avsedda resultatet uppnås. Om direktivet är ett minimidirektiv har medlemsstaterna möjlighet att införa strängare regler än vad som följer av direktivet. Om bestämmelserna däremot är fullharmoniserade (eller maximiharmoniserande) har medlemsstaterna inte rätt att införa kompletterande regler.

För att ett direktiv ska bli gällande i svensk rätt måste det genomföras, dvs. införlivas i den svenska rättsordningen. Det är regeringen som ansvarar för att EU-rättsliga direktiv genomförs korrekt och i rätt tid. I den utsträckning det krävs lagändringar för att genomföra hela eller delar av ett direktiv sker det i enlighet med den ordinarie lagstiftningsprocessen, vilket innefattar sedvanlig remiss- och riksdagsbehandling. Om det i svensk rätt redan finns bestämmelser som motsvarar bestämmelserna i ett direktiv uppfylls kraven i direktivet och några lagstiftningsåtgärder behöver då inte vidtas.

EU-kommissionen bevakar att medlemsstaterna följer och i rätt tid genomför de regler som EU har beslutat om. Om kommissionen anser att svensk lagstiftning eller beslut från svenska myndigheter inte följer EU:s regler kan den inleda ett så kallat överträdelseförfarande mot Sverige. Ett sådant förfarande kan ytterst leda till böter eller vite för fördragsbrott.

5.1.2 Utgångspunkter i NIS-direktivet

Vilka aktörer omfattas av NIS-direktivet?

För att en leverantör av samhällsviktiga tjänster ska omfattas av direktivet krävs att leverantören tillhandahåller tjänster inom någon av de i direktivet särskilt utpekade enheterna. Enheterna finns inom sju angivna sektorer. Sektorerna omfattar energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. De aktuella enheterna finns beskrivna i kapitel 4. Därutöver reglerar direktivet vissa leverantörer av digitala tjänster. Dessa leverantörer och regleringen av dem behandlas i kapitel 10.

Minimidirektiv eller full harmonisering?

När det gäller samhällsviktiga tjänster får medlemsstaterna anta eller behålla bestämmelser som syftar till att uppnå en högre nivå på säkerheten i nätverk och informationssystem än vad som anges i NIS-direktivet. För leverantörer av digitala tjänster får medlemsstaterna emellertid inte införa ytterligare säkerhets- eller rapporteringskrav (artiklarna 3 och 16.10).

Lex specialis

Vissa ekonomiska sektorer regleras redan eller kan komma att regleras av sektorspecifika unionsrättsakter som inbegriper regler med anknytning till säkerheten i nätverk och informationssystem. Om det i en sådan unionsrättsakt föreskrivs krav på att leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster antingen ska säkerställa säkerheten i sina nätverk och informationssystem eller rapportera incidenter, ska bestämmelserna i den sektorspecifika unionsrättsakten tillämpas, förutsatt att verkan av kraven i fråga minst motsvarar verkan av skyldigheterna i NIS-direktivet (artikel 1.7). I skälen till direktivet anges att medlemsstaterna då bör tillämpa bestämmelserna i sådana sektorsspecifika unionsrättsakter, inklusive sådana som rör jurisdiktion, och inte genomföra identifieringsförfarandet för leverantörer av samhällsviktiga tjänster. Vid fastställandet av om kraven på säkerhet i nätverk och informationssystem och

rapportering av incidenter i sektorspecifika unionsrättsakter motsvarar kraven i NIS-direktivet, bör enligt direktivet endast bestämmelserna i relevanta unionsrättsakter och deras tillämpning i medlemsstaterna beaktas. (skäl 9)

Åtgärder för att skydda väsentliga statliga funktioner

NIS-direktivet påverkar inte medlemsstaternas åtgärder för att skydda sina väsentliga statliga funktioner. Det gäller särskilt åtgärder för att skydda den nationella säkerheten, inklusive åtgärder för skydd av information vars avslöjande medlemsstaterna anser strida mot sina väsentliga säkerhetsintressen och åtgärder för att upprätthålla lag och ordning, särskilt för att möjliggöra utredning, upptäckt och lagföring av brott. (artikel 1.6)

Övriga undantag

Bestämmelserna i NIS-direktivet ska inte tillämpas på företag som omfattas av kraven i artiklarna 13a och 13b i Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektivet), eller på betrodda tjänster som omfattas av kraven i artikel 19 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. NIS-direktivet påverkar inte heller tillämpningen av 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 eller 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. En kortare redogörelse för dessa EU-rättsakter finns i avsnitt 3.3.

Beträffande leverantörer av digitala tjänster ska NIS-direktivets bestämmelser inte tillämpas på små företag eller mikroföretag enligt definitionen i kommissionens rekommendation 2003/361/EG av

den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.

5.2 Gällande rätt

I dag finns bestämmelser om informationssäkerhet för nätverk och informationssystem i flera nationella regelverk. Det finns också sektorer som regleras av sektorspecifika EU-rättsakter (lex specialis). Sjöfartssektorn, banksektorn och sektorn för finansmarknadsinfrastruktur är t.ex. i hög grad harmoniserade på unionsnivå. Även området för elektronisk kommunikation är i hög grad reglerat på EU-nivå.

5.2.1 Lex specialis enligt NIS-direktivet

Sjöfartssektorn

I sjöfartssektorn omfattar säkerhetskraven för rederier, fartyg, hamnanläggningar, hamnar och sjötrafikinformationstjänster enligt unionsrättsakter all verksamhet, även radio- och telekommunikationssystem, datorsystem och nätverk. De obligatoriska förfarandena innefattar rapportering av alla incidenter. I NIS-direktivet anges att dessa krav bör anses utgöra lex specialis i den mån kraven är åtminstone likvärdiga med kraven i NIS-direktivet. (skäl 10)

Banksektorn och sektorn för finansmarknadsinfrastruktur

Regleringen och tillsynen inom banksektorn och sektorn för finansmarknadsinfrastruktur har i hög grad harmoniserats på unionsnivå. Harmoniseringen har skett genom användning av unionens primärrätt och sekundärrätt samt standarder som utvecklats tillsammans med de europeiska tillsynsmyndigheterna. I unionsrättsakterna utgör operativ risk en viktig del av reglering och tillsyn. Operativ risk omfattar all verksamhet, även nätverks och informationssystems säkerhet, integritet och motståndskraft. Kraven på dessa system är ofta mer långtgående än de som föreskrivs i NIS-direktivet. Krav på rapportering av incidenter utgör vidare en del av normal tillsynspraxis inom finanssektorn. Dessa bestämmelser och krav bör enligt direk-

tivet beaktas av medlemsstaterna vid tillämpningen av lex specialis. (skäl 12 och 13)

Digital infrastruktur

Inom sektorn digital infrastruktur ska bestämmelserna i NIS-direktivet tillämpas på enheten internetknutpunkter. Internetknutpunkter som flera aktörer kan ansluta sig till anses i svensk rätt som ett allmänt kommunikationsnät och omfattas av 5 kap. 6 b och c §§ lagen (2003:389) om elektronisk kommunikation (LEK). Bestämmelserna genomför artiklarna 13a och 13b i Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektivet). Artikel 13a i det direktivet ställer krav på tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster att *dels* vidta lämpliga tekniska och organisatoriska åtgärder för att på ett tillfredsställande sätt skydda säkerheten för sina nät eller tjänster, *dels* meddela den behöriga nationella regleringsmyndigheten om överträdelser av säkerheten eller integriteten som i betydande omfattning påverkade driften av nät och tjänster.

5.2.2 Nationell reglering

I svensk rätt finns i dag ett flertal regelverk som ställer krav på informationssäkerhet utifrån olika förutsättningar. I säkerhetsskyddslagstiftningen finns t.ex. bestämmelser om hantering av hemliga uppgifter och i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (krisberedskapsförordningen, KBF) ges övergripande bestämmelser om informationssäkerhet och krav på it-incidentrapportering för statliga myndigheter. I lagen (2003:389) om elektronisk kommunikation (LEK) finns bestämmelser om krav på såväl säkerhetsåtgärder som incidentrapportering.

Säkerhetsskyddslagstiftningen

I säkerhetsskyddslagen (1996:627) finns bestämmelser om säkerhetsskydd. Med säkerhetsskydd avses enligt 6 § skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet, samt skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, även om brotten inte hotar rikets säkerhet.

Av 7 § säkerhetsskyddslagen framgår att säkerhetsskyddet ska förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet (hemliga uppgifter) obehörigen röjs, ändras eller förstörs (informationssäkerhet) att obehöriga får tillträde till platser där de kan få tillgång till sådana uppgifter eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning) och att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som är av betydelse för rikets säkerhet (säkerhetsprövning). Säkerhetsskyddet ska även i övrigt förebygga terrorism.

Vid utformningen av informationssäkerhet ska enligt säkerhetsskyddslagen behovet av skydd vid automatisk informationsbehandling beaktas särskilt (9 §).

Det saknas definition av begreppet rikets säkerhet i säkerhetsskyddslagen. I stället ska myndigheter och andra som omfattas av säkerhetsskyddsförordningen (1996:633) undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet ska dokumenteras i en säkerhetsanalys. (5 § säkerhetsskyddsförordningen)

Syftet med säkerhetsskyddslagen är framför allt att säkerhetsälla ett skydd för verksamheter där påverkan genom ett antagonistiskt angrepp skulle medföra allvarliga konsekvenser på nationell nivå.

En särskild utredare har haft i uppdrag att göra en översyn av säkerhetsskyddslagstiftningen och överlämnade betänkandet *En ny säkerhetsskyddslag* (SOU 2015:25) i mars 2015. Betänkandet har remissbehandlats och bereds för närvarande i Regeringskansliet. I betänkandet lämnas bl.a. förslag på en ny säkerhetsskyddslag. Lagen ska enligt förslaget tillämpas på verksamheter hos staten, kommuner, landsting och enskilda som är av betydelse för Sveriges säkerhet, eller

som omfattas av ett för Sverige i förhållande till annan stat eller mellanfolklig organisation förpliktande åtagande om säkerhetsskydd. Sådan verksamhet definieras enligt förslaget som säkerhetskänslig verksamhet. I betänkandet konstateras att de samhällssektorer som lyfts fram i Myndigheten för samhällsskydd och beredskaps (MSB) vägledning för identifiering av samhällsviktig verksamhet och konsekvensbedömning[1] även är relevanta för att identifiera särskilt skyddsvärd verksamhet, men att områdena inte är identiska. Som exempel på områden, verksamheter och funktioner som är av sådan karaktär att de skulle kunna omfattas av krav på skydd enligt säkerhetsskyddslagen anges i betänkandet följande: [2]

- Centrala statsledningen
- Totalförsvaret
- Internationella relationer
- Rättsväsendet
- Skydd mot olyckor
- Hälso- och sjukvård
- Energiförsörjning
- Vattenförsörjning och avloppshantering
- Annan livsmedelsförsörjning
- Elektronisk kommunikation
- Finansiella tjänster
- Industri, forskning och utveckling
- Transporter och kommunikation
- Folkbokföring och socialförsäkring

[1] Myndigheten för samhällsskydd och beredskaps publikation Att identifiera samhällsviktig verksamhet – En metod för identifiering av samhällsviktig verksamhet och bedömning av tolerabel avbrottstid, publ.nr. MSB620, januari 2014.
[2] En ny säkerhetsskyddslag (SOU 2015:25) s. 294 f.

Gemensamt för flera av dessa områden är att det inom dem finns skyddsvärda it-system för bl.a. ledning, styrning, reglering och övervakning av samhällsviktiga funktioner.

I säkerhetskyddsförordningen ges bestämmelser till säkerhetsskyddslagen utom när det gäller riksdagen och dess myndigheter. Om en hemlig uppgift kan ha röjts ska detta skyndsamt anmälas till Säkerhetspolisen, om röjandet kan antas medföra men för rikets säkerhet som inte endast är ringa (10 §). En myndighet ska också enligt 10 a §, till den myndighet som utövar tillsyn över säkerhetsskyddet, skyndsamt anmäla om det inträffat en it-incident i myndighetens informationssystem och

1. incidenten allvarligt kan påverka säkerheten i ett informationssystem där hemliga uppgifter behandlas i en omfattning som inte är ringa,
2. incidenten allvarligt kan påverka säkerheten i ett informationssystem som särskilt behöver skyddas mot terrorism, eller
3. incidenten upptäckts genom stöd enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt.

Försvarsmakten är tillsynsmyndighet när det gäller Fortifikationsverket, Försvarshögskolan och de myndigheter som hör till Försvarsdepartementet. Säkerhetspolisen är tillsynsmyndighet när det gäller övriga myndigheter utom Justitiekanslern. Om incidenten ska rapporteras till Försvarsmakten, ska den rapporterande myndigheten också skyndsamt informera Säkerhetspolisen. (10 a § och 39 § säkerhetsskyddsförordningen)

Säkerhetsskyddslagstiftningen skyddar alltså den nationella säkerheten. Den verksamhet som regleras där omfattas därmed inte av NIS-direktivet. Den rapportering av it-incidenter som myndigheter är skyldiga att göra enligt 10 a § säkerhetsskyddsförordningen ska med hänsyn till rikets säkerhet inte omfattas av ett nationellt regelverk till följd av NIS-direktivet. Sådana incidenter ska dock även fortsättningsvis rapporteras enligt säkerhetsskyddsförordningen.

Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

Krisberedskapsförordningen syftar till att statliga myndigheter genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och inför och vid höjd beredskap. I krisberedskapsförordningen finns bl.a. övergripande bestämmelser om informationssäkerhet för statliga myndigheter. Enligt 19 § ansvarar varje myndighet för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Därvid ska behovet av säkra ledningssystem särskilt beaktas. Till stöd för arbetet med samhällets informationssäkerhet ska en myndighet vidare enligt 20 § till Myndigheten för samhällsskydd och beredskap (MSB) skyndsamt rapportera it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. En myndighet som tillhandahåller tjänster åt en annan organisation ska i samband med rapportering informera och vid behov samråda med den eller de uppdragsgivare som berörs av incidenten. Rapporteringsskyldigheten omfattar inte sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen. Bestämmelsen i 20 § gäller för statliga myndigheter under regeringen med undantag av Regeringskansliet, kommittéväsendet, Säkerhetspolisen, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut (3 §).

MSB får meddela föreskrifter om sådana säkerhetskrav som avses i 19 § med beaktande av nationell och internationell standard. MSB får också, efter att ha gett Polismyndigheten, Säkerhetspolisen och Försvarsmakten tillfälle att yttra sig, meddela de ytterligare föreskrifter som behövs för verkställigheten av rapportering av it-incidenter. (21 §)

Vissa av de statliga myndigheter som omfattas av förordningen kan komma att omfattas även av bestämmelserna i NIS-direktivet. Som utredningen konstaterar i avsnitt 7.3.2 innebär detta att myndigheter kan bli skyldiga att rapportera incidenter enligt flera regelverk.

Lagen (2003:389) om elektronisk kommunikation

Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst är enligt lagen (2003:389) om elektronisk kommunikation (LEK) skyldig att vidta tekniska och organisatoriska åtgärder för att skydda uppgifter som behandlas i samband med tillhandahållande av tjänsten. Vilken säkerhetsnivå som ska uppnås beror på risken för en integritetsincident, tillgänglig teknik och kostnaderna för att genomföra åtgärderna. Sådana aktörer är också skyldiga att utan onödigt dröjsmål underrätta Post- och telestyrelsen (PTS) om integritetsincidenter. Med integritetsincident avses en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring, eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster. Om incidenten kan antas inverka negativt på de abonnenter eller användare som de behandlade uppgifterna berör, eller om tillsynsmyndigheten begär det, ska även dessa underrättas utan onödigt dröjsmål. (6 kap. 1 och 3–4 a §§) PTS har utfärdat föreskrifter som innehåller mer detaljerade krav på säkerhetsåtgärder (PTSFS 2014:1).

Den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster är skyldig dels att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet, dels att utan onödigt dröjsmål rapportera störningar eller avbrott av betydande omfattning till PTS (5 kap. 6 b–c §§). Av Post- och telestyrelsens föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning (PTSFS 2012:2) framgår på vilket sätt rapporteringsskyldigheten ska fullgöras och om undantag från skyldigheten. Genom bestämmelserna i 5 kap. 6 b–c §§ genomförs, som framgått ovan, artiklarna 13a och 13b i Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektivet). Säkerhets- och rapporteringskraven i NIS-direktivet ska enligt artikel 1.3 inte tillämpas på företag som omfattas av de nu nämnda artiklarna.

Informationssäkerhet för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster enligt NIS-direktivet

Av den övergripande inventering som utredningen har gjort med hjälp av bl.a. deltagarna i referensgruppen framgår att det endast i begränsad omfattning finns bestämmelser som direkt gäller informationssäkerhet för leverantörer av samhällsviktiga tjänster och digitala tjänster enligt NIS-direktivet.[3] I vissa fall finns dock krav på säkerhet som skulle kunna omfatta även informationssäkerhet. Som exempel kan nämnas mer allmänt formulerade bestämmelser om riskhantering eller bestämmelser med krav på driftsäkerhet eller kontinuitet i den tillhandahållna tjänsten.

5.3 En ny lag och en ny förordning införs

Förslag: Genomförandet av NIS-direktivet ska ske i en ny lag och en ny förordning. Den nya lagen och den nya förordningen ska heta

- lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster, respektive
- förordningen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster

Normgivning

I regeringsformen (RF) används beteckningen föreskrifter för rättsregler som styr enskildas och myndigheters handlande. Föreskrifter beslutas av riksdagen genom lag och av regeringen genom förordning. Även förvaltningsmyndigheter och kommuner meddelar föreskrifter. Förvaltningsmyndigheters föreskrifter brukar benämnas myndighetsföreskrifter.

Föreskrifter som avser förhållandet mellan enskilda och det allmänna och som gäller skyldigheter för enskilda eller i övrigt avser

[3] Inventeringen finns tillgänglig i ärende dnr Komm2017/00542-1.

ingrepp i enskildas personliga eller ekonomiska förhållanden ska som huvudregel meddelas i lag. Detsamma gäller i fråga om föreskrifter som avser t.ex. befogenheter och åligganden för kommuner. Efter bemyndigande i lag kan dock sådana föreskrifter i många fall meddelas av regeringen i förordning eller, efter vidaredelegation, av en förvaltningsmyndighet eller en kommun. (8 kap. 3 och 9 §§ RF)

Utöver de fall då riksdagen i lag kan delegera föreskriftsrätt, finns det direkt stöd i regeringsformen för regeringen att meddela föreskrifter på vissa områden. Regeringen får bl.a. meddela föreskrifter om verkställighet av lag (8 kap. 7 § första stycket 1 RF). Sådana bestämmelser kan fylla ut eller precisera lagbestämmelser. Exempel på verkställighetsföreskrifter är sådana som styr när och hur man ansöker om ett tillstånd som krävs enligt lag för att bedriva en viss verksamhet. En förutsättning för att verkställighetsföreskrifter ska kunna meddelas är att de inte tillför något väsentligt nytt i sak. Verkställighetsföreskrifter får t.ex. inte innebära att enskilda åläggs ytterligare skyldigheter. Verkställighetsföreskrifter får inte heller förändra innehållet i lagbestämmelsen. Däremot kan de tillföra vad som behövs för att lagen ska kunna tillämpas i praktiken.

Regeringen får även meddela sådana föreskrifter som inte enligt grundlag ska meddelas av riksdagen (8 kap. 7 § första stycket 2 RF). Denna föreskriftsrätt brukar kallas för regeringens restkompetens. Med stöd av restkompetensen kan regeringen meddela föreskrifter om t.ex. statliga förvaltningsmyndigheters organisation och arbetsuppgifter. Även gynnande föreskrifter, som visserligen avser förhållandet mellan enskilda och det allmänna men som inte gäller skyldigheter eller ingrepp, faller in under restkompetensen. Sådana föreskrifter kan alltså meddelas av regeringen utan något stöd av bemyndigande i lag.

NIS-direktivet innebär skyldigheter för både enskilda och offentliga aktörer. Ett genomförande av direktivet ska därmed ske huvudsakligen i lag. Direktivet innebär emellertid också att myndigheter bör åläggas arbetsuppgifter. I vissa delar är det vidare lämpligt att möjliggöra för myndigheter att meddela närmare föreskrifter om hur skyldigheterna i direktivet ska uppfyllas. Sådana bestämmelser bör meddelas i förordning.

Ett samlat regelverk

I kommittédirektiven anges att det i linje med regeringens ambition att verka för ett mer ändamålsenligt arbete med informationssäkerhet inom statsförvaltningen bör utredas ifall NIS-direktivet bör genomföras i ett samlat regelverk om säkerhet för nätverk och informationssystem. Det gäller särskilt kraven på operatörer som bedriver samhällsviktig verksamhet och leverantörer av digitala tjänster.

Fördelarna med ett samlat regelverk är enligt utredningens mening att det blir tydligt för myndigheter, enskilda och tillsynsmyndigheten vilken reglering som finns när det gäller samhällsviktiga tjänster och digitala tjänster. NIS-direktivet reglerar en miniminivå vilket lämpar sig väl för en övergripande ramlagstiftning. Bestämmelser som behöver anpassas till respektive sektor kan då regleras i myndighetsföreskrifter. Regleringen blir heltäckande och ingen tjänst riskerar att sakna reglering. Det blir också lättare att komplettera och ändra regelverket om ett sådant behov uppkommer. I NIS-direktivet betonas också vikten av att ta tillvara erfarenheter av tillämpningen från till exempel samordningsgruppen och CSIRT-nätverket.

Nackdelarna med ett samlat regelverk är att myndigheter och enskilda i vissa fall kommer att behöva tillämpa olika regelverk för samma nätverk och informationssystem men med olika syften. För myndigheter och enskilda inom sektorer som omfattas även av andra EU-rättsakter finns också en risk för att det kan bli otydligt vilken reglering som gäller. I vissa EU-rättsakter på till exempel transportområdet är avsikten att bestämmelser om säkerhet ska omfatta hela verksamheten, dvs. även nätverk och informationssystem.

Den inventering som utredningen har gjort av de nationella reglerna på området visar att det inom vissa sektorer finns ett mer utvecklat regelverk för informationssäkerhet än inom andra.[4] Det finns också skillnader mellan olika enheter inom samma sektor. Vissa bestämmelser tar inte heller direkt sikte på informationssäkerhet utan syftar till att upprätthålla kontinuiteten i tjänsten utifrån andra aspekter eller till att analysera eller hantera risker mer allmänt. I de fall tillhandahållandet av en tjänst är beroende av nätverk eller informationssystem kan dessa system utgöra en sådan risk som bör beaktas när tillhandahållaren av tjänsten gör sin riskanalys, oavsett

[4] Inventeringen finns tillgänglig i ärende dnr Komm2017/00542-1.

om bestämmelsen är formulerad som en informationssäkerhetsbestämmelse eller inte. Beträffande de digitala tjänster som regleras av NIS-direktivet saknas i dag reglering helt.

Att införa kompletterande bestämmelser i befintliga regelverk för samtliga de sektorer och enheter som NIS-direktivet omfattar skulle innebära ett omfattande kartläggningsarbete av ett stort antal bestämmelser, både nationella och i EU-rättsakter. En sådan reglering riskerar också att bli oöverskådlig och rörig, vilket är till nackdel inte minst för tillsynsmyndigheten.

Inom sektorn digital infrastruktur ska NIS-direktivet tillämpas på en relativt begränsad krets av enheter som är förhållandevis lätta att identifiera. Den svenska lagstiftningen på området är begränsad till två lagar, nämligen lagen (2003:389) om elektronisk kommunikation och lagen (2006:24) om nationella toppdomäner för Sverige på Internet. Utredningen har övervägt att särskilt beträffande registreringsenheter för toppdomäner genomföra NIS-direktivet genom att föra in nya och kompletterade bestämmelser i befintligt regelverk. Utredningen har dock kommit till slutsatsen att detta inte är lämpligt. En sådan lösning skulle bli onödigt komplicerad.

Vid genomförandet av NIS-direktivet bör man enligt utredningens mening sträva efter att åstadkomma en samlad lagstiftningsprodukt som till sin struktur ligger nära direktivet. Detta kommer att underlätta tillämpningen inte minst mot bakgrund av att myndigheter och enskilda kan komma att omfattas av NIS-direktivet i flera medlemsstater.

5.4 Den nya lagens tillämpningsområde

Förslag: Lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster ska tillämpas på

- leverantörer av samhällsviktiga tjänster som är etablerade på svenskt territorium. Med leverantörer av samhällsviktiga tjänster avses en enhet av den typ som anges i bilaga 2 till NIS-direktivet och som tillhandhåller en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, tillhandhållandet av tjänsten är beroende av nätverks och in-

formationssystem och en incident skulle medföra en betydande störning av tillhandahållandet av tjänsten.

- leverantörer av sådana digitala tjänster som anges i bilaga 3 till NIS-direktivet och som har sitt huvudsakliga etableringsställe i Sverige eller har utsett en företrädare som är etablerad här, dock inte mikroföretag eller små företag enligt definitionen i kommissionens rekommendation 2003/361/EG.

Lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster ska inte tillämpas på

- företag som omfattas av kraven i artiklarna 13a och 13b i direktiv 2002/21/EG, utom företag som tillhandahåller internetknutpunkter
- leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 i förordning (EU) nr 910/2014
- leverantörer som omfattas av lex specialis enligt NIS-direktivet
- verksamhet som är av betydelse för Sveriges säkerhet

Om det finns bestämmelser i bindande EU-rättsakter om krav på att leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster ska säkerställa säkerheten i sina nätverk och informationssystem eller rapportera incidenter så ska den nya lagen inte tillämpas förutsatt att verkan av kraven minst motsvarar verkan av skyldigheterna i den nya lagen. Finns sådana bestämmelser i annan författning ska de bestämmelserna tillämpas om kraven minst motsvarar verkan av skyldigheterna i den nya lagen.

Bedömning: Lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster ska tillämpas endast på sådana leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster som omfattas av NIS-direktivet.

Den nya lagen ska tillämpas endast på de leverantörer som omfattas av NIS-direktivet

NIS-direktivet reglerar säkerheten i nätverk och informationssystem hos leverantörer av samhällsviktiga tjänster inom särskilt utpekade sektorer. Endast vissa typer av operatörer (enheter) inom sektorerna omfattas.

Utredningen kan konstatera att det i Sverige tillhandahålls samhällsviktiga tjänster även av operatörer som inte utgör enheter enligt NIS-direktivet. Ett sådant exempel är fjärrvärme. Vidare kan en leverantör av samhällsviktiga tjänster som omfattas av direktivet vara direkt eller indirekt beroende av tjänster och system som inte omfattas.

Enligt utredningens mening kan det finnas behov av tydligare kravställning rörande informationssäkerhet även för verksamhet som inte omfattas av NIS-direktivet. Ett sådant behov skulle kunna tillgodoses genom att den nya lagen utformas som en plattform och knutpunkt för samhällets informationssäkerhetsarbete i sin helhet. En mer övergripande lag skulle kunna vara till fördel för enhetligheten på området, ge mindre utrymme för olika tolkningar och bättre förutsättningar för aktörerna att överblicka regelverket. En sådan lösning skulle också ligga i linje med de rekommendationer Riksrevisionens lämnat i sin rapport *Informationssäkerheten i den civila statsförvaltningen* (RiR 2014:23).

Utredarens uppdrag är bl.a. att föreslå hur NIS-direktivet ska genomföras i svensk rätt. I detta ryms inte att ta ställning till hur hela samhällets informationssäkerhet bör regleras i ett bredare perspektiv. Mot bakgrund av att NIS-direktivet syftar till att reglera samhällsviktiga tjänster ligger det i så fall närmare till hands att föreslå ett regelverk som omfattar även sådana leverantörer av samhällsviktiga tjänster som i och för sig inte utgör enheter enligt direktivet. Med hänsyn till den tidsram utredningen har att beakta bedömer utredningen emellertid inte att det är möjligt att föra fram ett sådant förslag. Utredningen har därför stannat vid att låta den nya lagen omfatta endast sådana leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster som omfattas av NIS-direktivet.

Jurisdiktion

Den nya lagen ska tillämpas på leverantörer av samhällsviktiga tjänster som är etablerade på svenskt territorium (artikel 5.1) och på leverantörer av sådana digitala tjänster som anges i bilaga 3 till NIS-direktivet och som har sitt huvudsakliga etableringsställe i Sverige eller har utsett en företrädare som är etablerad här, se avsnitt 10.2.5.

Uttryckliga undantag m.m.

Som framgått ovan är vissa företag och leverantörer uttryckligen undantagna från NIS-direktivets tillämpningsområde. I den nya lagen bör det anges att lagen inte är tillämplig på dessa aktörer.

Beträffande direktiv 2002/21/EG konstaterar utredningen dock att i svensk rätt anses internetknutpunkter som sådana allmänna kommunikationsnät som omfattas av 5 kap. 6 b och c §§ LEK. Dessa bestämmelser genomför artiklarna 13a och 13b i direktiv 2002/21/EG. Med hänsyn till att internetknutpunkter är en av de enheter som uttryckligen ska regleras enligt NIS-direktivet bedömer utredningen att undantaget för företag som omfattas av artiklarna 13a och 13b inte kan gälla internetknutpunkter. Det gäller oavsett om internetknutpunkter även enligt EU-rätten ska anses som ett allmänt kommunikationsnät eller inte. För att NIS-direktivet ska bli korrekt genomfört i svensk rätt bedömer utredningen att internetknutpunkter måste omfattas av den nya lagen. De kan inte undantas mot bakgrund av att de anses omfattas av den nationella lagstiftningen – oavsett om denna grundar sig på en EU-rättsakt. En annan sak är att internetknutpunkter kan anses omfattas av lex specialis enligt NIS-direktivet, se nedan.

Det bör också anges att lagen inte ska tillämpas på verksamhet som är av betydelse för Sveriges säkerhet. Lagen ska alltså inte tillämpas på sådan verksamhet som omfattas av säkerhetsskyddslagen. Den rapportering av it-incidenter som myndigheter är skyldiga att göra enligt 10 a § säkerhetsskyddsförordningen ska därmed även fortsättningsvis rapporteras enligt säkerhetsskyddsförordningen och inte enligt den nya lagen.

Med verksamhet avses verksamhet inom de typer av enheter som anges i bilaga 2 och 3 till NIS-direktivet. Under utredningens arbete har det framförts att incidenter som upptäcks genom stöd som läm-

nas enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt uttryckligen bör undantas från rapporteringsplikten enligt den nya lagen även om verksamheten till vilken stöd lämnas inte omfattas av säkerhetsskyddslagstiftningen. Utredningen bedömer dock att i den utsträckning stödet enligt FRA:s instruktion innebär att verksamheten får del av uppgifter som omfattas av försvarssekretess, får verksamheten betydelse för Sveriges säkerhet. Den nya lagen ska då inte tillämpas. En sådan tillämpning torde strida mot NIS-direktivets syfte, men inte mot dess lydelse. Tolkningen innebär också att den myndighet som får stöd av eller anlitar FRA ska vidta säkerhetsskyddsåtgärder enligt säkerhetsskyddslagen. Denna fråga gäller ytterst omfattningen och tillämpningen av säkerhetsskyddslagen och bör därför i första hand behandlas i ett annat sammanhang. När det gäller enskilda aktörer kan det nämnas att det i betänkandet *En ny säkerhetsskyddslag* (SOU 2015:25) föreslås att säkerhetsskyddslagen ska omfatta även sådana aktörer.

Att det inom en viss samhällssektor finns intressen som kräver skydd enligt säkerhetsskyddslagen innebär emellertid inte att all verksamhet inom sektorn ska betraktas som så skyddsvärd att den träffas av säkerhetsskyddslagstiftningen. Verksamhet som inte omfattas av säkerhetsskyddslagen kan vara skyddsvärd utifrån andra perspektiv och omfattas av andra krav på skyddsåtgärder, t.ex. enligt NIS-direktivet. Ytterligare annan verksamhet kan vara sådan att det helt saknas behov av särskilt skydd. I skälen till NIS-direktivet anges som exempel flygplatser som tillhandahåller samhällsviktiga tjänster såsom skötsel av start- och landningsbanor, men också tjänster som inte kan betraktas som samhällsviktiga, t.ex. tillhandahållande av butiksområden (skäl 22). Vilket behov av skyddsåtgärder som finns för en verksamhet får bedömas med hjälp av de avvägningar som sker inom ramen för säkerhetsanalys enligt säkerhetsskyddslagstiftningen eller enligt den riskanalys som utredningen föreslår att de leverantörer som omfattas av NIS-direktivet ska göra (se avsnitt 7.3.1).

I den nya lagen bör också anges att lagen inte ska tillämpas på små företag eller mikroföretag enligt definitionen i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.

Den nya lagen ska inte tillämpas på leverantörer som omfattas av lex specialis enligt NIS-direktivet

Som framgått ovan ska bestämmelser i en unionsrättsakt om krav på säkerhetsåtgärder eller incidentrapportering tillämpas i stället för bestämmelserna i NIS-direktivet, förutsatt att verkan av kraven minst motsvarar verkan av skyldigheterna enligt NIS-direktivet. Detta innebär enligt utredningens mening att leverantörer som är skyldiga att vidta säkerhetsåtgärder och att incidentrapportera inte bör omfattas av en nationell reglering till följd av NIS-direktivet om skyldigheterna grundas på bestämmelser i unionsrättsakter. Sådana bestämmelser finns som nämnts inom t.ex. sjöfartssektorn, banksektorn, sektorn för finansmarknadsinfrastruktur och sektorn för digital infrastruktur. Om de angivna kraven på dessa leverantörer motsvarar skyldigheterna enligt NIS-direktivet ska den nya lagen alltså inte tillämpas på leverantörerna. Det innebär t.ex. att identifieringsförfarandet för leverantörer av samhällsviktiga tjänster inte ska genomföras. Någon tillsyn av leverantörerna ska heller inte att utövas enligt den nya lagen. Inte heller ska incidentrapporteringen ske på det sätt som anges där.

Den nya lagens bestämmelser om krav på leverantörerna ska inte tillämpas om det i annan lag finns bestämmelser som minst motsvarar bestämmelserna i den nya lagen

För att ett direktiv ska anses korrekt genomfört krävs att det finns bestämmelser i nationell rätt som motsvarar direktivet. Finns redan sådana bestämmelser behöver några nya inte införas.

I svensk nationell rätt finns som nämnts endast i begränsad omfattning bestämmelser som motsvarar bestämmelserna i NIS-direktivet. En stor del av den reglering som finns utgörs av myndighetsföreskrifter angående informationssäkerhet. Ofta är bakgrunden till och syftet med bestämmelserna något annorlunda än vad som gäller för NIS-direktivet. Tillsynen är inte heller ordnad på ett sådant sätt att NIS-direktivets bestämmelser uppfylls. Inom de flesta sektorer saknas också möjligheter att vidta tillräckliga sanktioner mot den som inte följer regelverket.

Utredningen har bedömt att NIS-direktivet så långt som möjligt bör genomföras i en ny och samlad lag. I den utsträckning det finns

bestämmelser om krav på leverantörerna i annan lag som minst motsvarar bestämmelserna i den nya lagen bör emellertid de bestämmelserna kunna tillämpas. För att NIS-direktivet ska anses korrekt genomfört krävs dock att den nya lagens bestämmelser tillämpas i den utsträckning det saknas andra bestämmelser. Skulle det t.ex. finnas bestämmelser om krav på tekniska och organisatoriska åtgärder i en särskild lag, men saknas bestämmelser om t.ex. incidentrapportering, tillsyn eller sanktioner, bör den nya lagen tillämpas i dessa delar. Här finns alltså en skillnad gentemot vad som gäller för de leverantörer som omfattas av sådan reglering som i direktivet betecknas som lex specialis. För sådana leverantörer gäller som nämnts att den nya lagen inte ska tillämpas alls om de omfattas av krav på säkerhetsåtgärder eller incidentrapportering enligt någon annan EU-rättsakt och de kraven minst motsvarar verkan av skyldigheterna enligt NIS-direktivet.

5.5 Den nya förordningen

För genomförandet av NIS-direktivet i svensk rätt krävs att olika myndigheter åläggs vissa arbetsuppgifter. Utredningen bedömer också att det är lämpligt att ett antal myndigheter bemyndigas att meddela föreskrifter. I vilken utsträckning sådana bestämmelser ska tas in i lag respektive förordning behandlas löpande genom betänkandet.

6 Leverantörer av samhällsviktiga tjänster

6.1 Inledning

Enligt NIS-direktivet ska medlemsstaterna identifiera de offentliga och enskilda leverantörer som tillhandahåller samhällsviktiga tjänster inom ett antal särskilt utpekade enheter som finns inom sju olika sektorer, se kapitel 4.

För att omfattas av direktivets krav måste leverantören av den samhällsviktiga tjänsten vara etablerad i medlemsstaten (artikel 5.1). Med detta avses att leverantören måste bedriva en faktisk och reell verksamhet med hjälp av en stabil struktur i medlemsstaten (skäl 21). Den rättsliga formen för verksamheten är inte en avgörande faktorn.

6.2 Identifiering av leverantörer av samhällsviktiga tjänster

Vid förfarandet för identifiering av leverantörer av samhällsviktiga tjänster ska det

1. upprättas en förteckning över vilka tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet (samhällsviktiga tjänster),
2. bedömas om de enheter som anges inom respektive sektorer och delsektorer uppfyller kriterierna nedan,
   - tillhandahåller en samhällsviktig tjänst,
   - tillhandahållandet är beroende av nätverk och informationssystem samt

– en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten(artikel 5.2).

6.2.1 Förteckning över samhällsviktiga tjänster

Förslag: Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om vilka tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet (samhällsviktiga tjänster) för varje sektor som anges i bilaga 2 till NIS-direktivet (förteckning). Föreskriften ska uppdateras minst vartannat år.

Tillsynsmyndigheterna ska ges tillfälle att yttra sig innan föreskrifter meddelas.

Det första steget för att identifiera leverantörer av samhällsviktiga tjänster är att bedöma vilka tjänster som tillhandahålls av enheterna i bilaga 2 till NIS-direktivet som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, dvs. vad som utgör samhällsviktiga tjänster.

Varje medlemsstat ska upprätta en förteckning över dessa samhällsviktiga tjänster (artikel 5.3). Förteckningen ska ses över regelbundet och minst vartannat år samt uppdateras vid behov (artikel 5.5). Förteckningen över samhällsviktiga tjänster bör omfatta alla sådana tjänster som tillhandahålls på en viss medlemsstats territorium och som uppfyller kraven enligt NIS-direktivet. Medlemsstaterna bör kunna lägga till nya tjänster i den befintliga förteckningen. Förteckningen över samhällsviktiga tjänster bör fungera som referenspunkt för medlemsstaterna och möjliggöra identifiering av leverantörer av samhällsviktiga tjänster (skäl 23).

Syftet med förteckningen är att hitta de typer av samhällsviktiga tjänster som kan finnas inom en viss sektor och därmed skilja dem från övriga tjänster som sektorn tillhandahåller. Den förteckning över samhällsviktiga tjänster som varje medlemsstat upprättar utgör också ett bidrag till bedömningen av lagstiftningspraxis inom varje medlemsstat med syftet att säkerställa en övergripande enhetlighet mellan medlemsstaternas bedömning av samhällsviktiga tjänster (skäl 23).

Kravet på att upprätta en förteckning medför att begreppet samhällsviktig tjänst måste förklaras. Det måste också finnas en utpekad myndighet, med sådan kunskap om verksamheten i de olika sektorerna, att myndigheten kan bedöma vilka samhällsviktiga tjänster som tillhandahålls av såväl offentliga som enskilda aktörer.

Vad är en samhällsviktig tjänst?

Tjänster som omfattas av NIS-direktivet finns inom följande sektorer och delsektorer.

- Energi (elektricitet, olja, gas)
- Transporter (lufttransporter, järnvägstransporter, sjöfart, vägtransport)
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvård (hälso- och sjukvårdsmiljöer [inklusive sjukhus och privata kliniker])
- Leverans och distribution av dricksvatten
- Digital infrastruktur

Sektorerna och enheterna beskrivs närmare i kapitel 4 och i ärende dnr Komm2017/00542-1.

Begreppet samhällsviktiga tjänster förekommer inte i svensk lagstiftning eller föreskrifter. I stället används andra närliggande begrepp som kritisk europeisk infrastruktur och samhällsviktig verksamhet. Det förstnämnda definieras i artikel 2 a i ECI-direktivet[1]. Det senare återfinns i Myndighetens för samhällsskydd och beredskaps (MSB) föreskrifter om risk- och sårbarhetsanalyser, se nedan.

[1] 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.

Samhällsviktig verksamhet

Begreppet samhällsviktig verksamhet används bland annat i risk- och sårbarhetsanalysarbetet, vilket är en viktig del i krisberedskapsarbetet och som syftar till att minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och inför och vid höjd beredskap.

Begreppet definieras i MSB:s föreskrifter och allmänna råd[2] om risk- och sårbarhetsanalyser som en verksamhet som uppfyller minst ett av följande villkor:

- Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället.
- Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

I de allmänna råden till ovan nämnda föreskrifter beskrivs samhällsviktig verksamhet enligt följande.

> Med samhällsviktig verksamhet menas de verksamheter, anläggningar, noder, infrastrukturer och tjänster som upprätthåller den funktion som de ingår i och är verksamhet som är av avgörande betydelse för upprätthållandet av viktiga samhällsfunktioner. Endast verksamhet som absolut behövs för upprätthållandet av viktiga samhällsfunktioner vid allvarliga händelser eller kriser bör identifieras som samhällsviktig.
>
> Samhällsviktig verksamhet kan vara av nationell, regional eller lokal betydelse.
>
> Med samhällssektor avses i detta sammanhang de olika områden inom vilka viktiga samhällsfunktioner finns och samhällsviktig verksamhet kan identifieras.
>
> *Viktig samhällsfunktion* är ett samlingsbegrepp för de verksamheter som upprätthåller en viss funktionalitet. Varje sådan funktion ingår i en eller flera samhällssektorer och upprätthålls av en eller flera samhällsviktiga verksamheter.
>
> Exempel på viktiga samhällsfunktioner per samhällssektor.

[2] MSBFS 2015:5, MSBFS 2015:4, MSBFS 2016:7.

Energiförsörjning:

Produktion av el, distribution av el, produktion och distribution av fjärrvärme, produktion och distribution av bränslen och drivmedel.

Finansiella tjänster

Betalningar, tillgång till kontanter, centrala betalningssystemet, värdepappershandel.

Handel och industri

Bygg- och entreprenadverksamhet, detaljhandel, tillverkningsindustri.

Hälso- och sjukvård samt omsorg

Akutsjukvård, läkemedels- och materielförsörjning, omsorg om barn, funktionshindrade och äldre, primärvård, psykiatri, socialtjänst, smittskydd för djur och människor.

Information och kommunikation

Telefoni (mobil och fast), internet, radiokommunikation, distribution av post, produktion och distribution av dagstidningar, webbaserad information, sociala medier.

Kommunalteknisk försörjning

Dricksvattenförsörjning, avloppshantering, renhållning, väghållning.

Livsmedel

Distribution av livsmedel, primärproduktion av livsmedel, kontroll av livsmedel, tillverkning av livsmedel.

Offentlig förvaltning

Lokal ledning, regional ledning, nationell ledning, begravningsverksamhet, diplomatisk och konsulär verksamhet.

Skydd och säkerhet

Domstolsväsendet, åklagarverksamhet, militärt försvar, kriminalvård, kustbevakning, polis, räddningstjänst, alarmeringstjänst, tullkontroll, gränsskydd och immigrationskontroll, bevaknings- och säkerhetsverksamhet.

Socialförsäkringar

Allmänna pensionssystemet, sjuk- och arbetslöshetsförsäkringen.

Transporter

Flygtransport, järnvägstransport, sjötransport, vägtransport, kollektivtrafik.

Enligt 10 och 15 §§ förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (KBF) ska myndigheternas planering för krisberedskap och höjd beredskap bedrivas i sex samverkansområden när det gäller ansvar för krisberedskap och bevakningsansvar avseende åtgärder inför och vid höjd beredskap. Dessa områden är

- Teknisk infrastruktur
- Transporter
- Farliga ämnen
- Ekonomisk säkerhet
- Geografiskt områdesansvar
- Skydd, undsättning och vård

I bilagan till KBF anges ett antal utpekade myndigheter som har särskilda uppgifter inom samverkansområdena.

Europeisk kritisk infrastruktur

Det internationella perspektivet är en viktig del i arbetet med skydd av samhällsviktig verksamhet. På EU-nivå bedrivs arbetet framför allt inom ramen för det europeiska programmet för skydd av kritisk infrastruktur (EPCIP).

Målet med arbetet inom EPCIP är att förbättra skyddet av kritisk infrastruktur inom EU. Terrorismhotet är en högt prioriterad fråga, men arbetet ska omfatta alla slags hot och risker. En av de viktigaste delarna i programmet är ett EU-direktiv från 2008 (ECI-direktivet[3]) som reglerar arbetet inom området. Med kritisk infrastruktur avses anläggningar, system eller delar av dessa som är nödvändiga för att upprätthålla centrala samhällsfunktioner, hälsa, säkerhet, trygghet

[3] Rådets direktiv 2008/114/EG om identifiering av, och klassificering som europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna.

och människors ekonomiska eller sociala välfärd (artikel 2 a). Direktivet omfattar energi- och transportsektorerna (artikel 3), och går huvudsakligen ut på att EU:s medlemsstater ska identifiera och utse europeisk kritisk infrastruktur, ECI.

MSB är utpekad nationell kontaktpunkt för arbetet med EPCIP-frågorna i Sverige. Affärsverket svenska kraftnät och Statens energimyndighet identifierar och redovisar eventuell kritisk infrastruktur till MSB. Den nationella kontaktpunkten, MSB, ska samordna frågor kring skydd av kritisk infrastruktur i Sverige med andra medlemsstater och med EU-kommissionen.

Sverige har hittills inte pekat ut någon europeisk kritisk infrastruktur på sitt territorium.

Risk- och sårbarhetsanalyser

Myndigheter, kommuner och landsting har en skyldighet att genomföra risk- och sårbarhetsanalyser[4] i vilka bland annat samhällsviktig verksamhet och kritiska beroenden ska identifieras. Vidare ska bedömas vilka konsekvenser ett bortfall eller en allvarlig störning i verksamheten kan få. Statliga myndigheter, kommuner och landsting ska genomföra risk- och sårbarhetsanalyser inom sina respektive områden. Länsstyrelsen har därutöver ansvar för att identifiera samhällsviktig verksamhet inom länet som är av regional betydelse.

Myndigheter med särskilt ansvar för krisberedskap (10 § KBF) och myndigheter som MSB beslutar om i enskilda fall ska vartannat år lämna en sammafattande redovisning av analysen till Regeringskansliet och MSB. Landstingen rapporterar vart fjärde år till Socialstyrelsen, MSB och till länsstyrelsen. Kommuner rapporterar vart fjärde år till länsstyrelsen.

Liknande krav på analyser finns också inom vissa områden t.ex. ellagen (1997:857) för elnätsföretag, lagen (2003:778) om skydd mot olyckor när det gäller farlig verksamhet och i elberedskapslagen (1997:288) för företag som producerar el, distribuerar el eller handlar med el. Dessa krav gäller även enskilda aktörer.

[4] 8 § och 16 § 2 p. KBF och 2 kap. 1 § lagen (2006:644) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.

Slutsats

Vid bedömningen av om en tjänst är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, dvs. om tjänsten är samhällsviktig, kan stöd hämtas i de allmänna råd som beskriver samhällsviktig verksamhet. Även beskrivningar av identifierad europeisk kritisk viktig infrastruktur kan användas i identifieringsarbetet även om ingen sådan i dagsläget är utpekad i Sverige. Det är dock viktigt att vara medveten om de olika regelverkens utgångspunkter.

NIS-direktivets syfte är att förbättra den inre marknadens funktion genom att fastställa åtgärder för säkerhet i nätverk och informationssystem. Det rör sig därför om tjänster som är viktiga för samhällets funktionalitet i sin helhet och där ett avbrott i tjänsten hindrar genomförandet av ekonomisk verksamhet, genererar omfattande ekonomiska förluster, undergräver användarnas förtroende och medför allvarliga konsekvenser för landets och unionens ekonomi.

Detta innebär att begreppet samhällsviktiga tjänster kan omfatta fler funktioner än de som absolut behövs för upprätthållandet av viktiga samhällsfunktioner vid allvarliga händelser eller kriser. Utredningen bedömer dock att det i de flesta fall kommer att röra sig om tjänster som tillhandahålls av enheter som verkar inom de samhällsviktiga verksamheterna.

Bedömningen av om en tjänst är en samhällsviktig tjänst

I avsnittet undersöks om det finns myndigheter och nätverk som redan i dag har kunskap och erfarenhet som kan ligga till grund för att bedöma om en tjänst är en samhällsviktig tjänst.

Myndigheter, landsting, kommuner och vissa enskilda gör i dag risk- och sårbarhetsanalyser i syfte att stärka sin egen och samhällets krisberedskap. Det finns således i dag en systematik för att identifiera samhällsviktig verksamhet för offentliga aktörer samt vissa enskilda aktörer.

Inom vissa sektorer framgår det också redan av beskrivningen av enheten i bilaga 2 till NIS-direktivet vilken typ av tjänst som avses, till exempel sjötrafikinformationstjänst.

Flera myndigheter, bland annat inom expert- och referensgruppen, har uppgett till utredningen att de kan identifiera samhällsvik-

tiga tjänster utifrån definitionerna av enheterna som anges i bilaga 2 till NIS-direktivet. Dessa myndigheter har bred kunskap och erfarenhet av verksamheten inom respektive sektor och delsektor. Detta bör tas tillvara i arbetet med att öka säkerheten i nätverk och informationssystem. De myndigheter som utredningen avser är Statens energimyndighet för energisektorn, Transportstyrelsen för transportsektorn, Finansinspektionen för sektorerna bankverksamhet och finansmarknadsinfrastruktur, Inspektionen för vård och omsorg för hälso- och sjukvårdssektorn, Livsmedelsverket för sektorn leverans och distribution av dricksvatten samt Post- och Telestyrelsen för sektorn digital infrastruktur. Dessa myndigheter föreslås också vara tillsynsmyndigheter i kapitel 8. Vid behov kan dessa myndigheter inhämta synpunkter från andra myndigheter inom sektorn samt från befintliga nätverk inom området i arbetet med att identifiera samhällsviktiga tjänster.

Det finns flera myndigheter som tar emot uppgifter om samhällsviktig verksamhet enligt bestämmelserna för olika risk- och säkerhetsanalyser. MSB måste dock anses ha en central funktion när det gäller bedömningen av innehållet i risk- och sårbarhetsanalyser. Sedan MSB grundades har myndigheten årligen fått i regleringsbrevsuppdrag att redovisa en nationell bedömning av samhällets förmågor, risker, sårbarheter samt identifierade och genomförda åtgärder avseende krisberedskapen. Enligt rapporten *Nationell risk- och förmågebedömning 2016*, MSB1012, är underlaget till den nationella bedömningen i huvudsak statliga myndigheters och kommuners risk- och sårbarhetsanalyser. I MSB:s uppdrag ingår också att stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. Myndigheten har vidare en samordnande roll inom ramen för samhällets krisberedskap samt en central funktion i de nätverk som finns inom krisberedskapsområdet, se avsnitt 11.1.5. MSB har också genom sina uppdrag ett etablerat kontaktnät med merparten av de aktörer som kommer att beröras av bestämmelserna i NIS-direktivet.

Slutsatser

Mot bakgrund av att detta är ett första steg för att bedöma om en tjänst är en samhällsviktig tjänst på en mer övergripande nivå finns det enligt utredningen inget behov av att införa en särskild analys. Denna kunskap finns redan på myndigheter med verksamhet inom de berörda sektorerna, tillsynsmyndigheterna.

MSB har genom sitt uppdrag redan i dag en övergripande kännedom om den verksamhet inom vilka de flesta samhällsviktiga tjänsterna bedöms finnas. MSB är också utsedd som nationell kontaktpunkt enligt NIS-direktivet med ett ansvar för samordning och gränsöverskridande samarbete på unionsnivå. Det är därför mest naturligt att det är MSB som får ansvaret för att bedöma vilka tjänster som är att anse som samhällsviktiga.

I och med att MSB har fått ansvaret för att bedöma vilka tjänster som är att anse som samhällsviktiga ska MSB också ha ansvaret för upprätta och uppdatera en sådan förteckning över samhällsviktiga tjänster som anges i artikel 5.3.

Utredningen har övervägt i vilken form förteckningen ska upprättas. Den som tillhandhåller en samhällsviktig tjänst som finns på förteckningen ska undersöka om tjänsten är beroende av nätverk eller informationssystem och om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Det innebär att förteckningen måste finnas tillgänglig. Förteckningen ska också uppdateras minst vartannat år. Eftersom förteckningen i sig inte får några direkta rättverkningar i form av krav på rapportering och säkerhetsåtgärder och då den riktar sig till en större krets anser utredningen att förteckningen bör meddelas i form av föreskrifter. Ett bemyndigande för MSB föreslås därför i den nya förordningen.

Tillsynsmyndigheterna tillsammans med andra myndigheter och nätverk har stor kunskap om verksamheten inom de olika sektorerna som ska tas tillvara i arbetet med att identifiera de samhällsviktiga tjänsterna. Tillsynsmyndigheterna ska därför ges tillfälle att yttra sig innan föreskrifterna meddelas.

Utredningen föreslår också att MSB ska ansvara för ett samarbetsforum, se avsnitt 8.5.4.

6.2.2 Vilka leverantörer tillhandahåller samhällsviktiga tjänster?

Förslag: Det ska införas en bestämmelse om skyldighet för den som är ansvarig för en verksamhet som tillhandahåller en samhällsviktig tjänst att undersöka om tillhandahållandet av tjänsten är beroende av nätverk eller informationssystem och om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Undersökningen ska dokumenteras.

Följande sektoröverskridande faktorer ska beaktas när leverantören fastställer om en störning är betydande.

1. Det antal användare som är beroende av den tjänst som den berörda enheten tillhandahåller.
2. Hur beroende andra sektorer enligt bilaga 2 till NIS-direktivet är av den tjänst som enheten tillhandahåller.
3. Vilken inverkan incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet eller allmän säkerhet, uttryckt i grad och varaktighet.
4. Enhetens marknadsandel.
5. Hur stort geografiskt område som skulle kunna påverkas av en incident.
6. Enhetens betydelse för upprätthållandet av en tillräcklig tjänstenivå, med beaktande av tillgången till alternativa sätt för att tillhandahålla tjänsten.

När det är lämpligt ska även sektorspecifika faktorer beaktas.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om vilka sektorspecifika och sektoröverskridande faktorer som ska beaktas för att fastställa om en incident medför en betydande störning vid identifieringen av leverantörer av samhällsviktiga tjänster.

Tillsynsmyndigheten ska lämna upplysning till leverantörer av samhällsviktiga tjänster vid bedömning av om annan lag eller bindande EU-rättsakt ska tillämpas i stället för lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster.

NIS-direktivet ålägger medlemstaterna att senast den 9 november 2018 identifiera de leverantörer som tillhandahåller samhällsviktiga tjänster inom ett antal särskilt utpekade enheter och som är beroende av nätverk och informationssystem där en incident skulle medföra en betydande störning (artikel 5).

Vid bedömningen av om en enhet tillhandahåller en samhällsviktig tjänst är det tillräckligt att undersöka om tjänsten finns upptagen i förteckningen över samhällsviktiga tjänster. Därefter ska bedömas om tjänsten är beroende av nätverk eller informationssystem samt om en incident skulle medföra betydande störning av tjänsten. Detta innebär att det utöver att tjänsten finns på förteckningen ställs ytterligare krav för att en leverantör ska kunna identifieras som en leverantör av en samhällsviktig tjänst.

Den samarbetsgrupp som inrättats genom NIS-direktivet ska verka för ett enhetligt tillvägagångssätt för identifieringen av leverantörerna (artikel 5.6), se även avsnitt 11.3.3. En av samarbetsgruppens uppgifter är att, med Enisas[5] bistånd, utbyta bästa praxis för medlemsstaternas identifiering av leverantörer av samhällsviktiga tjänster, inklusive i samband med beroende, vad gäller risker och incidenter, som sträcker sig över gränser (artikel 11.3 l). Myndigheten för samhällsskydd och beredskap representerar Sverige i samarbetsgruppen, se avsnitt 11.3.2.

När medlemsstaterna identifierar operatörer i sjöfartssektorn, bör de ta hänsyn till befintliga och framtida internationella koder och riktlinjer som utvecklats särskilt av Internationella sjöfartsorganisationen, i syfte att skapa ett enhetligt tillvägagångssätt för enskilda sjöfartsoperatörer.

När det finns EU-rättsakter som anses utgöra lex specialis bör dessa bestämmelser inklusive sådana som rör jurisdiktion tillämpas, och det bör inte genomföras något identifieringsförfarande för leverantörer av samhällsviktiga tjänster, se avsnitt 5.4.

[5] Europeiska unionens byrå för nät- och informationssäkerhet (European Union Agency för Network and Information Security, ENISA).

Identifiering av leverantörer

Utredningen ska analysera hur direktivets krav på identifiering av leverantörer av samhällsviktiga tjänster ska genomföras i svensk rätt. Analysen bör enligt kommittédirektiven göras med utgångspunkten att det är verksamhetsutövaren som är ansvarig för att avgöra om denne omfattas av regelverket, vilket motsvarar vad som gäller enligt till exempel säkerhetsskyddslagen (1996:627).

Enligt 5 § säkerhetsskyddsförordningen (1996:633) ska myndigheter och andra som säkerhetsskyddsförordningen gäller för undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet av undersökningen (säkerhetsanalys) ska dokumenteras. I förslaget till ny säkerhetsskyddslag[6] föreslås att den som är ansvarig för säkerhetskänslig verksamhet ska se till att behovet av säkerhetsskydd för den egna verksamheten utreds i form av en säkerhetsskyddsanalys. Ett syfte med denna analys är att identifiera de allra känsligaste delverksamheterna.

Som framgår av avsnitt 6.2.1 gör myndigheter, kommuner och landsting risk- och sårbarhetsanalyser regelbundet för att stärka sin egen och samhällets krisberedskap genom att analysera om det finns sådan sårbarhet eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området.

Förteckning över samhällsviktiga tjänster

Förteckningen över samhällsviktiga tjänster bör meddelas i föreskriftsform, se avsnitt 6.2.1. MSB ska meddela föreskrifter om vilka tjänster som är viktiga för att upprätthålla kritisk samhällelig och/eller ekonomisk verksamhet, dvs. som bedöms vara samhällsviktiga.

[6] *En ny säkerhetsskyddslag*, SOU 2015:25.

Beroende av nätverk eller informationssystem

Leverantörer av sådana samhällsviktiga tjänster som finns upptagna på förteckningen som MSB meddelat i föreskriftsform ska undersöka om tillhandahållandet av tjänsten är beroende av nätverk eller informationssystem. Denna undersökning ska dokumenteras.

Betydande störning

Slutligen ska leverantörer av sådana samhällsviktiga tjänster som finns upptagna på förteckningen som MSB meddelat i föreskriftsform och som är beroende av nätverk eller informationssystem undersöka om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Denna undersökning ska dokumenteras.

I NIS-direktivet anges ett antal faktorer som ska beaktas när det fastställs vad som är en betydande störning. Utöver dessa sektorsöverskridande faktorer kan det också finnas skäl att beakta sektorspecifika faktorer (artikel 6).

Följande sektoröverskridande faktorer ska beaktas.

- Det antal användare som är beroende av den tjänst som den berörda enheten tillhandahåller.
- Hur beroende andra sektorer enligt bilaga 2 till NIS-direktivet är av den tjänst som enheten tillhandahåller.
- Vilken inverkan incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet eller allmän säkerhet, uttryckt i grad och varaktighet.
- Enhetens marknadsandel.
- Hur stort geografiskt område som skulle kunna påverkas av en incident.
- Enhetens betydelse för upprätthållandet av en tillräcklig tjänstenivå, med beaktande av tillgången till alternativa sätt för att tillhandahålla tjänsten.

För att fastställa om en incident skulle medföra en betydande störning vid tillhandahållandet av en samhällsviktig tjänst, bör medlemsstaterna beakta ett antal olika faktorer, såsom antalet användare som är beroende av tjänsten för privata eller yrkesmässiga ändamål. Användningen av tjänsten kan vara direkt, indirekt eller ske genom förmedling. Vid bedömningen av en incidents eventuella inverkan på ekonomisk och samhällelig verksamhet eller allmän säkerhet, uttryckt i grad och varaktighet, bör medlemsstaterna också bedöma hur länge det sannolikt skulle ta tills avbrottet skulle börja ha en oacceptabel inverkan (skäl 27).

Medlemsstaterna ska även, i lämpliga fall, beakta sektorspecifika faktorer. När det gäller energileverantörer kan sådana faktorer omfatta mängden eller andelen producerad nationell el, för oljeleverantörer mängden olja per dag, för lufttransport, inbegripet flygplatser och lufttrafikföretag, järnvägstransport och kusthamnar andelen nationell trafikmängd och antalet passagerare eller lastningar per år, för bankverksamhet eller finansmarknadsinfrastrukturer deras betydelse för systemet på grundval av samlade tillgångar eller förhållandet mellan dessa tillgångar och BNP, för hälso- och sjukvårdssektorn antalet patienter som leverantören vårdar per år, för produktion, bearbetning och leverans av vatten, volym, antal och typer av användare, inbegripet t.ex. sjukhus, offentlig sektor, organisationer och personer samt förekomsten av alternativa vattenkällor för samma geografiska område (skäl 28).

Ett stöd i arbetet med att fastställa när en störning är betydande är Myndigheten för samhällsskydd och beredskaps vägledningar[7] som bl.a. beskriver en modell för att bedöma acceptabel avbrottstid och bedömning av konsekvenser.

För att fastställa vad som ska anses vara en betydande störning utifrån de sektoröverskridande faktorerna krävs det enligt utredningens mening kunskap om verksamheten och om konsekvenserna av en incident. Vikten av verksamhetskunskap blir dock ännu tydligare vid bedömning av och framtagande av sektorspecifika faktorer. Det torde därför vara den myndighet som har kunskap om verksamhetsområdet som i första hand kan bedöma vad som ska anses vara en betydande störning.

[7] Vägledning för samhällsviktig verksamhet, MSB620, januari 2014 och Vägledning för risk- och sårbarhetsanalys, MSB245, april 2011.

När det gäller bedömningen huruvida en incident medför en betydande störning i den samhällsviktiga tjänsten finnas ett bra underlag eftersom myndigheter, landsting, kommuner m.fl. gör risk- och sårbarhetsanalyser med liknande bedömningar av konsekvenser och acceptabel avbrottstid m.m. Inför 2015 års risk- och sårbarhetsanalysarbete fick också samtliga myndigheter som omnämns i bilagan till förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (KBF) i uppdrag av regeringen att särskilt beakta och analysera informationssäkerhet ur olika perspektiv. I dessa sammanställningar bör finnas uppgifter och bedömningar som kan utgöra underlag i arbetet med att fastställa om en störning är betydande.

I de fall det utifrån andra bestämmelser redan finns bedömningar avseende störningar i tillhandahållandet av tjänsten inom sektorn bör dessa givetvis användas i detta arbete.

Utredningens bedömning är att tillsynsmyndigheten ska utfärda närmare föreskrifter som behövs för att fastställa om en incident medför en betydande störning.

Tillsynsmyndigheten ska stödja MSB i arbetet i den samarbetsgrupp som inrättats genom NIS-direktivet och bistå MSB med information om antalet leverantörer och eventuella befintliga tröskelvärden avseende betydande störning (artikel 5.7). I arbetet med att ta fram sektorspecifika faktorer har också samarbetsgruppen en viktig uppgift i att verka för att bedömningen blir enhetlig inom hela unionen, se avsnitt 11.3.3.

Omfattas leverantören av NIS-direktivet – lex specialis

I vissa fall är det otydligt i vilken utsträckning bestämmelserna i en EU-rättsakt motsvarar kraven i NIS-direktivet. I sådana fall ska tillsynsmyndigheterna lämna upplysning till leverantörerna av samhällsviktiga tjänster om annan lag eller bindande EU-rättsakt ska tillämpas i stället för den nya lagen. Detta gäller också när nya EU-rättsakter beslutas.

Slutsatser

Utredningen konstaterar att de flesta offentliga verksamhetsutövare inom de sektorer och delsektorer som anges i NIS-direktivet redan gör analyser utifrån liknande krav genom till exempel risk- och sårbarhetsanalyser som görs med stöd av krisberedskapsbestämmelserna. När det gäller enskilda verksamhetsutövare görs risk- och sårbarhetsanalyser endast i begränsad omfattning inom till exempel energisektorn och finanssektorn.

Utredningen anser därför att det mest effektiva sättet att identifiera leverantörer av samhällsviktiga tjänster är att komplettera ett befintligt system. Det innebär att aktörer som är ansvariga för en verksamhet som tillhandahåller en sådan tjänst som anges i föreskriften om samhällsviktiga tjänster ska undersöka om tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten

För de myndigheter och enskilda som redan i dag omfattas av ett krav på att göra risk- och säkerhetsanalyser kan, om det är lämpligt, identifieringen av leverantörer av samhällsviktiga tjänster ingå som en del i detta arbete. För andra aktörer blir kravet på en undersökning en ny uppgift.

Utredningens bedömning är därför att det ska införas en bestämmelse om skyldighet för aktörer som är ansvariga för en verksamhet som tillhandahåller en tjänst som anges i föreskriften om samhällsviktiga tjänster att undersöka om tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Undersökningen ska dokumenteras.

Under utredningens arbete har fråga uppkommit om vem som slutligen avgör vem som är en leverantör av en samhällsviktig tjänst i de fall tillsynsmyndigheten och den som tillhandahåller en samhällsviktig tjänst har olika uppfattningar. I ett sådant fall kan tillsynsmyndigheten enligt utredningens uppfattning utfärda ett föreläggande eller vidta andra åtgärder som kan överklagas och därmed prövas av domstol.

Närmare bestämmelser om hur de sektoröverskridande kriterierna i artikel 6 samt, i lämpliga fall, sektorspecifika kriterier ska bedömas, bör regleras i myndighetsföreskrifter som utfärdas av tillsyns-

myndigheterna. Ett bemyndigande ska därför införas i den nya lagen. MSB ska ges tillfälle att yttra sig innan föreskrifterna meddelas.

I den nya förordningen föreslås att tillsynsmyndigheterna ska lämna upplysning till leverantörerna av samhällsviktiga tjänster vid bedömning av om annan lag eller annan bindande EU-rättsakt ska tillämpas i stället för den nya lagen.

6.2.3 Samhällsviktig tjänst i flera länder i EU

Förslag. Tillhandahålls tjänsten även i andra länder i den Europeiska unionen ska den nationella kontaktpunkten samråda med motsvarande funktion i andra berörda länder innan beslut om identifiering fattas.

Myndigheten för samhällsskydd och beredskap ska företräda Sverige i bilaterala och multilaterala samråd när en samhällsviktig tjänst tillhandahålls i ett eller flera andra länder i den Europeiska unionen.

Tillsynsmyndigheterna ska ges tillfälle att yttra sig före samrådet och vid behov lämna stöd till Myndigheten för samhällsskydd och beredskap.

Tillhandahålls tjänsten i två eller flera medlemsstater ska dessa medlemsstater samråda med varandra innan beslut om identifiering av leverantören fattas (artikel 5.4).

Om en enhet tillhandahåller en samhällsviktig tjänst i två eller flera medlemsstater, bör dessa medlemsstater vid identifieringsförfarandet föra bilaterala eller multilaterala diskussioner med varandra. Denna samrådsprocess är avsedd att hjälpa medlemsstaterna att bedöma om leverantören i fråga är av kritisk betydelse när det gäller gränsöverskridande inverkan, varigenom varje berörd medlemsstat ges möjlighet att lägga fram sina synpunkter avseende riskerna med de tjänster som tillhandahålls. I denna process bör de berörda medlemsstaterna beakta varandras synpunkter, och bör i detta avseende kunna begära bistånd från samarbetsgruppen, som har detta som en av sina uppgifter (artikel 11.3 l).

I den samarbetsgrupp som inrättats genom direktivet ska Sverige företrädas av MSB, se avsnitt 11.3. Mot bakgrund härav och eftersom utredningen föreslår att MSB ska ha det samordnande ansvaret

att bedöma vilka tjänster som är att betrakta som samhällsviktiga är det enligt utredningen lämpligt att MSB ska ansvara för att samråda med andra medlemsstater innan man fattar beslut om att identifiera en leverantör av en samhällsviktig tjänst. En bestämmelse om detta föreslås i den nya förordningen.

Inför samrådet bör MSB ha kontakt med berörd tillsynsmyndighet eftersom det i sektorerna redan finns upparbetade samverkanskanaler med motsvarande myndigheter i Europa. Denna erfarenhet och kunskap inom sektorerna ska tas tillvara och tillsynsmyndigheterna ska vid behov lämna stöd till MSB inför bilaterala samråd.

7 Säkerhetskrav och incidentrapportering – leverantörer av samhällsviktiga tjänster

7.1 Inledning

Den tekniska utvecklingen har skapat nya möjligheter för både offentlig sektor, näringsliv och medborgare. Detta har lett till ökade krav på att information ska vara tillgänglig dygnet runt och oavsett var informationen finns. För att tillgodose dessa krav är nätverk och informationssystem i allt större utsträckning sammankopplade eller beroende av varandra. Ökad funktionalitet och ömsesidiga beroenden har medfört att nya hot, risker och sårbarheter har introducerats, såsom brister i uppdatering, handhavandefel, tekniska fel, olyckor och brott.

Samhället måste fungera även vid störningar, olyckor, kriser och krig. För samhällets funktionalitet är det i många fall av avgörande betydelse att information är tillgänglig, riktig, att konfidentialiteten upprätthålls samt att den är spårbar. Eftersom information i de flesta fall hanteras i nätverk och informationssystem när det gäller samhällsviktiga tjänster är det av stor vikt att dessa är tillräckligt säkra. I många fall är också systemen helt avgörande för att kunna tillhandahålla tjänsten. Konsekvenserna av ett driftavbrott i nätverk och informationssystem kan bli stora och oöverskådliga. När en aktör med många kunder drabbas av driftstörningar kan konsekvenserna bli kännbara och oväntade på många håll samtidigt.

Det blir därför viktigt att leverantörer som tillhandahåller samhällsviktiga tjänster analyserar hot, risker och befintliga men även potentiella sårbarheter i nätverk och informationssystem som tillhandahåller samhällsviktiga tjänster för att kunna vidta adekvata

säkerhetsåtgärder. Leverantörerna bör även identifiera vilka skadekonsekvenser ett driftavbrott medför.

Information om incidenter blir alltmer värdefull för allmänheten och företag för att kunna hantera och förebygga incidenter i den egna verksamheten. Redan i dag tillhandhålls information om incidenter på nationella webbplatser, till exempel www.cert.se. I NIS-direktivet föreslås att CSIRT-nätverket ska upprätthålla en webbplats där allmän information om allvarliga incidenter i unionen görs tillgänglig för allmänheten. Informationen ska dock vara särskilt inriktad på företags intressen och behov. CSIRT-enheter uppmuntras att på frivillig väg tillhandahålla information till denna webbplats. I vissa fall finns det säkerhetsskäl som medför att den information som görs tillgänglig bör vara begränsad. Det kan till exempel röra sig om säkerhetsbrister som skulle kunna utnyttjas av en antagonist.

I detta kapitel behandlas kraven på leverantörer av samhällsviktiga tjänster. Kraven beträffande leverantörer av digitala tjänster behandlas i avsnitt 10.3.

7.2 Nuvarande reglering

Samhällsviktiga tjänster tillhandhålls av statliga myndigheter, kommuner, landsting samt privata aktörer på alla nivåer från lokalt till nationellt.

I många fall tillhandahåller en verksamhet både samhällsviktiga och icke samhällsviktiga tjänster. Luftfartssektorn tillhandahåller till exempel skötsel av start- och landningsbanor, men också tjänster som inte kan betraktas som samhällsviktiga, såsom butiksområden. Kraven på incidentrapportering och säkerhetskraven i NIS-direktivet omfattar endast sådana tjänster som är samhällsviktiga.

7.2.1 Säkerhetsåtgärder

Leverantörer inom de sektorer som omfattas av NIS-direktivet omfattas även av annan lagstiftning som rör säkerhetsåtgärder. Kraven på säkerhetsåtgärderna utgår från de förhållanden och skyddsbehov som råder inom respektive sektor. Ett exempel är krav på driftsäkerhet för tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster. De aktörerna ska vidta tek-

niska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet[1]. Syftet med bestämmelsen är att bidra till effektiva elektroniska kommunikationer samt att skapa en grundläggande driftsäkerhetsnivå för dessa. Med driftsäkerhet avses främst upprätthållande av funktion och tillgänglighet, men även uthållighet vid extraordinära händelser. I Post- och telestyrelsens föreskrifter om krav på driftsäkerhet (PTSFS 2015:2) förtydligas vilka åtgärder som tillhandahållaren ska vidta för att leva upp till lagens krav på en grundläggande driftsäkerhet. Det är bland annat regler om övergripande driftsäkerhetsarbete, dokumentation av tillgångar och förbindelser, riskanalys och konsekvensanalys, incidenthantering, kontinuitetsplanering, åtgärder efter riskbedömning, åtgärder avseende åtkomst och behörighet och åtgärder avseende övervakning och beredskap.

Det finns också mer övergripande bestämmelser om säkerhetsåtgärder. Bestämmelser om tekniska och organisatoriska åtgärder när det gäller personuppgiftsbehandling finns i personuppgiftslagen (1998:204). Till exempel ska den som omfattas av personuppgiftslagen och är personuppgiftsansvarig vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna (31 § personuppgiftslagen). Till tekniska åtgärder räknas saker som brandväggar, krypteringsfunktioner och antivirus, medan organisatoriska åtgärder handlar om hur säkerhetsarbetet organiseras, styrs och följs upp med hjälp av rutiner, instruktioner och policyer. Generellt gäller att ju känsligare personuppgifterna är eller ju fler personuppgifter som hanteras, desto mer omfattande bör säkerhetsåtgärderna vara. När man gör en lämplighetsbedömning, det vill säga bestämmer vilken säkerhetsnivå man ska ha, ska man tänka på att åtgärderna ska ge en säkerhetsnivå som är lämplig i förhållande till tillgänglig teknik, kostnaden för åtgärderna, om det finns några särskilda risker med behandlingen samt hur pass känsliga uppgifterna är. I Datainspektionens allmänna råd[2] finns en närmare beskrivning av säkerhetsåtgärder.

I förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (KBF) finns bestämmelser för statliga myndigheters informationssäkerhet som

[1] 5 kap. 6 b § lagen (2003:389)om elektronisk kommunikation.
[2] Säkerhet för personuppgifter, Datainspektionens allmänna råd, reviderad november 2008.

gäller om inte något annat följer av lag eller annan förordning. Varje myndighet ansvarar för att egna informationssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Behovet av säkra ledningssystem ska särskilt beaktas (19 § KBF). Myndigheten för samhällsskydd och beredskap (MSB) får meddela verkställighetsföreskrifter om säkerhetskraven. I MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet, MSBFS 2016:1, finns bestämmelser om ledningssystem för informationssäkerhet, krav på informationssäkerhetsarbetet, intern incidenthantering och kontinuitetshantering.

7.2.2 Incidentrapportering

Incidentrapportering enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

För statliga myndigheter som omfattas av KBF gäller sedan den 1 april 2016 krav på att rapportera allvarliga it-incidenter (20 § KBF och MSB:s föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter, MSBFS 2016:2).

Statliga myndigheter är skyldiga att, till stöd för arbetet med samhällets informationssäkerhet, skyndsamt rapportera it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation.

Rapportering ska ske till MSB (20 § KBF). En myndighet som tillhandahåller tjänster åt en annan organisation ska i samband med rapportering informera och vid behov samråda med den eller de uppdragsgivare som berörs av incidenten.

Rapporteringsskyldigheten omfattar inte incidenter som ska rapporteras till Säkerhetspolisen eller Försvarsmakten enligt 10 a § säkerhetsskyddsförordningen (1996:633). Exempel på sådana incidenter är incidenter i informationssystem där sekretessbelagda uppgifter som rör rikets säkerhet behandlas eller i system som särskilt behöver skyddas mot terrorism.

Om det kan antas att en incident som rapporterats till MSB har sin grund i en brottslig gärning, ska MSB skyndsamt uppmana den rapporterande myndigheten att anmäla incidenten till polisen.

MSB:s tillämpningsföreskrifter

MSB har meddelat närmare föreskrifter rapportering av it-incidenter[3].

De rapporteringspliktiga it-incidenterna utgöras av kategorierna

1. störning i mjuk- eller hårdvara,
2. störning i driftmiljö,
3. informationsförlust eller informationsläckage,
4. informationsförvanskning,
5. hindrad tillgång till information,
6. säkerhetsbrist i en produkt,
7. angrepp,
8. handhavandefel,
9. oönskad eller oplanerad störning i kritisk infrastruktur, eller
10. annan plötslig oförutsedd händelse som lett till skada (3 §).

Varje myndighet ska rapportera en it-incident senast 24 timmar efter det att myndigheten upptäckt incidenten (4 §). Rapporterna ska lämnas till MSB via anvisade kontaktvägar (5 §).

En rapport ska innehålla

- myndighetens namn,
- en beskrivning av it-incidenten som även inkluderar en övergripande redovisning av händelseförlopp och vidtagna åtgärder,
- den exakta eller uppskattade tidpunkten för när it-incidenten inträffade,
- när myndigheten upptäckte it-incidenten och om den alltjämt pågår eller är avslutad,

[3] MBSFS 2016:2.

- till vilken eller vilka kategorier enligt 3 § som it-incidenten hör, samt
- myndighetens initiala bedömning av it-incidentens omfattning och konsekvenser, både faktiska och potentiella.

I rapporten ska om möjligt även anges bedömd sekretess för den information som rapporteras in. Om den rapporterande myndigheten vid sin interna incidentutredning konstaterar att inrapporterade uppgifter om kategorier, omfattning och konsekvenser varit missvisande eller felaktiga ska myndigheten komplettera eller korrigera sin rapport så snart som möjligt (6 §).

På begäran av MSB ska en rapporterande myndighet lämna uppgifter som kompletterar rapporteringen. Sådana uppgifter ska lämnas snarast, om inget annat överenskommits med MSB (7 §).

En myndighet som inte kan lämna en rapport får i samråd med MSB lämna en preliminär rapport. Samråd ska ske innan tidsfristen för rapportering går ut. Rapporten ska innehålla den information som finns att tillgå vid inrapporteringstillfället samt när myndigheten upptäckte it-incidenten, om den fortfarande pågår eller är avslutad, samt vilken eller vilka kategorier som orsakat incidenten. Den fullständiga rapporten ska i ett sådant fall lämnas senast två veckor från det att it-incidenten upptäcktes (8 §).

Om en myndighet överlåter en del av sin informationshantering till en icke statlig aktör ska myndigheten, i överlåtelseavtalet, se till att motparten åtar sig att rapportera it-incidenter i berörda system till myndigheten på ett sätt som motsvarar kraven enligt MSB:s föreskrifter. Myndigheten ska utan dröjsmål vidarebefordra en sådan rapport till MSB. Den skyldigheten gäller med avseende på avtal som träffas efter den 4 april 2016 (9 §).

En myndighet som har polisanmält en it-incident behöver inte lämna en rapport utan endast en kopia på polisanmälan (10 §).

MSB tog i samband med att obligatoriet infördes fram både metodstöd och en kryptolösning för säker kommunikation. Myndigheten har därefter stegvis utvecklat funktionen för it-incidentrapportering, exempelvis pågår arbete med att ta fram ett tekniskt rapporteringsverktyg vilket kommer att underlätta det praktiska arbetet för de rapporterande myndigheterna. Verktyget beräknas kunna tillhandahållas under 2017. Det sker dessutom ett kontinuerligt arbete med att förbättra och förfina metodstödet för rapporteringen. MSB arbetar

aktivt i förhållande till rapporteringsskyldiga myndigheter för att underlätta tillämpningen av regelverket och säkerställa en hög rapporteringsgrad.

Innan obligatoriet infördes hanterade MSB 40–80 incidenter per år som rapporterats in av olika aktörer i samhället, både privata och offentliga. Antalet inrapporterade incidenter har ökat från och med april 2016.

Av 244 rapporteringsskyldiga myndigheter har 77 myndigheter lämnat it-incidentrapporter till MSB under 2016. Åtta myndigheter har rapporterat fem eller fler incidenter. Den myndighet som rapporterat flest har rapporterat 20 incidenter. Trettionio myndigheter har rapporterat endast en incident. Huvuddelen av dessa incidenter var av begränsad/okänd eller ej angiven betydelse för verksamhetsviktiga tjänster. De vanligaste incidentkategorierna är störning i driftmiljön och angrepp. Den vanligaste konsekvensen av de rapporterade incidenterna är hindrande av tillgång till information. Sammanlagt har det under 2016 inkommit 214 incidentrapporter. Av dessa har 12 incidenter polisanmälts. Rapportflödet har varit relativt jämnt med runt 25 rapporter i månaden, bortsett från sommarmånaderna juli och augusti där antalet gick ner. Nedgången kan sannolikt till viss del förklaras av att färre användare är aktiva i systemen och att det sker mindre drift- och utvecklingsåtgärder i it-miljöer under sommaren. Säkerhetspolisen har under 2016 fått in tre it-incidentrapporter enligt 10 a § säkerhetsskyddsförordningen. Försvarsmakten har inga uppgifter att lämna avseende rapporterade incidenter eftersom de under 2016 inte fått in några formella rapporter enligt 10 a § säkerhetsskyddsförordningen[4].

Där det kan antas att incidenten har sin grund i en brottslig gärning har MSB i enlighet med förordningen (20 § KBF) uppmanat den rapporterande myndigheten att anmäla incidenten till polisen. Uppmaningen sker enligt MSB dels genom ett automatsvar, dels genom personlig kontakt.

Informationsutbytet mellan Polismyndigheten och MSB regleras i en överenskommelse.

Det har visat sig att rapporteringsfrekvensen skiljer sig åt mellan olika myndigheter. Förklaringarna till den ojämna rapporteringen kan enligt MSB vara flera. Att en myndighet inte rapporterar kan bero

[4] MSB:s Årsrapport It-incidentrapportering 2016, dnr 2016-6304-7.

på att säkerheten är så god att några rapporteringspliktiga incidenter inte inträffar. Det kan emellertid även bero på att det finns sådana säkerhetsbrister att incidenter, exempelvis intrång, inte upptäcks. Vissa myndigheter har framfört att tillämpliga sekretessregler för inrapporterade it-incidenter inte upplevs som tillräckligt heltäckande och att detta har bidragit till att incidenter inte rapporteras alls alternativt att rapporten innehåller endast knapphändig information om vad som hänt. MSB arbetar aktivt med att öka benägenheten att rapportera.

Utöver bestämmelserna i KBF finns ytterligare bestämmelser om rapporteringsskyldighet för incidenter, bland annat i lagen (2003:389) om elektronisk kommunikation, lagen (2007:528) om värdepappersmarknaden och i den kommande regleringen i direktiv (EU) 2015/2366 av den 25 november 2016 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (det andra betaltjänstdirektivet).

Incidentrapportering enligt lagen (2003:389) om elektronisk kommunikation

Den som tillhandahåller ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst är skyldig att utan onödigt dröjsmål rapportera störningar eller avbrott av betydande omfattning till Post- och telestyrelsen enligt 5 kap. 6 c § lagen (2003:389) om elektronisk kommunikation (LEK). Av Post- och telestyrelsens föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning (PTSFS 2012:2) framgår på vilket sätt den skyldigheten ska fullgöras och om undantag från skyldigheten.

Den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster ska utan onödigt dröjsmål underrätta PTS om integritetsincidenter. Med integritetsincident avses en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring, eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster. Om incidenten kan antas inverka negativt på de abonnenter eller användare som de behandlade upp-

gifterna berör, eller om tillsynsmyndigheten begär det, ska även dessa underrättas utan onödigt dröjsmål. (6 kap. 1 och 4 a §§ LEK).

Rapportering av händelser av väsentlig betydelse enligt lagen (2007:528) om värdepappersmarknaden.

En börs, dvs. ett svenskt företag som har fått tillstånd att driva en reglerad marknad, ska enligt lagen (2007:528) om värdepappersmarknaden identifiera och hantera de risker som kan uppstå i verksamheten och ha säkra tekniska system (13 kap. 1 § tredje stycket 1 och 2). För bl.a. företag som ansöker om tillstånd att som börs driva en reglerad marknad eller en handelsplattform gäller Finansinspektionens föreskrifter (FFFS 2007:17) om verksamhet på marknadsplatser. Av föreskrifterna framgår att ett företag som ansöker om sådant tillstånd till sin ansökan ska bifoga en verksamhetsplan (1 a kap. 3 § 5 och 12 kap. 8 § värdepappersmarknadslagen). I verksamhetsplanen ska det också finnas en hänvisning till eventuella riktlinjer för hantering av händelser av väsentlig betydelse, som företaget fastställt i enlighet med Finansinspektionens allmänna råd (FFFS 2013:11) om rapportering av händelser av väsentlig betydelse (1 a kap. 20 §).

Direktiv (EU) 2015/2366 av den 25 november 2016 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG.

I november 2015 antogs det andra betaltjänstdirektivet med syfte att bidra till att utveckla en EU-omfattande marknad för elektroniska betalningar och till att skapa bättre förutsättningar för säkra och effektiva betalningar. Direktivet innehåller bl.a. bestämmelser som reglerar frågor om säkerhet och hantering av risker i samband med betaltjänstleverantörers kommunikation med betaltjänstanvändare, till exempel i fråga om en betalningstransaktion.

Av artikel 96.1 följer att betaltjänstleverantörer vid allvarliga operativa eller säkerhetsincidenter utan onödigt dröjsmål ska underrätta den behöriga myndigheten i hemmedlemsstaten. Om incidenten påverkar eller kan påverka betaltjänstanvändarnas ekonomiska intressen ska leverantören dessutom utan onödigt dröjsmål informera

användarna om incidenten och om alla tillgängliga åtgärder som de kan vidta för att begränsa dess negativa effekter.

Enligt artikel 96.2 ska den behöriga myndigheten i hemmedlemsstaten, efter att ha mottagit en underrättelse som avses i artikel 96.1, utan onödigt dröjsmål låta EBA och ECB ta del av relevanta uppgifter om incidenten. Myndigheten ska också, efter att ha gjort en bedömning av incidentens relevans för andra berörda myndigheter i den medlemsstaten, informera dem om incidenten.

7.3 NIS-direktivet

7.3.1 Säkerhetsåtgärder

Förslag: Leverantörer av samhällsviktiga tjänster ska bedriva ett systematisk och riskbaserat informationssäkerhetsarbete.

Leverantörer av samhällsviktiga tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder i sin verksamhet. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till den föreliggande risken.

Leverantörer av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga och minimera verkningarna av incidenter som påverkar säkerheten i nätverk och informationssystem som används för att tillhandahålla sådana samhällsviktiga tjänster, i syfte att säkerställa kontinuiteten i dessa tjänster.

Leverantörer av samhällsviktiga tjänster ska göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder. I analysen ska ingå en åtgärdsplan. Analysen ska dokumenteras och uppdateras årligen.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om ett systematiskt och riskbaserat informationssäkerhetsarbete och den närmare utformningen av säkerhetsåtgärder.

Myndigheten för samhällsskydd och beredskap ska lämna råd och stöd till tillsynsmyndigheterna vid utarbetandet av myndighetsföreskrifter.

Med säkerhet i nätverk och informationssystem avses i NIS-direktivet systemens 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 nätverk och informationssystem (artikel 4.2).

Nätverks och informationssystems tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och i synnerhet för den inre marknadens funktion. Systemen har en viktig roll för att underlätta gränsöverskridande rörlighet för varor, tjänster och personer. Genom NIS-direktivet införs gemensamma säkerhetskrav för leverantörer av samhällsviktiga tjänster i unionen.

Bestämmelser om säkerhetsåtgärder i nätverk och informationssystem finns i flera av de sektorer som omfattas av NIS-direktivet både i nationella bestämmelser och i EU-rättsakter. Regleringen är emellertid inte heltäckande och i några fall är syftet med säkerhetsåtgärderna ett annat än det som anges i NIS-direktivet. Utredningens bedömning är därför att det måste införas bestämmelser med krav på säkerhetsåtgärder enligt NIS-direktivet.

Om det i en sektorspecifik unionsrättsakt föreskrivs krav på att leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster antingen ska säkerställa säkerheten i sina nätverk och informationssystem eller rapportera incidenter, ska bestämmelserna i den sektorspecifika unionsrättsakten tillämpas, förutsatt att verkan av kraven i fråga minst motsvarar verkan av skyldigheterna i NIS-direktivet (artikel 1.7). Angående denna princip om lex specialis, se avsnitt 5.4.

Riskhantering

Leverantörer av samhällsviktiga tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder i sin verksamhet. Åtgärderna ska, med beaktande av den senaste tekniska utvecklingen, säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till den föreliggande risken (artikel 14.1).

Med risk avses i NIS-direktivet en rimlig identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i nätverk och informationssystem (artikel 4.9). Riskhantering omfattar åtgärder för att identifiera alla incidentrisker samt att ta fram åtgärder för att förebygga, upptäcka och hantera incidenter för att begränsa deras inverkan. Säkerheten i nätverk och informationssystem omfattar lagrade, överförda och behandlade uppgifters säkerhet (skäl 46).

Den nationella strategi som ska antas enligt artikel 7 ska omfatta en riskbedömningsplan.

Incidenthantering

Leverantörer av samhällsviktiga tjänster ska också vidta lämpliga åtgärder för att förebygga och minimera verkningarna av incidenter som påverkar säkerheten i nätverk och informationssystem som används för att tillhandahålla sådana samhällsviktiga tjänster, i syfte att säkerställa kontinuiteten i dessa tjänster (artikel 14.2).

Med incidenthantering avses alla förfaranden som stöder upptäckt, analys och begränsning av en incident och åtgärder mot en incident (artikel 4.8). I detta arbete är det viktigt att dra lärdom om incidenter som har inträffat. Det är därför viktigt att den rapporterande leverantören får del av den ytterligare information som CSIRT-enheten fått eller upprättat om incidenten. Sådan information bidrar till en effektiv hantering av både pågående och framtida incidenter (artikel 14.5 andra stycket), se avsnitt 11.2.3.

Tekniska och organisatoriska åtgärder

Säkerhetsåtgärder för informationssäkerhet omfattar åtgärder inom det administrativa och tekniska säkerhetsområdet. Med teknisk säkerhet brukar avses områdena it-säkerhet (data- och kommunikationssäkerhet) och fysisk säkerhet. I begreppet tekniska åtgärder ingår bl.a. skydd mot oönskad förändring, skydd mot obehörig insyn, att behöriga har åtkomst vid rätt tillfälle, skydd av personer, lokaler och utrustning av betydelse för informationssäkerhet samt skydd vid överföring av data. Skyddsåtgärderna ingår i det som brukar benämnas teknisk säkerhet. I begreppet organisatoriska åtgärder ingår

bl.a. att upprätta styrdokument, utforma rutiner, övervaka efterlevnad samt genomföra uppföljningar; det som brukar benämnas administrativ säkerhet[5].

Leverantören av den samhällsviktiga tjänsten är ansvarig för att säkerställa säkerheten i de nätverk och informationssystem som leverantören använder. Säkerhetskraven gäller för leverantören oavsett om denne sköter underhållet av sina nätverk och informationssystem internt eller lägger ut uppgifterna på entreprenad (skäl 52).

För att identifiera vilka tekniska och organisatoriska åtgärder som är relevanta för leverantörerna i de olika sektorerna är det nödvändigt att känna till vad det är som ska skyddas, mot vad och i vilket syfte.

I den undersökning som leverantören gjort för att identifiera om den samhällsviktiga tjänst som leverantören tillhandahåller omfattas av bestämmelserna i den nya lagen framgår vilka nätverk och informationssystem som används för att tillhandahålla tjänsten, se avsnitt 6.2.2.

En förutsättning för att kunna vidta ändamålsenliga och proportionella säkerhetsåtgärder som är anpassade till riskerna är enligt utredningens mening att leverantören genomför en riskanalys. Leverantörer som tillhandahåller samhällsviktiga tjänster ska därför beskriva och bedöma relevanta hot och risker som de föreslagna säkerhetsåtgärderna är tänkta att hantera. Analysen ska också beskriva och bedöma hur effektiva befintliga säkerhetsåtgärder är i förhållande till kända sårbarheter. Vidare bör leverantören identifiera potentiella sårbarheter. Det bör framgå av analysen vilka negativa konsekvenser en incident skulle kunna medföra. Denna riskanalys har därför ett annat syfte än risk- och sårbarhetsanalyser som görs med anledning av krisberedskap och höjd beredskap, se avsnitt 6.2.1. Analysen kan dock ingå som en del i andra liknande säkerhets- och riskanalyser som genomförs i leverantörens verksamhet.

Säkerhetsåtgärderna ska säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till den föreliggande risken. Säkerhetsåtgärder ska också förebygga och minimera verkningar av incidenter som påverkar säkerheten i syfte att säkerställa kontinuiteten i den samhällsviktiga tjänsten.

[5] Terminologi för informationssäkerhet, Teknisk rapport SIS-TR 50:2015.

De tekniska och organisatoriska åtgärder som leverantörer av samhällsviktiga tjänster ska vidta bör inte innebära krav på att någon särskild kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt (skäl 51). Trots att hårdvarutillverkare och mjukvaruutvecklare varken är leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster, ökar deras produkter säkerheten i nätverk och informationssystem. De spelar därför en viktig roll när det gäller att göra det möjligt för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster att skydda sina nätverk och informationssystem. Sådana hårdvaru- och mjukvaruprodukter omfattas redan av befintliga bestämmelser om produktansvar (skäl 50).

När leverantören beslutar om vilka säkerhetsåtgärder som ska vidtas ska den senaste tekniska utvecklingen beaktas, dvs. samtliga tekniska lösningar som vid var tid finns tillgängliga på marknaden. Teknisk utveckling kan dels medföra att behovet av säkerhetsåtgärder förändras, dels innebära nya möjligheter att vidta effektiva säkerhetsåtgärder. Det innebär också att säkerhetskraven regelbundet måste ses över för att säkerställa en hög nivå av säkerhet i nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster. Har en incident inträffat bör det medföra att säkerhetsåtgärderna skyndsamt ses över. Underlåtenhet att vidta säkerhetsåtgärder kan medföra beslut om sanktionsavgift.

Bedömningarna i analysen ska ligga till grund för valet av säkerhetsåtgärder och ska också kunna användas som beslutsstöd för leverantörens prioriteringar och avvägningar mellan olika typer av säkerhetsåtgärder i förhållande till tjänstens funktionalitet samt finansiella och administrativa konsekvenser. Behandlas personuppgifter är det också nödvändigt att försäkra sig om att skyddet för den personliga integriteten upprätthålls enligt de bestämmelser som gäller för personuppgiftsbehandling.

Analysen ska dokumenteras och kompletteras med en åtgärdsplan. Analysen ska uppdateras årligen.

Riskanalysen bör också används som underlag när sektorsvisa myndighetsföreskrifter utformas.

En förutsättning för en väl anpassad säkerhet i nätverk och informationssystem är att det bedrivs ett systematiskt och riskbaserat informationssäkerhetsarbete. Det är ett sätt för verksamhetens ledning att på ett systematiskt sätt styra arbetet med informationssäker-

het i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering. En del i detta arbete är olika typer av analyser, till exempel verksamhetsanalys, riskanalys och GAP-analys. Arbetet bör utgå från en godkänd europeisk eller internationell standard utan att ställa krav på att en viss standard måste användas. För att skapa en gemensam grund för leverantörer av samhällsviktiga tjänster anser utredningen att det ska införas ett krav på att leverantörer av samhällsviktiga tjänster bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete samt att regeringen eller den myndighet regeringen bestämmer ska få meddela föreskrifter om ett systematiskt informationssäkerhetsarbete enligt den nya lagen. Föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete finns redan i dag för statliga myndigheter i Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet, MSBFS 2016:1, se avsnitt 7.2.1. Det bör därför vara MSB som vid behov får utfärda generella föreskrifter om hur ett systematiskt informationssäkerhetsarbete för samtliga sektorer kan bedrivas.

Det har under utredningens arbete framförts att detta i stället borde göras av tillsynsmyndigheterna med vägledning från MSB. Utredningen menar dock, i och med att MSB redan föreskrivit om ett systematiskt och riskbaserat informationssäkerhetsarbete för statliga myndigheter, att det är mest effektivt om MSB föreskriver om en gemensam grund även på den nya lagens tillämpningsområde.

När det gäller föreskrifter för verksamheterna inom de sju olika sektorerna anser utredningen, mot bakgrund av att nätverk och informationssystem är en integrerad del av verksamheten, att det är den myndighet med kunskap om verksamheten som ska ha ansvaret för att utfärda föreskrifter. I den nya förordningen föreslås därför att tillsynsmyndigheten bemyndigas att meddela föreskrifter om utformningen av säkerhetsåtgärder. Viktiga underlag i föreskriftsarbetet är riskanalysen, resultaten från tillsyn och de incidentrapporter som leverantörerna inom respektive sektor har lämnat till CSIRT-enheten. Som anges i avsnitt 11.2.6 ska tillsynsmyndigheten få del av samtliga incidentrapporter för sin sektor. I föreskriftsarbetet bör tillsynsmyndigheten vid behov inhämta synpunkter från andra myndigheter som är verksamma inom sektorn samt från de nätverk som finns inom sektorerna. I den nya förordningen föreslås att MSB ska

lämna stöd till tillsynsmyndigheterna i föreskriftsarbetet samt ges tillfälle att yttra sig över föreskrifterna innan de meddelas.

7.3.2 Incidentrapportering

Förslag: Leverantörer av samhällsviktiga tjänster ska utan onödigt dröjsmål rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst de tillhandahåller. Rapporteringen ska göras till CSIRT-enheten (Myndigheten för samhällsskydd och beredskap).

För att fastställa om en incident har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten ska hänsyn framför allt tas till följande faktorer.

1. Det antal användare som påverkas av störningen av den samhällsviktiga tjänsten.
2. Hur länge incidenten varar.
3. Hur stort geografiskt område som påverkas av incidenten.

Rapporterna ska innehålla information som gör det möjligt för CSIRT-enheten att fastställa incidentens eventuella gränsöverskridande verkningar.

Rapportering ska inte medföra ökat ansvar för den rapporterande parten.

Är en leverantör av samhällsviktiga tjänster beroende av en tredjepartsleverantör av digitala tjänster för tillhandahållandet av en tjänst som är viktig för att upprätthålla kritisk samhällelig och ekonomisk verksamhet, ska leverantören av samhällsviktiga tjänster rapportera varje betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten till följd av en incident som påverkar leverantören av digitala tjänster.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om vilka faktorer som ska användas för att avgöra om en incident har betydande inverkan på kontinuiteten i en samhällsviktig tjänst och därför medför krav på rapportering, när incidentrapporteringen ska ske, på vilket sätt skyldigheten att rapportera incidenter ska fullgöras och incidentrapportens utformning.

Tillsynsmyndigheterna ska ges tillfälle att yttra sig innan föreskrifter meddelas.

Bedömning: Incidentrapporteringen bör ske efter att de första kritiska åtgärderna för att avhjälpa incidenten har vidtagits. Påverkar incidenten fler leverantörer eller är incidenten gränsöverskridande bör rapporteringen ske snarast.

Leverantörer av samhällsviktiga tjänster ska, utan onödigt dröjsmål, till den behöriga myndigheten eller CSIRT-enheten rapportera incidenter som har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänster som de tillhandahåller. Rapporterna ska innehålla information som gör det möjligt för den behöriga myndigheten eller CSIRT-enheten att fastställa incidentens eventuella gränsöverskridande verkningar. Rapportering ska inte medföra ökat ansvar för den rapporterande parten. (artikel 14.3)

Bestämmelser om incidentrapportering finns i flera av de sektorer som omfattas av NIS-direktivet. Regleringen är emellertid inte heltäckande och i några fall är syftet med incidentrapporteringen ett annat. Utredningens bedömning är därför att det måste införas bestämmelser med krav på incidentrapportering enligt NIS-direktivet.

Vem ska rapportera

Leverantörer av samhällsviktiga tjänster ska rapportera incidenter. Rapporteringskraven gäller för leverantören oavsett om leverantören sköter underhållet av sina nätverk och informationssystem internt eller lägger ut uppgifterna på entreprenad (skäl 52).

Ansvaret för incidentrapportering åligger den som identifierats som leverantör av samhällsviktiga tjänster.

Underlåtenhet att rapportera incidenter kan medföra beslut om sanktionsavgift.

När ska rapporteringen ske

Enligt NIS-direktivet ska rapportering av incidenter ske utan onödigt dröjsmål (artikel 14.3). Någon närmare precisering anges inte i direktivet.

Incidentrapporteringen är en åtgärd för att förebygga och minimera verkningar av incidenter för att säkerställa kontinuiteten i de samhällsviktiga tjänsterna.

Att CSIRT-enheten ska underrättas utan onödigt dröjsmål när en incident som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten inträffat, betyder att den berörda leverantören som regel ska lämna underrättelsen så snart de uppgifter som ska lämnas finns tillgängliga. Samtidigt är det inte rimligt att leverantören, för att fullgöra sin underrättelseskyldighet, tvingas prioritera ned arbetet med att hantera den inträffade incidenten. CSIRT-enheten bör därför underrättas så snart detta kan ske utan att störa sådant prioriterat arbete. Internt utredningsarbete kan ofta fordras för att leverantören ska kunna sammanställa samtliga uppgifter som ska lämnas till CSIRT-enheten. Utredningens bedömning är, mot bakgrund av direktivets syfte att säkerställa kontinuitet i de samhällsviktiga tjänsterna, att utgångspunkten bör vara att rapporteringen inte ska inverka negativt på arbetet med att avhjälpa incidenten. Rapporteringen bör därför ske efter att de första kritiska åtgärderna för att avhjälpa incidenten har vidtagits. Påverkar incidenten däremot fler leverantörer eller är incidenten gränsöverskridande bör rapporteringen ske snarast för att konsekvenserna ska kunna begränsas.

En väl fungerande incidenthantering är en viktig del i det förebyggande informationssäkerhetsarbetet som skapar förutsättningar för att anpassa säkerhetsåtgärder allteftersom hot och risker förändras, se avsnitt 7.3.1. Det är därför viktigt att den rapporterande leverantören får återkoppling från CSIRT-enheten om relevant information som skulle kunna bidra till effektiv hantering av incidenten och det fortsatta förebyggande arbetet, se avsnitt 11.2.3.

Är incidenten gränsöverskridande ska andra berörda medlemsstater informeras i de fall incidenten har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i den medlemsstaten. I vissa fall kan det bli aktuellt att informera allmänheten för att det ska vara möjligt att förhindra en incident eller hantera en pågående incident, se avsnitt 11.2.3. I sådana fall torde det vara lämpligt att CSIRT-enheten dels underrättas i direkt anslutning till den inträffade incidenten om det som då är känt, dels erhåller fullständig information om händelsen vid ett senare tillfälle när samtliga uppgifter har sammanställts.

Närmare bestämmelser om när rapporteringen ska ske får meddelas av regeringen eller den myndighet regeringen bestämmer. Utredningens bedömning är att MSB ska meddela föreskrifter om detta. Tillsynsmyndigheterna ska beredas tillfälle att yttra sig innan föreskrifter meddelas.

Vilka incidenter ska rapporteras?

Incidenter som rör Sveriges säkerhet ska inte rapporteras enligt den nya lagen. Sådana incidenter ska rapporteras enligt 10 a § säkerhetsskyddsförordningen (1996:633), se avsnitt 5.4. Är leverantören som tillhandahåller tjänsten tveksam om vilket regelverk som gäller för en inträffad incident bör Säkerhetspolisen eller Försvarsmakten kontaktas. Även MSB och tillsynsmyndigheten kan lämna stöd vid denna typ av frågor.

Endast incidenter som har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänster som leverantören tillhandahåller ska rapporteras. Med en incident avses en händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem (artikel 4.7). För att avgöra om en incident har en betydande inverkan ska hänsyn framför allt tas till följande faktorer (artikel 14.4):

1. Det antal användare som påverkas av störningen av den samhällsviktiga tjänsten.
2. Hur länge incidenten varar.
3. Hur stort geografiskt område som påverkas av incidenten.

Om leverantörer av samhällsviktiga tjänster är beroende av en tredjepartsleverantör av digitala tjänster för att tillhandahålla en tjänst som är viktig för att upprätthålla kritisk samhällelig och ekonomisk verksamhet, ska leverantörerna av samhällsviktiga tjänster rapportera varje betydande inverkan på kontinuiteten i de samhällsviktiga tjänsterna till följd av en incident som påverkar leverantören av digitala tjänster (artikel 16.5).

Endast händelser med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem och som orsakat en betydande inverkan på kontinuiteten på tjänsten ska rapporteras. Kravet på att incidenten ska påverka kontinuiteten i tjänsten torde medföra att

incidenter som inverkar negativt på säkerheten i övrigt i nätverk och informationssystem inte behöver rapporteras. Det kan till exempel vara fråga om intrång i systemen som inte upptäckts och som inte heller syftar till att påverka kontinuiteten. Denna typ av incidenter kan för leverantörens del vara minst lika allvarliga och bör hanteras inom ramen för det ordinarie systematiska informationssäkerhetsarbetet. För statliga myndigheter som omfattas kraven på it-incidentrapportering enligt 20 § KBF ska samtliga incidenter som allvarligt kan påverka säkerheten i informationshanteringen rapporteras. Det bör därför vara möjligt att inom ramen för frivillig rapportering rapportera även andra incidenter än de som omfattas av den nya lagen, se avsnitt 7.3.4.

Bedömningen av vilka incidenter som har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänsterna bör utgå från de ovan nämnda faktorerna samt de förhållanden som finns inom respektive sektor. Beroende på vilken sektor som avses kan faktorerna också tillmätas olika vikt. Utredningen menar att denna bedömning bäst görs av en myndighet med god kunskap om verksamheten och, i de fall det är möjligt, i samverkan med befintliga nätverk inom sektorn. I de fall bestämmelser om driftsäkerhet finns för sektorn bör dessa användas som utgångspunkt i den utsträckning det är möjligt, t.ex. PTSFS 2015:2. Närmare föreskrifter om vilka faktorer som ska användas för att avgöra om en incident har betydande inverkan på kontinuiteten som medför krav på rapportering ska därför meddelas i myndighetsföreskrifter. Ett bemyndigande ska därför föras in i den nya lagen. Utredningens bedömning är att tillsynsmyndigheten ska meddela sådana myndighetsföreskrifter. Det kan även finnas fördelar med att utforma faktorerna likartat inom de olika sektorerna. Denna typ av frågor bör enligt utredningen diskuteras i det nationella samarbetsforum som utredningen föreslår och som ska ledas av MSB.

Den samarbetsgrupp som inrättats genom NIS-direktivet får utarbeta och anta riktlinjer om incidentrapportering och om vilka faktorer som ska användas för fastställandet av hur betydande en incidents inverkan är (artikel 14.7). MSB är Sveriges representant i samarbetsgruppen. I den utsträckning samarbetsgruppen utarbetar och antar riktlinjer för skyldigheten att rapportera incidenter och vilka faktorer som ska användas bör MSB lämna råd och stöd till tillsynsmyndigheten vid utarbetandet av myndighetsföreskrifter.

MSB ska också ges tillfälle att yttra sig innan sådana föreskrifter meddelas.

Bedömningen av hur betydande en incidents inverkan är bör samordnas med förfarandet för fastställande om en störning är betydande när leverantörer av samhällsviktiga tjänster identifieras, se avsnitt 6.2.2.

Vem ska leverantörerna rapportera till?

Rapporteringen ska enligt NIS-direktivet ske till den behöriga myndigheten eller CSIRT-enheten (artikel 14.3).

Statliga myndigheter rapporterar i dag vissa it-incidenter till i första hand MSB. Utredningen föreslår i avsnitt 11.2.2 att MSB ska ha funktionen som CSIRT-enhet. Behöriga myndigheter ska utöva tillsyn och utredningen föreslår att det ska utses en tillsynsmyndighet för varje sektor, se avsnitt 8.5. I utredningsarbetet har diskuterats om incidentrapporteringen i stället bör ske till tillsynsmyndigheterna eftersom rapporteringen är ett av de viktigaste verktygen i tillsynsmyndigheternas arbete med att granska regelefterlevnaden. Erfarenheter från arbetet med incidentrapporter enligt lagen (2003:389) om elektronisk kommunikation är till exempel att tillsyn tillsammans med sanktionsmöjligheter är viktiga verktyg för att få till stånd en fungerande incidentrapportering, både när det gäller att incidenter rapporteras och att rapporternas innehåll blir tillfyllest. Flera tillsynsmyndigheter har också redan i dag upparbetade rutiner för incidentrapportering. För att kunna bistå i hanteringen av en incident, varna andra som kan drabbas både nationellt och internationellt, analysera och återföra kunskap kring inträffade incidenter krävs en omfattande organisation och vissa tekniska lösningar. Mot bakgrund av CSIRT-enhetens roll och uppdrag avseende hantering av it-säkerhetsincidenter samt att det redan finns en etablerad nationell funktion för incidentrapportering på MSB är utredningens bedömning att incidentrapportering enligt NIS-direktivet ska göras till CSIRT-enheten vid MSB. Leverantörerna ska enligt utredningens mening inte vara skyldiga att rapportera incidenter till tillsynsmyndigheten. För att tillgodose det behov av information om incidenter som finns hos tillsynsmyndigheterna ska det i stället åligga CSIRT-enheten att skyndsamt överlämna de incidentrapporter som lämnats av leve-

rantörerna till den tillsynsmyndighet som utövar tillsyn över den rapporterande leverantören, se avsnitt 11.2.6. Utformningen av rapporteringsstöd och verktyg kopplade till rapportering enligt den nya lagen bör göras i samarbete med respektive tillsynsmyndighet. Rapporterna ska också vara ett underlag när sektorsvisa myndighetsföreskrifter utformas avseende tekniska och organisatoriska åtgärder. För de tillsynsmyndigheter som också har ansvar enligt KBF finns även ett behov av incidentrapporterna för att uppfylla krav på rapportering och lägesbilder i sin sektor.

De nya bestämmelserna kan innebära att en leverantör måste rapportera samma incident till olika myndigheter men med olika syften, men så är fallet redan i dag för vissa leverantörer. Rapporteringen enligt NIS-direktivet ersätter inte sådan rapporteringsskyldighet.

Rapportens innehåll och utformning

Rapporten ska innehålla uppgifter som gör det möjligt för CSIRT-enheten att fastställa om incidenten har gränsöverskridande verkningar (artikel 14.3). Enligt utredningens mening bör det också framgå om incidenten påverkar andra leverantörer i sektorn eller leverantörer i andra sektorer, se avsnitt 11.2.3. För att den nationella kontaktpunkten ska kunna fullgöra sin skyldighet enligt artikel 10.3 bör rapporten också innehålla en beskrivning av vad som har inträffat, omfattningen och konsekvenserna av incidenten, vilka åtgärder som vidtagits för att minimera verkningarna av incidenten samt vilka åtgärder som vidtagits för att förebygga liknande incidenter i framtiden. Det ska vidare framgå av rapporten om incidenten är en följd av en incident hos en leverantör av digitala tjänster (artikel 16.5).

Rapporten ska också kunna utgöra grund för tillsynsmyndighetens bedömning av om det finns anledning att vidta tillsynsåtgärder till följd av den inträffade händelsen.

Rapporteringen får inte medföra ökat ansvar för den rapporterande parten utöver det som följer av NIS-direktivet (artikel 14.3). Det går därmed inte att ställa krav på att leverantören ska utreda händelsen åt CSIRT-enheten. I och med att rapporten är lämnad upphör leverantörens skyldigheter när det gäller incidentrapportering.

För att inte ålägga leverantörerna en onödig administrativ börda bör rapporten i så stor utsträckning som möjligt utformas på samma sätt som annan incidentrapportering. Vägledning bör hämtas från MSB:s föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter, MSBFS 2016:2. I den utsträckning det finns andra branschspecifika bestämmelser bör dessa beaktas vid utformningen av rapporten. Det kan även finnas krav från tillsynsmyndigheterna på innehållet i rapporten eftersom den är ett viktigt verktyg för tillsynsverksamheten. Dock bör rapporteringen så långt det är möjligt utformas på samma sätt för samtliga sektorer. Bestämmelser om den närmare utformningen av rapporten bör meddelas i myndighetsföreskrifter. Ett bemyndigande ska därför föras in i den nya förordningen. Utredningens bedömning är att MSB ska meddela dessa föreskrifter. Tillsynsmyndigheterna ska ges tillfälle att yttra sig innan föreskrifterna om rapportens utformning utfärdas.

Se även avsnitt 12.2 om CSIRT-enhetens uppgifter.

7.3.3 Sanktioner

NIS-direktivet ålägger medlemsstaterna att fastställa regler om sanktioner för överträdelse av nationella bestämmelser som har antagits enligt direktivet och vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Frågan om sanktioner behandlas i kapitel 9.

7.3.4 Standardisering och frivillig rapportering

Förslag: Vid utformning av säkerhetsåtgärder bör leverantörer av samhällsviktiga tjänster beakta europeiska eller internationellt accepterade standarder och specifikationer.

Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om förutsättningarna för frivillig rapportering. Tillsynsmyndigheterna ska ges tillfälle att yttra sig innan föreskrifterna meddelas.

Standardisering

För att främja en enhetlig tillämpning av säkerhetsåtgärder ska medlemsstaterna, utan att föreskriva eller gynna användning av en viss typ av teknik, uppmuntra användningen av europeiska eller internationellt accepterade standarder och specifikationer av relevans för säkerheten i nätverk och informationssystem.

Enisa ska i samarbete med medlemsstaterna utarbeta råd och riktlinjer för de tekniska områden som ska beaktas när det gäller säkerhetsåtgärder samt för redan befintliga standarder, inklusive medlemsstaternas nationella standarder, som skulle kunna täcka dessa områden (artikel 19).

Med *standard* avses en standard i den mening som avses i artikel 2.1 i förordning (EU) nr 1025/2012[6]. Där definieras standard som en teknisk specifikation som antagits av ett erkänt standardiseringsorgan för upprepad eller fortlöpande tillämpning, som inte är tvingande och som tillhör någon av följande typer:

a) internationell standard: en standard som antagits av ett internationellt standardiseringsorgan,

b) europeisk standard: en standard som antagits av en europeisk standardiseringsorganisation,

c) harmoniserad standard: en europeisk standard som antagits på grundval av kommissionens begäran för tillämpningen av unionens harmoniseringslagstiftning,

d) nationell standard: en standard som antagits av ett nationellt standardiseringsorgan.

Med *specifikation* avses en teknisk specifikation i den mening som avses i artikel 2.4 i förordning (EU) nr 1025/2012. Där definieras specifikation som ett dokument som föreskriver de tekniska krav som en produkt, process, tjänst eller ett system ska uppfylla och som fastställer ett eller flera av följande:

[6] 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.

a) De egenskaper som krävs av en produkt, exempelvis i fråga om kvalitetsnivåer, prestanda, interoperabilitet, miljöskydd, hälsa, säkerhet eller dimensioner, och inbegripet sådana krav som avser varubeteckning, terminologi, symboler, provning och provningsmetoder, förpackning, märkning eller etikettering samt förfaranden för bedömning av överensstämmelse.

b) Produktionsmetoder och processer för de jordbruksprodukter som definieras i artikel 38.1 i EUF-fördraget, för produkter avsedda att konsumeras av människor eller djur samt läkemedel, liksom produktionsmetoder och processer för andra produkter om de påverkar dessa produkters egenskaper.

c) De krav som ställs på en tjänst, inklusive kvalitetsnivåer, prestanda, interoperabilitet, miljöskydd, hälsa eller säkerhet, och inbegripet krav på leverantören om att ställa uppgifter till tjänstemottagarnas förfogande i enlighet med artikel 22.1–22.3 i direktiv 2006/123/EG[7].

I och med att säkerhetsproblem som påverkar nätverk och informationssystem är globala till sin natur behövs ett närmare internationellt samarbete för att förbättra säkerhetstandarder och informationsutbyte och för att främja ett gemensamt sätt att hantera säkerhetfrågor (skäl 43).

För att säkerställa en enhetlig tillämpning av säkerhetsåtgärder bör medlemsstaterna främja efterlevnad eller överensstämmelse med specificerade standarder för att garantera en hög nivå på säkerheten i nätverk och informationssystem på unionsnivå. Enisa bör bistå medlemsstaterna genom rådgivning och riktlinjer (skäl 66).

Kontaktpunkt mot Enisa i dessa frågor bör vara MSB. Detta bör ingå i uppdraget som företrädare i samarbetsgruppen. Detta påverkar dock inte de befintliga samarbeten som Post- och telestyrelsen och andra tillsynsmyndigheter har med Enisa.

I den nya förordningen ska det tas in en bestämmelse som att europeiska eller internationellt accepterade standarder och specifikationer bör beaktas vid utformningen av säkerhetsåtgärder.

[7] Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden.

MSB bör vid behov ta fram riktlinjer och vägledningar om tillämpning av standarder och specifikationer som kan användas för att utforma säkerhetssåtgärder. Tillsynsmyndigheterna ska stödja MSB i detta arbete genom att vid behov redovisa befintliga standarder och specifikationer eller behov av nya standarder och specifikationer.

Frivillig rapportering

Enheter som inte har identifierats som leverantörer av samhällsviktiga tjänster eller är leverantörer av digitala tjänster ska, på frivillig grund, ges möjlighet att rapportera incidenter som har en betydande inverkan på kontinuiteten i de tjänster som de tillhandahåller eller andra incidenter. Vid behandlingen av rapporter ska medlemsstaterna agera i enlighet med det förfarande som fastställs för incidentrapportering för leverantörer av samhällsviktiga tjänster. Medlemsstaterna får ge behandling av obligatoriska rapporter företräde framför behandling av frivilliga rapporter. Frivilliga rapporter ska endast behandlas om behandlingen inte utgör en oproportionell eller orimlig börda för de berörda medlemsstaterna. En frivillig rapport får inte leda till att den rapporterande enheten åläggs skyldigheter som den inte skulle ha varit föremål för om den inte hade gett in rapporten. (artikel 20)

Rapportering ska endast ske om dessa enheter anser att det ligger i allmänhetens intresse att rapportera förekomsten av sådana incidenter till CSIRT-enheten (skäl 67).

Utredningens bedömning är att det kan finnas skäl att även andra leverantörer ska kunna rapportera incidenter enligt det förfarande som gäller för leverantörer av samhällsviktiga tjänster och digitala tjänster. Det skulle t.ex. kunna vara incidenter i nätverk och informationssystem inom enheter som fjärrvärme eller tjänster i andra sektorer som bedöms som samhällsviktiga för svenskt vidkommande. Behandlingen av obligatoriska incidenterapporter ska dock ges företräde. MSB föreslås få rollen som CSIRT-enhet och bör i denna egenskap även undersöka vilka samhällsviktiga tjänster som inte omfattas av NIS- direktivet men där det kan vara relevant att ge möjlighet till frivillig rapportering.

Närmare föreskrifter om frivillig incidentrapportering bör därför meddelas genom myndighetsföreskrifter enligt ett bemyndigande i den nya förordningen. Utredningens bedömning är att MSB ska meddela dessa. Tillsynsmyndigheterna ska ges tillfälle att lämna synpunkter på föreskrifterna.

8 Tillsyn

8.1 Inledning

Varje medlemsstat ska enligt NIS-direktivet utse en eller flera nationella behöriga myndigheter för säkerhet i nätverk och informationssystem för åtminstone de sektorer som avses i bilaga 2 och de tjänster som avses i bilaga 3 till NIS-direktivet. De behöriga myndigheterna ska övervaka tillämpningen av direktivet på nationell nivå (artikel 8.1–2).

Utredningen ska lämna förslag på ett system för tillsyn i enlighet med direktivets krav.

I kommittédirektiven anges att befintliga myndigheter bör behålla eller komplettera sina nuvarande roller. Myndigheten för samhällsskydd och beredskap (MSB) bör, mot bakgrund av sitt ansvar att samordna arbetet med samhällets informationssäkerhet, få en samordnande roll mellan tillsynsmyndigheterna i syfte att få en samlad bild över EU-direktivets genomförande och tillämpning i Sverige. Detta ska dock inte medföra något övertagande av sektorsmyndigheternas ansvar för tillsyn över aktörer eller något mandat att styra hur dessa myndigheter ska använda sina resurser.

Utgångspunkten bör därför vara att tillsynsmyndigheterna inom de sektorer som omfattas av NIS-direktivet även fortsättningsvis har kvar ansvaret för att kontrollera att aktörerna följer respektive sektors regler om informationssäkerhet.

För de sektorer där det i dag saknas tillsyn över informationssäkerhet behöver det övervägas vilken myndighet som kan anförtros den uppgiften. Inriktningen bör enligt kommittédirektiven vara att Post- och telestyrelsen (PTS) ges fortsatt och vid behov kompletterande ansvar för tillsyn av de digitala infrastrukturer som nämnas i bilaga 2 till NIS-direktivet.

8.2 Allmänt om tillsyn

8.2.1 Generella utgångspunkter för reglering om tillsyn

Vid genomförandet av NIS-direktivets bestämmelser om tillsyn finns det anledning att beakta de principiella bedömningar som gjorts i fråga om tillsyn. I regeringens skrivelse till riksdagen, *En tydlig, rättsäker 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 bl.a. 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 ha möjlighet att ålägga den som är objektsansvarig ansvar för att utöva egen kontroll av sin verksamhet. Enligt skrivelsen bör samtliga ingripanden kunna överklagas. Ett viktigt skäl för att precisera tillsynsbegreppet anges vara att en tydlig definition gör det enklare att skilja granskandet 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

[1] Skr. 2009/10:79, bet. 2009/10:FiU12.

rätt, även rekommendationer och vägledning ska vara en del av tillsynen.

8.2.2 Annan reglering

Det finns bestämmelser i förvaltningslagen (1986:223) och myndighetsförordningen (2007:515) som ska beaktas av den som utövar tillsyn.

Förvaltningslagen

Varje myndighet ska lämna andra myndigheter hjälp inom ramen för den egna verksamheten 6 § förvaltningslagen.

Myndighetsförordningen

Myndigheten ska verka för att genom samarbete med myndigheter och andra ta tillvara de fördelar som kan vinnas för enskilda samt för staten som helhet (6 § andra stycket myndighetsförordningen).

Myndigheten ska se till att de kostnadsmässiga konsekvenserna begränsas när den begär in uppgifter eller utövar tillsyn (19 § myndighetsförordningen).

8.3 Tillsyn enligt NIS-direktivet

8.3.1 Syftet med tillsyn enligt NIS-direktivet

Det övergripande syftet med de åtgärder som fastställs i NIS-direktivet är att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen för att förbättra den inre marknadens funktion.

Syftet med åtgärden tillsyn är att kunna bedöma hur leverantörerna av samhällsviktiga tjänster uppfyller säkerhetskraven och kraven på incidentrapportering samt bedöma vilka effekter direktivets krav får på säkerheten i nätverk och informationssystem.

När det gäller leverantörer av digitala tjänster ska tillsyn utövas i efterhand när tillsynsmyndigheten fått bevis på att leverantören inte

vidtagit de säkerhetsåtgärder som leverantören själv ställt upp som krav för att säkerställa att nivån på säkerheten är lämplig. Tillsynsmyndigheten ska på begäran av behöriga myndigheter i andra medlemsstater kunna bistå med tillsynsåtgärder.

Resultatet från en tillsyn kan ligga till grund för sanktioner och förelägganden om att avhjälpa brister.

8.3.2 Befogenheter

Tillsynsmyndigheternas rätt att utföra kontroller och kräva information

Tillsynsmyndigheterna ska ha de befogenheter och medel de behöver för att bedöma om leverantörer av samhällsviktiga tjänster uppfyller sina skyldigheter enligt artikel 14 i NIS-direktivet samt vilka effekter åtgärderna får på säkerheten i nätverk och informationssystem.

Tillsynsmyndigheterna ska också ha de befogenheter och medel som krävs för att ålägga leverantörer av samhällsviktiga tjänster att tillhandahålla

a) den information som är nödvändig för att bedöma säkerheten i deras nätverk och informationssystem, inbegripet dokumenterade säkerhetsprinciper,

b) bevis för ett effektivt genomförande av säkerhetsprinciper, såsom resultaten av en säkerhetsrevision utförd av tillsynsmyndigheten eller en auktoriserad revisor och, i det senare fallet, att ge tillsynsmyndigheten tillgång till resultaten, inklusive de underliggande bevisen.

När tillsynsmyndigheten begär sådan information eller sådana bevis ska den uppge syftet med begäran och precisera vilken information som krävs (artikel 15.1–3).

När det gäller leverantörer av digitala tjänster ska tillsynsmyndigheten vid behov utöva tillsyn i efterhand när myndigheten mottagit bevis på att en leverantör inte uppfyllt kraven i artikel 16 i NIS-direktivet. Sådana bevis får läggas fram av en behörig myndighet i en annan medlemsstat där tjänsten tillhandahålls (artikel 17.1.) Tillsynsmyndigheten har ingen allmän skyldighet att utöva tillsyn över leverantörer av digitala tjänster.

Tillsynsmyndigheten ska ha de befogenheter och medel som krävs för att ålägga leverantörer av digitala tjänster att tillhandahålla den information som behövs för en bedömning av säkerheten i deras nätverk och informationssystem, inbegripet dokumenterade säkerhetsprinciper.

Åläggande att vidta åtgärder

Tillsynsmyndigheten ska kunna utfärda bindande anvisningar till leverantörer av samhällsviktiga tjänster om hur de ska avhjälpa identifierade brister (artikel 15.3).

Tillsynsmyndigheten ska ha de befogenheter och medel som krävs för att ålägga leverantörer av digitala tjänster att åtgärda varje underlåtenhet att uppfylla kraven i artikel 16 (artikel 17.2). Frågan om förelägganden att vidta åtgärder behandlas i avsnitt 9.5.

Sanktioner

NIS-direktivet ålägger medlemsstaterna att fastställa regler om sanktioner för överträdelse av nationella bestämmelser som har antagits enligt direktivet och vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska anmäla dessa regler och åtgärder till kommissionen senast den 9 maj 2018 samt utan dröjsmål eventuella ändringar som berör dem (artikel 21). Frågan om ingripanden och sanktioner behandlas i kapitel 9.

8.3.3 Samordning och informationsutbyte

Samarbete på nationell nivå

Tillsynsmyndigheterna och den nationella kontaktpunkten (MSB) ska, när så är lämpligt och i överensstämmelse med nationell rätt, samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna och Datainspektionen (artikel 8.6). Tillsynsmyndigheterna ska vidare samarbeta med CSIRT-enheten (MSB) när det gäller fullgörandet av NIS-direktivet (artikel 10.1). Tillsynsmyndigheterna, nationell kontaktpunkt och CSIRT-enhet ska också samarbeta på

ett effektivt och säkert sätt i samarbetsgruppen (artikel 8.5). Det innebär bland annat att tillsynsmyndigheterna ska lämna stöd till Sveriges representant i samarbetsgruppen, MSB, se avsnitt 11.3.

Krav på samordning med Datainspektionen

Säkerheten för personuppgifter undergrävs ofta till följd av incidenter. Tillsynsmyndigheterna ska därför ha ett nära samarbete med dataskyddsmyndigheterna innan de utfärdar anvisningar om hur incidenter ska avhjälpas om incidenten också medför personuppgiftsincidenter Det innebär t.ex. att samarbeta och utbyta information om alla relevanta frågor för att hantera personuppgiftsincidenter till följd av incidenter. (artikel 15.4 och skäl 63)

Dataskyddsmyndigheter är i den nya lagen och den nya förordningen Datainspektionen. Frågan om samordning med Datainspektionen behandlas i avsnitt 9.5.

Informationsutbyte med tillsynsmyndigheter i andra medlemsstater

Om en leverantör av digitala tjänster har sitt huvudsakliga etableringsställe eller en företrädare i en medlemsstat, men dess nätverk och informationssystem är belägna i en eller flera andra medlemsstater, ska den tillsynsmyndigheten i den medlemsstat där det huvudsakliga etableringsstället eller företrädaren finns och de tillsynsmyndigheterna i dessa andra medlemsstater samarbeta och vid behov bistå varandra. Detta bistånd och samarbete får omfatta informationsutbyte mellan de berörda tillsynsmyndigheterna och begäranden om att vidta tillsynsåtgärder (artikel 17.3). Frågan om informationsutbyte med tillsynsmyndigheter i andra medlemsstater behandlas i avsnitt 8.5.3.

8.4 System för tillsyn

8.4.1 Befintliga system för tillsyn när det gäller säkerhetsåtgärder

Tillsyn enligt säkerhetsskyddslagstiftningen

Enligt säkerhetsskyddslagstiftningen finns två huvudansvariga tillsynsmyndigheter, Säkerhetspolisen och Försvarsmakten, som i samråd med sektorsansvariga myndigheter (Affärsverket svenska kraftnät, Post- och telestyrelsen, Transportstyrelsen och länsstyrelsen) även kan utöva tillsyn över sektorns myndigheter. Sektorsmyndigheterna utövar också egen tillsyn sektorn. Samtliga tillsynsmyndigheter har föreskriftsrätt.

Formerna för tillsynen av säkerhetsskyddet avviker i flera avseenden från de redovisade principiella bedömningarna om hur tillsyn bör utformas. I tillsynsmyndigheternas uppgifter ligger bland annat att kontrollera att myndigheter och andra verksamheter som säkerhetsskyddslagen gäller för, följer reglerna om säkerhetsskydd och att säkerhetsskyddet är tillräckligt för den verksamhet som bedrivs. Tillsynen utövas bl.a. genom besök och uppföljning varvid eventuella brister och behov av åtgärder påpekas. Någon sanktion finns inte. Tillsynen utgår från att de verksamheter som berörs av lagstiftningen samarbetar med de myndigheter som kontrollerar säkerhetsskyddet och självmant vidtar de åtgärder som rekommenderas. Säkerhetspolisens, Försvarsmaktens och de övriga tillsynsmyndigheternas rådgivande och stödjande funktioner i fråga om säkerhetsskyddet är också tydligt uttalade.

I betänkandet *En ny säkerhetsskyddslag* (SOU 2015:25) s. 476 ff. görs en analys avseende behovet av förändring när det gäller utformningen av tillsyn i säkerhetsskyddslagen. Att tillsynen av säkerhetsskyddet i viktiga avseenden avviker från principiella riktlinjer för hur tillsyn bör utformas skulle kunna tala för att en genomgripande förändring behövs. Det är dock viktigt, som också skrivelsen[2] ger uttryck för, att utgå från de förutsättningar som gäller för det specifika tillsynsområdet. I skrivelsen anförs att det inte går att bortse från att många tillsynsområden har väsentligt olika förutsättningar som påverkar hur tillsynsregelverket bör utformas för att effektivt

[2] Skr. 2009/10:79.

bidra till att de materiella reglerna efterlevs och intentionerna i regelverken förverkligas. Faktorer som kan behöva vägas in är bland annat vem som bedriver den verksamhet som tillsynen avser, vilket slag av verksamhet som tillsynen riktas mot, vilka risker regelöverträdelser kan orsaka och hur det materiella regelverk som tillsynen avser är utformat. Vidare framhålls att det måste beaktas att tillsyn är kostnadskrävande och orsakar störningar och påfrestningar för den som kontrolleras. Mot den bakgrunden betonas att det vid tillskapande eller översyn av regelverk för tillsyn även är väsentligt att överväga andra styrformer, till exempel ekonomiska incitament, information eller utvärdering, för att uppnå regelverkets mål.

En väsentlig faktor är vilka organ som bedriver den verksamhet som tillsynen avser. De verksamheter som berörs av tillsynen av säkerhetsskyddet utgörs främst av myndigheter och andra former av allmän verksamhet, bl.a. vissa företag med statligt ägande. Exempel på sådana företag som bedriver säkerhetskänslig verksamhet är Vattenfall, TeliaSonera och SOS Alarm. Andra enskilda företag berörs av tillsynen främst i egenskap av anbudsgivare och leverantörer. Det kan handla om till exempel företag inom säkerhets- och försvarsmaterielområdet eller om företag som tillhandahåller it- och telekommunikationslösningar. Därutöver berörs också enskilda företag som bedriver verksamhet som är att anse som säkerhetskänslig, till exempel företag vars verksamhet har väsentlig betydelse för landets elförsörjning.

I fråga om enskilda verksamheter bör, enligt betänkandet, beaktas att för det fall att det rör sig om säkerhetsskyddad upphandling, så innebär avtalsförhållandet i sig att det finns ett incitament för en leverantör att leva upp till krav på säkerhetsskydd för att behålla sin position som leverantör på området. I förarbetena till säkerhetsskyddslagen tas också upp att det finns möjlighet att i säkerhetsskyddsavtalen ta in klausuler om skadestånd, vite och hävningsrätt.

Samhällsutvecklingen medför att säkerhetskänslig verksamhet i högre grad än tidigare bedrivs av enskilda. En rimlig slutsats, enligt betänkandet, bör kunna vara att omfattningen av enskilda verksamhetsformer troligen kommer att öka inom tillsynsområdet men att det även i fortsättningen i avsevärd utsträckning handlar om tillsyn av myndigheter och andra offentliga organ. I fråga om enskilda verksamheter måste vidare beaktas att en anledning till att de i högre grad berörs av säkerhetsskyddslagstiftningen är utvecklingen i fråga

om användandet av externa leverantörer. I sådana situationer finns som nämnts andra incitament än sanktioner vid tillsyn för att uppfylla krav på säkerhetsskydd.

En annan faktor som tas upp i regeringens skrivelse och som kan påverka bl.a. vilka befogenheter tillsynsorganen behöver är vilket slag av verksamhet som tillsynen riktas mot. Det exemplifieras med de skilda förutsättningar som gäller vid tillsyn mot fysiska objekt, till exempel livsmedelslokaler och mer svårgreppbar verksamhet, till exempel försäkringsverksamhet. I fråga om säkerhetsskydd handlar det inte om ett homogent slag av verksamheter utan om verksamheter av vitt skilda slag. Det underlättar inte ett utformande av lämpliga ingripandebefogenheter.

Ytterligare en annan faktor som tas upp i skrivelsen i fråga om styrning av ett regelverks efterlevnad är vilka risker regelöverträdelser kan orsaka. Regelöverträdelser som innebär risker för exempelvis människors liv och hälsa anges påverka såväl utformning av sanktioner som behovet av en enhetlig tillsyn över hela landet. Det anges även kunna innebära att tillsynen i viss utsträckning ges en förebyggande inriktning. Säkerhetsskydd tar sikte på att förebygga allvarliga konsekvenser till följd av hot mot Sveriges säkerhet. En förebyggande inriktning är enligt betänkandet därför given. Av betydelse är också hur det materiella regelverk som lagstiftningen ska utövas från är utformat. Inom många tillsynsområden finns ett omfattande och detaljerat materiellt regelverk som utgör grund för tillsynen. Vanligen råder heller ingen tvekan om vilka tillsynsobjekten är, dvs. vilka verksamheter som omfattas av det materiella regelverket. För säkerhetsskyddet gäller enligt betänkandet det motsatta. Säkerhetsskyddslagen är utformad på ett sätt som ger den verksamhetsansvarige ett stort ansvar och bedömningsutrymme i fråga om att såväl avgöra lagens tillämplighet som att bestämma hur ett för verksamheten väl anpassat säkerhetsskydd ska åstadkommas. Det innebär svårigheter i fråga om ingripandemöjligheter som förutsätter tydlighet och precision rörande de brister som behöver åtgärdas.

Ett annat förhållande som är viktigt att beakta enligt betänkandet är att lagstiftningens karaktär medför att det finns ett stort behov av vägledning och stöd till de verksamheter som har att tillämpa säkerhetsskyddslagen. Särskilt i förhållande till enskilda är behovet av råd och stöd framträdande. Det behovet kommer antagligen inte att minska med en reformerad säkerhetsskyddslag. Mot den bak-

grunden förefaller det rimligt att anta att lagens genomslag i relativt hög grad även i fortsättningen kan komma att vara beroende av att de myndigheter som har ett särskilt ansvar för säkerhetsskyddet på olika sätt kan vägleda och stödja de säkerhetskänsliga verksamheterna i en tillräcklig omfattning. Flera av experterna i utredningen om säkerhetsskyddslagen framhöll att det är viktigt att tillsynen i fråga om säkerhetsskydd utgår från samverkan och ger utrymme för en dialog mellan myndighet och den verksamhet som berörs av tillsynen. Det var också utredningens uppfattning att det överlag inom säkerhetsskyddsområdet är viktigt att det finns goda förutsättningar för samverkan mellan myndigheter och enskilda verksamheter. Om brister i säkerhetsskyddet skulle kunna medföra åtgärder som till exempel varningar och vitessanktionerade åtgärdsförelägganden, kan det också få till följd att benägenheten att på eget initiativ ta upp brister med den myndighet som kontrollerar säkerhetsskyddet kan påverkas negativt. Utredningen om säkerhetsskyddslagen såg en betydande risk att sådana inslag skulle kunna medföra att värdefullt erfarenhetsutbyte, till exempel i fråga om säkerhetshotande incidenter, mellan de verksamheter som kontrolleras och de myndigheter som utövar tillsynen motverkas.

Några av experterna i utredningen om säkerhetsskyddslagen framförde, utifrån erfarenheter av den nuvarande ordningen, att det finns en svårighet med att förena en rådgivande och kontrollerande roll. Sådana dubbla roller är svåra att undvika utan att göra stora förändringar av myndigheternas ansvar och uppgifter. Antagligen skulle motsättningen upplevas som större om säkerhetsskyddet förändrades mot sådana tillsynsformer där ingripandebefogenheter är i fokus. Det vore olyckligt med en utveckling mot att myndigheter som utövar tillsyn är så restriktiva i sin rådgivning att det innebär ett försämrat säkerhetsskydd.

Utredningen om säkerhetsskyddslagen anförde bland annat att formerna för tillsynen av säkerhetsskyddet avviker i väsentliga avseenden från de generella riktlinjerna för hur offentlig tillsyn bör ordnas. Ingripandebefogenheter vid tillsyn är av betydelse. I dag finns inte sådana befogenheter i fråga om säkerhetsskyddet. Sammantaget gjorde utredningen om säkerhetsskyddslagen bedömningen att det för närvarande inte finns tillräckliga skäl för att förändra tillsynens inriktning och genomförande. Något förslag om att införa sanktioner lämnades därför inte. Utredningen pekade dock på att det är ange-

läget att noga följa utvecklingen och inom en inte alltför avlägsen framtid följa upp frågan. I detta sammanhang nämns bl.a. NIS-direktivet. I betänkandet föreslås att grunddragen i den nuvarande tillsynsorganisationen behålls.

- Säkerhetspolisen och Försvarsmakten har huvudansvaret för tillsynen.
- När det gäller bolag, föreningar, stiftelser och enskilda näringsidkare utövas kontrollen av de säkerhetsskyddsstödjande myndigheterna (Affärsverket svenska kraftnät för elförsörjningsverksamhet, Post- och telestyrelsen för verksamhet som avser elektronisk kommunikation, Transportstyrelsen för flygtransportverksamhet och i övrigt Myndigheten för samhällskydd och beredskap som också utövar kontroll över kommuner och landsting). Även på dessa områden kan dock säkerhetsskyddet kontrolleras av Säkerhetspolisen och Försvarsmakten. Kontrollen ska i så fall utföras i samråd med den primärt ansvariga myndigheten.

Ett flertal myndigheter har således ett särskilt ansvar för säkerhetsskyddet. Det förhållandet i sig kan givetvis göra ansvar och roller otydliga. Utredningen om säkerhetsskyddslagens direktiv fann inte skäl för någon genomgripande förändring av den ordningen. Tvärtom framhölls att det är viktigt att den samlade kompetens som finns hos de myndigheter som har till uppgift att kontrollera säkerhetsskyddet kan användas på ett effektivt sätt.

På samma sätt som i fråga om behovet av sanktioner anförde utredningen om säkerhetsskyddslagen att det var viktigt att frågan om tillsynsorganisation följs upp när en ny lag har varit i kraft en tid. Om sanktioner övervägs, är det inte självklart att tillsynen bör organiseras på samma sätt som i dag.

System enligt personuppgiftslagstiftningen

Det nu gällande dataskyddsdirektivet föreskriver att varje medlemsstat ska ha en eller flera tillsynsmyndigheter som ska övervaka tillämpningen av de nationella bestämmelser som antagits till följd av direktivet. Tillsynsmyndigheten ska ha vissa angivna uppgifter och

befogenheter. I Sverige är Datainspektionen denna myndighet[3]. Datainspektionen har det övergripande, ansvaret för tillsynen över behandling av personuppgifter. Tillsynsuppdraget är brett och Datainspektionen är behörig att utöva tillsyn över all personuppgiftsbehandling. Tillsynen avser både sådan behandling som regleras av personuppgiftslagen och sådan som omfattas av särskilda registerlagar med avvikande eller kompletterande bestämmelser. Härutöver har några ytterligare myndigheter i uppdrag att utöva tillsyn över behandling av personuppgifter inom vissa särskilt angivna områden, till exempel Säkerhets- och integritetsskyddsnämnden och Post-och telestyrelsen.

Utformningen av Datainspektionens behörighet innebär att det inte finns några ”luckor” i tillsynen över behandlingen av personuppgifter. Det finns med andra ord inte någon personuppgiftsbehandling som inte omfattas av någon myndighets tillsynsbefogenhet. Om inte någon annan myndighet utövar tillsyn kan Datainspektionen alltid göra det. Datainspektionen avgör själv när det finns anledning att inleda ett tillsynsärende. Beslutet kan grunda sig på exempelvis iakttagelser vid ett annat tillsynsärende, en beslutad tillsynsplan, ett tips från massmedia eller andra myndigheter och klagomål från enskilda. Tillsyn kan också initieras efter en anmälan från ett personuppgiftsombud. Datainspektionen tar emot klagomål från enskilda som anser att de har varit föremål för en felaktig personuppgiftsbehandling men är inte skyldig att inleda ett tillsynsärende på grund av en gjord anmälan. Alla som klagar får dock ett besked i någon form från Datainspektionen.

System inom transportsektorn

Transportstyrelsen har ansvaret för merparten av all normgivning, tillståndsgivning, tillsyn och registerhållning för de fyra trafikslagen. Transportstyrelsen inrättades den 1 januari 2009 samtidigt som Luftfartsstyrelsen och Järnvägsstyrelsen lades ner.

Statens haverikommission har till uppgift att från säkerhetssynpunkt utreda alla typer av allvarliga civila eller militära olyckor och tillbud, oavsett om de inträffar till lands, till sjöss eller i luften.

[3] 2 a § förordningen (2007:975) med instruktion för Datainspektionen.

En trafikslagsövergripande myndighet

Motiven för en trafikslagsövergripande myndighet angavs i prop. 2008/09:31 för det första vara vikten av att en effektiv och tillförlitligt genomförd tillsyn kan garanteras inom alla trafikslag. En förutsättning för detta ansågs vara att det råder ett oberoende mellan det organ som utövar tillsynen och den verksamhet som tillsynen avser. För det andra konstaterades att tillsynen var splittrad och svåröverskådlig inom många områden. Det påpekades att det i budgetpropositionen för 2008 framhölls att en väl fungerande tillsyn är avgörande för den rättssäkerhet som tillsammans med effektivitet och medborgarorientering ska vara utpekande för statsförvaltningen. Vidare bedömdes att behovet av en optimal tillsyn ökade i takt med den ökade delegeringen av offentliga åtaganden, driften av offentlig verksamhet i privat regi, avregleringen av flera marknader liksom Sveriges EU-medlemskap. Regeringen bedömde därför att en myndighet med ett samlat tillsynsansvar på ett avgörande sätt skulle komma att bidra till en utveckling i enlighet med det nu sagda. Den tredje aspekten som beaktades var det faktum att dagens transporter och resor ofta sker med flera olika trafikslag inblandade. Likformighet och likabehandling mellan trafikslagen när det gäller tillsyn och normgivning – i den grad det är möjligt – ansågs därför vara önskvärda. I en samlad verksamhet, där jämförelser av erfarenheter kan ske och nytta dras av resultaten, ansågs förutsättningarna för att uppnå dessa mål öka. Vidare bedömdes att effektivitet skulle uppnås även inom den administrativa verksamheten genom att denna skulle ske sammanhållet för en större myndighetskropp. Ett viktigt krav för att en korrekt och trovärdig tillsyn kan garanteras ansågs också vara att det råder ett oberoende mellan den organisation som utövar tillsyn och den verksamhet som tillsynen avser. Regeringens uttalade vidare att det var såväl lämpligt som effektivt att den myndighet som utfärdar föreskrifter inom ett område också har det ansvar och de befogenheter som behövs för att säkerställa att föreskrifterna får avsedd verkan. I utövandet av ansvaret och användandet av befogenheterna förmodades myndigheten därutöver tillägna sig erfarenheter som kan ligga till grund för utformningen av föreskrifterna.

Statskontoret, som fått i uppdrag att följa upp Trafikverkets och Transportstyrelsens verksamhet, har bl.a. anfört följande avseende renodling av roller[4].

> Ett viktigt ledord bakom de senaste årens organisationsförändringar har varit renodling av roller och ansvar mellan transportmyndigheterna. Ansvaret för tillsyn och normgivning har skilts från förvaltarrollen. Vidare har det inom den förvaltande rollen skett en renodling dels genom att produktionsverksamheten har avskilts från förvaltarrollen dels genom att Trafikverket har strävat efter att lägga över ett större åtagande på entreprenörer och konsulter.
>
> Statskontoret kan konstatera att denna utveckling har både för- och nackdelar. Att ansvaret för tillsyn och normgivning har skilts från förvaltarrollen har inneburit bättre förutsättningar för en oberoende tillsyn och normgivning. Transportstyrelsen bör ha lättare än tidigare myndigheter att verka fristående från de olika ”branschkrafterna” då myndigheten inte själv har ansvar för förvaltningen av infrastrukturen. För Trafikverket innebär renodlingen av beställarrollen sannolikt att en mer effektiv infrastrukturproduktion kan organiseras.
>
> För både Transportstyrelsen och Trafikverket innebär dock denna renodling utmaningar i olika avseenden. Som vi har beskrivit riskerar en alltför stark renodling av beställarrollen innebära att Trafikverket förlorar kunskap över väg- och järnvägssystemet. Inom Transportstyrelsen finns det inte några strukturella motverkande krafter till det regleringsarbete som genomförs på det sätt som fanns tidigare. I de tidigare trafikverken, där de reglerande uppgifterna låg inom samma organisation som de förvaltande, fanns det en inbyggd ”naturlig broms” mot alltför ingripande reglering eftersom det kunde påverka myndigheternas förvaltande uppgifter.

System inom hälso- och sjukvården

Inspektionen för vård och omsorg (IVO) bildades den 1 juni 2013 och ansvarar för tillsyn över hälso- och sjukvård, hälso- och sjukvårdspersonal, socialtjänst och verksamhet enligt lagen (1993:387) om stöd och service till vissa funktionshindrade (LSS). IVO har också ansvar för viss tillståndsprövning. IVO har inget ansvar för normgivning.

[4] *På rätt väg? Uppföljning av Trafikverket och Transportstyrelsen* s.145, Statskontoret, 2015:14.

En tillsynsmyndighet för bl.a. hälso- och sjukvård, LSS-verksamhet och socialtjänst

Enligt regeringens uppfattning[5] bör det finnas en tydlig gränslinje mellan å ena sidan kunskapsutveckling, bidragsgivning och normering och å andra sidan tillsyn. En sådan åtskillnad ger störst tydlighet och oberoende och därmed legitimitet åt tillsynsarbetet. En självständig tillsynsmyndighet ger också riksdag och regering bäst förutsättningar att kunna styra tillsynens resurser via anslag till myndigheten. Regeringen bedömde liksom Statskontoret att det inte finns några principiella eller andra hinder för att separera dessa två uppgifter.

En fristående tillsynsmyndighet i form av IVO underlättar också för medborgarna att hitta rätt när de vill framföra klagomål eller anmäla brister som gäller såväl hälso- och sjukvård som socialtjänst och verksamhet enligt LSS. Den kan också bidra till att tillsynen utövas med mer långsiktig planering, tydligare prioriteringar, ett mer strategiskt inriktat arbete och att möjligheter till gemensamma beslut och rapporter skapas, dvs. möjliggör en effektivare tillsyn.

En ny inspektionsmyndighet har enligt regeringens bedömning möjlighet att från början anpassa sina interna styrmodeller, uppföljningssystem och ärendehanteringssystem till de stora ärendevolymerna och sin myndighetsutövande roll. Att från början kunna utveckla en myndighetskultur som grundas på det lagreglerade tillsynsuppdraget innebär enligt regeringens mening betydande fördelar. Detta skulle förbättra möjligheterna att inom myndigheten kunna utveckla en tydlig yrkesroll och utarbeta en strategi för kompetensförsörjningen.

IVO bör även bygga upp lämpliga samarbetsformer med huvudmännen så att inspektionens arbete på bästa möjliga sätt samspelar med huvudmännens kvalitetsansvar. Detta förutsattes kunna ske genom att ett effektivt kunskapsutbyte mellan IVO och Socialstyrelsen kan etableras.

[5] Prop. 2012/13:20 s. 94 ff.

Tillsyn enligt förslag av NISU 2014

I betänkandet *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten* (SOU 2015:23) föreslår NISU 2014 bland annat att tillsynen över den statliga sektorns informationssäkerhet bör samordnas och förstärkas. MSB ska enligt förslaget utöva tillsyn över myndigheternas informationssäkerhetsarbete. I betänkandet konstateras att ett en sådan tillsynsuppgift säkerligen kommer att kräva samverkan med myndigheter i det föreslagna myndighetsrådet. Det är vidare nödvändigt att samordning sker i förhållande till den tillsyn som utövas under säkerhetsskyddslagen för att undvika överlappande tillsynsansvar. Vidare krävs samordning med den tillsyn inom staten avseende informationssäkerhet som sker genom sektorsansvariga myndigheters försorg.

NISU 2014 anförde vidare att ett antal myndigheter vid sidan om Försvarsmakten, Säkerhetspolisen och sektorsmyndigheterna har tillsynsansvar inom informationssäkerhetsområdet, t.ex. Datainspektionen, Finansinspektionen och Strålsäkerhetsmyndigheten. Det är en krävande uppgift som ställer höga krav på expertkompetens. Tillsynsansvaret omfattar alla aspekter av informationssäkerhet, allt från administrativ säkerhet till it-säkerhet och krypto. Det är inte rimligt att kräva eller förutsätta att den bredd och djup i kompetens som krävs ska finnas inom varje tillsynsmyndighet. Betydligt effektivare och mer rationellt vore om tillsynen genomförs i samverkan med en utpekad myndighet som har den djupa kompetens som krävs. Då skulle tillsynsmyndigheten ha ansvaret och kunskapen om föremålet för tillsyn, och samtidigt dra fördel av expertmyndighetens djupa fackkunskaper. Detta bidrar till kvalitet och stabilitet i tillsynen och en jämn tillämpning av informationssäkerhetskraven på tillsynsobjekten. En samordning av stöd till tillsynsverksamheten vore också effektivt sett till både ekonomi och säkerhet.

I betänkandet förslås att MSB ska utöva tillsyn samt utfärda föreskrifter.

8.4.2 Nuvarande reglering i sektorerna

Inom de sektorer som omfattas av NIS-direktivet finns olika system för tillsyn.

8.5 Utredningens överväganden och förslag

8.5.1 En tillsynsmyndighet för varje sektor

Förslag: Den myndighet som regeringen bestämmer ska vara nationell behörig myndighet.

Den nationella behöriga myndigheten ska utöva tillsyn över att lagen och föreskrifter som meddelats i anslutning till lagen följs.

Det ska finnas en nationell behörig myndighet, tillsynsmyndighet, för varje sektor som utövar tillsyn.

Tillsynsmyndigheten ska lämna stöd till representanten i samarbetsgruppen.

Utredningen har i sina överväganden avseende systemet för tillsyn enligt NIS-direktivet utgått från regeringens generella bedömningar av hur en tillsynsreglering bör vara utformad (skr. 2009/10:79) samt från att befintliga tillsynsmyndigheter bör behålla sitt ansvar. I skälen till NIS-direktivet anges att medlemsstaterna bör kunna utse mer än en nationell behörig myndighet med ansvar för att utföra uppgifter som rör säkerheten i de nätverk och informationssystem som används av leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster enligt NIS-direktivet (skäl 30). Medlemsstaterna bör vid behov kunna använda eller anpassa befintliga organisationsstrukturer vid tillämpningen av direktivet (skäl 37).

I dag finns flera olika system för tillsyn inom de sektorer som omfattas av NIS-direktivet och verksamheterna inom sektorerna har i många fall flera olika tillsynsmyndigheter. Vissa tillsynsmyndigheter utövar redan i dag tillsyn över säkerhet i nätverk och informationssystem medan andra har en annan inriktning på tillsynen, se avsnitt 8.4.

Enligt skrivelsen (skr. 2009/10:79) bör man utgå från de förutsättningar som gäller för det specifika tillsynsområdet. I skrivelsen

anförs att det inte går att bortse från att många tillsynsområden har väsentligt olika förutsättningar som påverkar hur tillsynsregelverket bör utformas för att effektivt bidra till att de materiella reglerna efterlevs och att intentionerna i regelverken förverkligas. Faktorer som kan behöva vägas in är bland annat vem som bedriver den verksamhet som tillsynen avser, vilket slag av verksamhet som tillsynen riktas mot, vilka risker regelöverträdelser kan orsaka och hur det materiella regelverk som tillsynen avser är utformat. Vidare framhålls att det måste beaktas att tillsyn är kostnadskrävande och orsakar störningar och påfrestningar för den som kontrolleras.

De verksamheter som kan komma att beröras av tillsyn enligt NIS-direktivet utgörs av statliga myndigheter, kommuner, landsting, statligt och kommunalt ägda bolag samt enskilda företag. När det gäller enskilda företag kan dessa vara etablerade i Sverige eller i en annan medlemsstat. En enhetlig tillsyn i vart fall inom respektive sektorer bör därför vara utgångspunkten.

En annan faktor som bör vägas in är vilket slag av verksamhet som tillsynen riktas mot. De enheter som finns inom de berörda sektorer och delsektorer finns inom sju olika verksamhetsområden. Det rör sig därför om verksamheter av vitt skilda slag såsom vårdgivare, kreditinstitut och registreringsenheter för toppdomäner. Detta talar också för att ha en enhetlig tillsyn inom respektive sektor. Ytterligare en faktor som ska beaktas när man bedömer vilket system som lämpar sig bäst är vilka risker regelöverträdelser kan orsaka. NIS-direktivets syfte är att höja nivån av säkerhet i nätverk och informationssystem för samhällsviktiga tjänster och digitala tjänster. Åtgärderna ska hantera risker samt förebygga och minimera verkningar av incidenter. Det kan också röra sig om incidenter som har gränsöverskridande verkan. Tillsynen bör ha därför även ges en förebyggande inriktning.

Inom de sju sektorer som omfattas av NIS-direktivet finns stora skillnader i omfattning och utformning av det regelverk som tillsynen utövas utifrån. I dag saknas reglering avseende informationssäkerhet i vissa fall och i andra finns tydliga EU-rättsakter på området. Även om den nu föreslagna lagstiftningen utformas på ett enhetligt sätt kommer kraven på säkerhetsåtgärder inom de olika sektorerna att se olika ut beroende på vilken verksamhet som regleras. Detta kommer naturligtvis även att påverka utformningen av tillsynen. Kunskap om verksamheten inom området bör tillmätas stor betydelse men

även kunskap om informationssäkerhet är en viktig komponent för en tillsynsmyndighet.

Enligt utredningens mening bör därför utgångspunkten för tillsynens utformning vara att det ska finnas en tillsynsmyndighet för varje sektor.

Ett system med en tillsynsmyndighet i varje sektor har naturligtvis både för- och nackdelar. Det som talar för detta system är att en sådan tillsynsmyndighet har kunskap om både sektorn och dess reglering. Detta blir särskilt viktigt i de sektorer och delsektorer som redan i dag regleras av nationell lagstiftning eller EU-rättsakter och där en bedömning måste göras om NIS-direktivets krav redan är tillgodosedda genom befintlig reglering. Kunskap om verksamheten minskar också risken för att de krav på säkerhetsåtgärder som finns olika regelverk kommer att motverka varandra. Tillsynsmyndigheten är också redan etablerad inom sektorn och behöver ingen längre förberedelsetid för att påbörja tillsynsverksamheten. En effektiv tillsyn kräver förtroende mellan tillsynsmyndighet och verksamhet vilket också finns i dag enligt uppgift från referensgruppens deltagare. Ett sådan förtroende bygger på långsiktiga relationer samt kunskap och förståelse för verksamheten.

Utredningen ser att det är en fördel att hålla samman normgivning och tillsyn. Leverantörerna omfattas i de flesta fall av såväl nationella regleringar som EU-rättsakter. Inom såväl transportsektorn som bank- och finansmarknadsinfrastruktursektorerna finns väl fungerande struktur med tillsyn och normgivning på en och samma myndighet. Eftersom informationssäkerhet är en del av verksamheten är det särskilt viktigt att erfarenheter från tillsyn och incidenter tas tillvara i föreskriftsarbetet på ett sätt som förbättrar den inre marknadens funktion.

Det som talar emot att utse flera tillsynsmyndigheter är att tillsyn när det gäller säkerhet i nätverk och informationssystem kräver expertkunskap. I dag finns inte den bredd och djup i kompetens som krävs inom alla tillsynsmyndigheter. Utredningen anser att det inom de nu berörda sektorerna är viktigt att höja informationssäkerhetskompetensen och att det därför är rimligt att tillsynsmyndigheterna skaffar den kompetens som krävs. Det kan innebära att man stärker den egna kompensen eller söker hjälp hos alternativt sam-

arbetar med andra tillsynsmyndigheter.[6] Det samarbetsforum som leds av MSB fyller en viktig funktion för att utveckla och stärka kompetensen, se avsnitt 8.5.4. En annan lösning kan vara att anlita konsulter för vissa delar i en tillsyn. Försvarets radioanstalt (FRA) stödjer i dag flera tillsynsmyndigheter i deras tillsynsuppdrag. Det sker inom ramen för FRA:s uppdrag i vilket anges att FRA får lämna stöd till statliga myndigheter och statligt ägda bolag när det gäller informationssäkerhet.[7] Detta stöd är dock förbehållet verksamheter som hanterar information som bedöms vara känslig från säkerhetssynpunkt eller i ett säkerhets- och försvarspolitiskt avseende.

Det går också att argumentera för att välja ett system med en tillsynsmyndighet som utövar tillsyn över NIS-direktivets tillämpning. Enligt utredningens mening finns dock i dag ingen självklar myndighet som skulle kunna utses till en sådan tillsynsmyndighet. NISU 2014 föreslår att MSB ska få ett liknade ansvar när det gäller statliga myndigheter tillsammans med sektorsmyndigheterna. Även i ett sådant system krävs dock samverkan. Samverkan behöver då ske med sektorsmyndigheterna och andra tillsynsmyndigheter. NISU 2014 hänvisar också till vad som anförs i Riksrevisionens rapport *Informationssäkerheten i den civila statsförvaltningen* (RiR 2014:23) när det gäller att agera i rollen som i tillsynsmyndighet. I rapporten uttalas följande.[8]

> MSB har ett omfattande uppdrag att stödja samhällets informationssäkerhet, men har inget uppdrag att utöva tillsyn. MSB är därför till stor del beroende av att aktörer lämnar uppgifter frivilligt. Den nätverksstruktur som MSB delvis grundar sin informationsinhämtning på ger enligt Riksrevisionen en insyn i vilka problem och hot som finns mot samhället i stort. Sättet att inhämta informationen kan dock innebära svårigheter för MSB att agera mot myndigheter och företag som deltar i informationsutbytet, eftersom agerandet kan riskera förtroendet och därmed grunden för informationsinsamlingen.

Utredningen konstaterar också att det med hänsyn till den korta tid som utredningen har till sitt förfogande samt att NIS-direktivet ska vara genomfört i svensk rätt senast den 9 maj 2018 inte är möjligt göra några större förändringar i det mandat som de befintliga till-

[6] 6 § förvaltningslagen (1986:223) och 6 § andra stycket myndighetsförordningen (2007:515).
[7] 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt.
[8] Informationssäkerheten i den civila statsförvaltningen, RiR 2014:23 s. 43.

synsmyndigheterna har, genom att utse en myndighet som utövar tillsyn över samtliga sektorer.

Utredningen har övervägt olika förslag och har funnit att ett system med en tillsynsmyndighet för varje sektor är mest ändamålsenligt för en effektiv tillsyn enligt NIS-direktivet. Tillsynsmyndighetens kunskap om den verksamhet som är föremål för tillsynen och om annan närliggande reglering medför enligt utredningen att det föreslagna systemet bidrar till en effektiv tillsyn samtidigt som tillsynsverksamheten på ett ändamålsenligt sätt bidrar till att höja nivån av säkerhet i nätverk och informationssystem i syfte att förbättra den inre marknadens funktion.

Tillsynsmyndigheterna, den nationella kontaktpunkten och CSIRT-enheten ska också samarbeta på ett effektivt och säkert sätt i samarbetsgruppen (artikel 8.5). Det innebär att tillsynsmyndigheterna ska lämna stöd till Sveriges representant i samarbetsgruppen, MSB, se avsnitt 6.2.2, 7.3.2 och 11.3.3. Detta regleras i den nya förordningen som en uppgift för tillsynsmyndigheterna.

8.5.2 Tillsynsmyndigheter i Sverige

Förslag: Statens energimyndighet ska vara tillsynsmyndighet i energisektorn, Transportstyrelsen i transportsektorn, Finansinspektionen i sektorerna för bankverksamhet och finansmarknadsinfrastruktur, Inspektionen för vård och omsorg för hälso- och sjukvårdssektorn, Livsmedelsverket för sektorn leverans och distribution av dricksvatten samt Post- och telestyrelsen för sektorn digital infrastruktur.

Post- och telestyrelsen ska vara tillsynsmyndighet för samtliga typer av digitala tjänster.

Medlemsstaterna ska utse en eller flera nationella behöriga myndigheter som ska övervaka tillämpningen av NIS-direktivet på nationell nivå (artikel 8.1–2). De nationella behöriga myndigheterna i Sverige ska utöva tillsyn över direktivets genomförande och tillämpning (tillsynsmyndigheter).

Nästa fråga blir då om det finns befintliga tillsynsmyndigheter inom de respektive sektorerna som är lämpliga att utöva tillsyn när det gäller säkerheten i nätverk och informationssystem.

Utredningen har gjort en översiktlig inventering av tillsynsansvaret när det gäller informationssäkerhet inom de sektorer och delsektorer som framgår av bilaga 2 till NIS-direktivet.[9] Inventeringen har gjorts i samverkan med och kvalitetssäkrats av deltagarna i referensgruppen m.fl. Utredningen konstaterar att det inte finns någon tydlig enhetlig struktur som är gemensam för samtliga sektorer. Inom vissa sektorer finns flera tillsynsmyndigheter med olika ansvar, i andra är ansvaret tydligt utpekat och för några enheter saknas tillsynsmyndighet.

Utredningen har därför valt att utgå från de myndigheter som i dag har

- ett tillsynsansvar i sektorn eller i närliggande sektorer även om det i dag inte omfattar tillsyn av informationssäkerhet,
- kunskap om verksamheten i sektorn,
- kunskap om sårbarheter, hot och risker inom sektorn,
- kunskap om befintliga och kommande EU-rättsakter inom sektorn och
- ansvar för att utfärda föreskrifter.

En annan utgångspunkt har varit att tillsynsmyndigheten inte själv ska tillhandahålla tjänster som omfattas av NIS-direktivet.

Utredningen har också utgått från de synpunkter som framförts av deltagarna i referensgruppen. Gruppen har framfört att en tillsynsmyndighet bör ha god kunskap om NIS-direktivet, erfarenhet av tillsynsverksamhet, kompetens inom informationssäkerhetsområdet, branschkunskap, kunna granska både form och innehåll samt vara oberoende. En förutsättning för att tillsynsarbetet ska vara effektivt och också ha en förebyggande verkan är att tillsynsmyndigheten kan skapa förtroendefulla relationer.

Enligt NIS-direktivet ska säkerställas att tillsynsmyndigheterna upprätthåller informella och tillförlitliga kanaler för informationsutbyte (skäl 59).

Mot bakgrund av det som framkommit om befintliga tillsynsmyndigheter inom sektorerna samt de krav som framförts av referens-

[9] Inventeringen finns tillgänglig i ärende dnr Komm2017/00542-1..

gruppen gör utredningen bedömningen att det finns lämpliga myndigheter inom samtliga sektorer.

Utredningen föreslår att tillsynsansvaret fördelas enligt följande.

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	Tillsynsmyndighet
Digitala tjänster	Post- och telestyrelsen

På energiområdet är tillsynsansvaret uppdelat på flera olika myndigheter. Såväl Energimarknadsinspektionen som Statens energimyndighet är tillsynsmyndigheter och har etablerade kontaker med el- och gasbranscherna samt kunskap om verksamheten, sårbarheter, hot och risker inom energiområdet. Ingen av de myndigheterna har något utpekat ansvar för informationssäkerhet inom sektorn. Även Affärsverket svenska kraftnät utövar tillsyn inom sektorn. Verket är dock även en enhet som omfattas av NIS-direktivet.

Energimarknadsinspektionen har framfört att inspektionen bör bli tillsynsmyndighet för delsektorerna el och gas. Dessa delsektorer finns ofta i samma koncern och med samma it-system vilket talar för att den som har ansvaret för el även bör ha samma ansvar för gas. Statens energimyndighet har anfört att en myndighet bör få ansvaret för samtliga delsektorer, el, gas och olja, samt att det bör vara Statens energimyndighet.

Ett samlat ansvar skulle ge bonuseffekter på andra områden t.ex. krisberedskapsarbetet, arbetet med det civila försvaret och säkerhetskyddsarbetet. Utredningen anser att både Energimarknadsinspektionen och Statens energimyndighet skulle vara lämpliga tillsynsmyndigheter men att det mot bakgrund av tillsynsmyndighetens

uppdrag enligt förslagen i den nya lagen med tillhörande förordning är lämpligast och mest kostnadseffektivt att en myndighet utses till tillsynsmyndighet för en sektor. Utredningen anser att Statens energimyndighet bör vara tillsynsmyndighet för energisektorn.

Finansinspektionen och Transportstyrelsen är i dag tillsynsmyndigheter med föreskriftsrätt inom de sektorer som omfattas av NIS-direktivet. Båda myndigheterna har kunskap om verksamheten samt sårbarheter, hot och risker inom sektorn.

IVO är i dag utpekad tillsynsmyndighet för hälso- och sjukvård och ska som en del av tillsynen pröva klagomål mot hälso- och sjukvården och dess personal när det gäller patientsäkerhet. Socialstyrelsen har ansvaret för att utfärda föreskrifter i sektorn och har ett särskilt ansvar för krisberedskap samt är bevakningsansvarig myndighet enligt krisberedskapsförordningen. Socialstyrelsen har i dag inget tillsynsansvar. IVO utfärdar verkställighetsföreskrifter men samverkar med Socialstyrelsen när det gäller föreskriftsarbete som rör tillsynsområdet. Läkemedelsverket utövar tillsyn enligt bestämmelserna om medicintekniska produkter. Dessa bestämmelser riktar sig mot tillverkaren av produkten.

Socialstyrelsen och Sveriges kommuner och landsting har anfört att IVO bör ha tillsynsansvaret enligt den nya lagen enligt den tillsynsstruktur som finns inom sektorn. Utredningen anser att IVO, mot bakgrund av att IVO i dag är utpekad tillsynsmyndighet för sektorn, bör utses till tillsynsmyndighet enligt den nya lagen. Socialstyrelsen bör inledningsvis bistå IVO med stöd i föreskriftsarbetet och när det gäller identifieringen av leverantörer som tillhandahåller samhällsviktiga tjänster. Eftersom det befintliga systemet för tillsyn inom hälso- och sjukvården har en gränslinje mellan å ena sidan kunskapsutveckling, bidragsgivning och normering och å andra sidan tillsyn skulle ett alternativ kunna vara att Socialstyrelsen även när det gäller genomförandet av NIS-direktivet får det normerande ansvaret. Utredningen anser dock att fördelarna med ett enhetligt system och den viktiga samverkan mellan tillsyn, incidenthantering och normering medför att IVO bör vara tillsynsmyndighet.

Livsmedelsverket har i dag inget tillsynsansvar inom sektorn leverans och distribution av dricksvatten men har tillsynsansvar på andra områden. Verket har också en bred kunskap om säkerhetsarbete inom sektorn liksom kunskap om sårbarheter, hot och risker. Kommunerna utövar offentlig kontroll över dricksvattenanläggningar och

kontrollen utövas av den nämnd som fullgör uppgifter inom miljö- och hälsoskyddsområdet. En kommun kan också vara en sådan enhet som omfattas av NIS-direktivet. Länsstyrelserna samordnar kommunernas verksamhet i länet. Utredningen anser att en myndighet, Livsmedelsverket, ska ha tillsynsansvaret.

Post- och telestyrelsen (PTS) har tillsynsansvar enligt lagen om elektronisk kommunikation samt över vissa av de enheter som omfattas av NIS-direktivet. PTS har också kunskap om verksamheten samt om sårbarheter, hot och risker inom sektorn. PTS bör därför utses till tillsynsmyndighet för hela sektorn digital infrastruktur samt digitala tjänster.

I de fall det finns överlappande tillsyn eller tillsyn utövas av två olika myndigheter med stöd av olika bestämmelser finns det inget hinder mot att tillsynen görs i samverkan för att den som är föremål för tillsynen inte ska åsamkas onödiga kostnader, störningar i verksamheten eller andra påfrestningar.

8.5.3 Tillsyn m.m.

Förslag: Vid tillsyn ska en leverantör av samhällsviktiga tjänster tillhandahålla tillsynsmyndigheten

1. den information som är nödvändig för att bedöma säkerheten i leverantörens nätverk och informationssystem, inbegripet dokumenterade säkerhetsprinciper
2. bevis för ett effektivt genomförande av säkerhetsprinciper, såsom resultaten av en säkerhetsrevision utförd av tillsynsmyndigheten eller en auktoriserad revisor och, i det senare fallet, att ge den behöriga myndigheten tillgångtill resultaten, inklusive de underliggande bevisen.

När tillsynsmyndigheten begär sådan information eller bevis ska den uppge syftet med begäran och precisera vilken information som krävs.

Tillsynsmyndigheten ska, i den utsträckning det behövs för tillsynen, ha tillträdesrätt till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av lagen bedrivs.

Tillsynsmyndigheten ska få förelägga den som står under tillsyn att tillhandahålla information i enlighet med skyldigheterna i lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster. Beträffande leverantörer av samhällsviktiga tjänster ska sådant föreläggande få meddelas även när det gäller annan information som behövs vid bedömning av om leverantören uppfyller sina skyldigheter. Ett föreläggande ska få förenas med vite.

Tillsynsmyndigheten ska ha rätt att få verkställighet hos Kronofogdemyndigheten av beslut som avser åtgärder enligt lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster. Då gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet eller avhysning.

Tillsynsmyndigheten ska samarbeta med och vid behov bistå behöriga myndigheter i andra medlemsstater när det gäller tillsynsåtgärder mot leverantörer av digitala tjänster.

Tillsynsmyndigheten ska samarbeta med och bistå tillsynsmyndigheter i andra länder i Europeiska unionen när det gäller tillsynen över leverantörer av digitala tjänster. Detta bistånd och samarbete får omfatta informationsutbyte mellan de berörda behöriga myndigheterna och begäranden om att tillsynsåtgärder beträffande leverantörer av digitala tjänster enligt den nya lagen ska vidtas.

Tillsynsmyndigheten ska lämna vägledning till leverantörerna av samhällsviktiga tjänster vid tillämpningen av lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster och tillhörande förordning.

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. Bakgrunden till förslagen finns i avsnitt 8.3.

För att tillsynsmyndigheten ska kunna utöva en effektiv tillsyn och identifiera brister som behöver åtgärdas, både genom förelägganden och genom nya föreskrifter, ska den ha tillgång till samtliga incidentrapporter för sin sektor. CSIRT-enheten ansvarar för att till respektive tillsynsmyndighet skyndsamt överlämna incidentrapporterna, se avsnitt 11.2.6.

Förelägganden att tillhandahålla information och tillträde till lokal eller liknande som behövs för tillsyn

Om en leverantör av samhällsviktiga tjänster inte samarbetar med tillsynsmyndigheten vid tillsynen bör tillsynsmyndigheten kunna meddela de förelägganden som behövs för att förmå leverantören att tillhandahålla information och ge tillträde till lokaler. Rätten till information och tillträde till lokaler bör givetvis endast avse sådan information och sådant tillträde som behövs i tillsynsverksamheten. För att inte åsamka den objektsansvarige större olägenheter än vad som behövs ska tillsynsmyndigheten precisera vilken information som avses samt uppge syftet med begäran. Ett beslut om föreläggande bör kunna förenas med vite. Besluten ska kunna överklagas, se avsnitt 9.10.

Om en leverantör av samhällsviktiga tjänster vägrar att ge tillsynsmyndigheten tillträde till en lokal eller liknande för undersökning kan tvångsåtgärder behöva användas. Att vidta sådana åtgärder ligger inte inom tillsynsmyndighetens befogenheter. Det finns inte anledning att anta att det kommer finnas risk för hot eller handgripligheter i samband med tillsynen enligt de aktuella bestämmelserna. De eventuella hinder som kan uppstå får i stället antas vara av fysiskt art. Det bör därför inte vara behövligt att förordna om att tillsynsmyndigheten ska ha möjlighet till biträde av Polismyndigheten. Tillsynsmyndigheten bör i stället kunna begära biträde av Kronofogdemyndigheten.

Överväganden och förslag i dessa delar beträffande leverantörer av digitala tjänster finns i avsnitt 10.4.

Överväganden och förslag avseende tillsynsmyndighetens möjlighet att meddela förelägganden om att vidta säkerhetsåtgärder och att incidentrapportera samt om samverkan med Datainspektionen finns i avsnitt 9.5.

Bistånd och samarbete med andra medlemsstater angående tillsynsåtgärder mot leverantörer av digitala tjänster

Om en leverantör av digitala tjänster har sitt huvudsakliga etableringsställe eller en företrädare i en medlemsstat, men dess nätverk och informationssystem är belägna i en eller flera andra medlemsstater, ska den behöriga myndigheten i den medlemsstat där det

huvudsakliga etableringsstället eller företrädaren finns och de behöriga myndigheterna i dessa andra medlemsstater samarbeta och vid behov bistå varandra. Detta bistånd och samarbete får omfatta informationsutbyte mellan de berörda behöriga myndigheterna och begäranden om att leverantören av digitala tjänster ska tillhandahålla information eller åtgärda underlåtenhet att vidta säkerhetsåtgärder eller att incidentrapportera. (artikel 17.3). Tillsynsmyndighetens uppgift i detta avseende bör regleras i förordning.

Tillsynsmyndighetens befogenhet att meddela förelägganden för att förmå leverantören att tillhandahålla information har behandlats ovan. Befogenheten att meddela förelägganden vid underlåtenhet att vidta säkerhetsåtgärder eller att incidentrapportera behandlas i avsnitt 9.5.

Tillsynsmyndighetens uppdrag i det förebyggande säkerhetsarbetet

Mot bakgrund av att syftet med NIS-direktivet är att höja nivån av säkerhet i nätverk och informationssystem anser utredningen att det förebyggande säkerhetsarbetet bör uppmärksammas. Den snabba tekniska utvecklingen, digitalisering, bristande kunskaper om informationssäkerhet samt att det införs en ny reglering innebär att det finns ett stort behov av att leverantörerna kan få tillgång till rådgivning i sitt säkerhetsarbete. Detta har också framhållits av deltagarna i referensgruppen som en viktig del i säkerhetsarbetet.

I MSB:s uppdrag ingår ett övergripande ansvar för samhällets informationssäkerhetsarbete, se avsnitt 11.1.5. MSB har bl.a. gett ut ett stort antal publikationer, vägledningar och allmänna råd till föreskrifter. På webbplatsen Informationssäkerhet.se finns stöd för systematiskt arbete med informationssäkerhet, lagar och regler, kompetensutveckling samt aktuella rapporter och studier. Även CERT.se har en webbplats där det bl.a. finns övergripande information om obligatorisk it-incidentrapportering samt nyhetsrapportering.

Utöver den övergripande information och upplysningar som MSB ger finns behov av en mer anpassad rådgivning inom respektive sektorer utifrån de förutsättningar och den reglering som gäller för sektorn. Utredningen anser att det är tillsynsmyndigheterna som är mest lämpade att ge denna typ av rådgivning. Det kan till exempel avse hur det systematiska informationssäkerhetsarbetet ska bedrivas

men också hur sektorsspecifika föreskrifter ska tillämpas. Rådgivningen avseende systematiskt arbete bör utgå från det generella material som finns på webbsidan informationssäkerhet.se om inte det finns ett ledningssystem som tillämpas inom sektorn.

Både svårigheter att vara objektiv och att hålla isär tillsyn och rådgivning är skäl som talar emot att en och samma myndighet utövar rådgivning och tillsyn. Utredningen delar dock den uppfattning som framförs i betänkandet *En ny säkerhetsskyddslag* (SOU 2015:25) att det går att hålla rådgivningen på en nivå där inte specifika säkerhetsåtgärder föreslås. Tillsynsmyndigheten kan i stället vara ett bollplank där olika åtgärder diskuteras. Då kan tillsynsmyndighetens erfarenheter från hela sektorn tas tillvara liksom kunskap om sektorns reglering avseende informationssäkerhet. Utredningen ser inte att tillsynsmyndigheternas ansvar för rådgivning enligt den nya lagen skapar några oklarheter. Ett liknade system finns inom säkerhetsskyddsområdet sedan många år tillbaka. Vidare bör eventuella otydligheter i lagstiftning och föreskrifter kunna hanteras i det samarbetsforum som utredningen föreslår, se avsnitt 8.5.4.

8.5.4 Samordnad funktion mellan tillsynsmyndigheterna

Bedömning: Myndigheten för samhällsskydd och beredskap ska inom ramen för sitt nuvarande uppdrag

- ha en samlad bild av NIS-direktivets genomförande och tillämpning i Sverige genom att
  - leda ett samarbetsforum där samtliga tillsynsmyndigheter ingår
  - ta emot tillsynsmyndigheternas bedömningar av brister i nätverk och informationssystem m.m.
- tillhandahålla det metodstöd för tillsyn som behövs för en effektiv tillsyn enligt NIS-direktivet.

Utredningen har undersökt behovet av att ha en samordnande funktion mellan tillsynsmyndigheterna. Den samordnande funktionens uppgift skulle enligt kommittédirektiven vara att få en samlad bild över EU-direktivets genomförande och tillämpning i Sverige. För

att få denna bild skulle funktionen behöva få del av samtliga tillsynsrapporter.

I samarbetsforumets uppgifter bör det ingå att diskutera tillsynsmetoder samt övrigt som forumet finner viktigt att samordna när det gäller säkerhet i nätverk och informationssystem.

Samlad bild av NIS-direktivets genomförande och tillämpning

När det gäller att få en samlad bild av direktivets genomförande och tillämpning i Sverige utifrån de tillsyner som genomförs är det enligt utredningens bedömning inte nödvändigt att ha tillgång till samtliga detaljer som finns i en tillsynsrapport. Det kan också ifrågasättas om det är lämpligt att samla samtliga tillsynsrapporter hos en myndighet, särskilt med hänsyn till kravet på konfidentialitet för vissa uppgifter i tillsynsrapporten. Delgivning av tillsynsrapporterna till en samordnande funktion kan också få negativa konsekvenser för tillsynsmyndighetens möjligheter att upprätta förtroliga relationer med de enheter som omfattas av NIS-direktivet eftersom detta innebär att ytterligare en myndighet delges de eventuella brister och sårbarheter som kommit fram i en tillsyn.

En samlad bild av NIS-direktivets genomförande och tillämpning i Sverige erhålls enligt utredningens mening bäst dels genom att MSB får i uppdrag att leda ett samarbetsforum där samtliga tillsynsmyndigheter ingår, dels genom att tillsynsmyndigheterna vid behov lämnar en samlad bedömning av brister i informationssäkerhet i nätverk och informationssystem och andra resultat som kan vara av intresse för tillämpningen av direktivet till MSB. I en samlad bedömning från sektorn kan resultaten från tillsyner analyseras och bearbetas till en nivå som är mer anpassad till syftet att få en samlad bild över NIS-direktivets genomförande och tillämpning i Sverige. Den samlade bedömningen kan också utgöra stöd i MSB:s förebyggande informationssäkerhetsarbete.

Information om brister som upptäcks vid tillsyn liksom svårigheter vid tillämpning och tolkning av direktivet bör framgå av bedömningen eftersom sådan information är viktig för MSB att känna till i sin roll som nationell kontakpunkt, CSIRT-enhet och representant i samarbetsgruppen. Det närmare innehållet i den informa-

tion som tillsynsmyndigheter ska lämna bör MSB och tillsynsmyndigheterna komma överens om.

I uppdraget att leda ett samarbetsforum för samtliga tillsynsmyndigheter bör ingå att uppmärksamma frågor kring tillsynsmetoder och annat som forumet finner viktigt att samordna när det gäller säkerhet i nätverk och informationssystem. Forumet kan t.ex. identifiera behovet av vägledningar och diskutera gemensamma frågor om föreskrifter, säkerhetsåtgärder och incidentrapporter m.m. Samarbetsforumets uppgifter bör också kunna förändras över tid utifrån tillsynsmyndigheternas och MSB:s behov. Ett väl fungerande samarbetsforum bygger på ett aktivt deltagande från både tillsynsmyndigheterna och MSB. Mot bakgrund av att det kan finnas behov av diskussion och erfarenhetsutbyte om skiftande frågor bör inte heller deltagandet i gruppen begränsas till tillsynsmyndigheterna och MSB. Utredningen anser inte att uppdraget ska författningsregleras.

Metodstöd – tillsyn

För att få en enhetlig och effektiv tillsyn när det gäller NIS-direktivet bör tillsynsmyndigheterna i så stor utsträckning det är möjligt använda samma metod. Behov av samordning mellan tillsynsmyndigheterna har också framkommit i diskussioner med deltagarna i referensgruppen. MSB:s övergripande ansvar när det gäller samhällets informationssäkerhet och det arbete som MSB utför i dag har lyfts fram som ett bra exempel på sådant stöd.

Utredningen anser att MSB bör tillhandahålla ett sådant metodstöd. Myndigheten har redan i dag har ett brett uppdrag att stödja samhällets informationssäkerhet och har också en väl uppbyggd nätverksstruktur, en övergripande bild av de problem och hot som finns i samhället samt tillgång till incidentrapporterna. MSB har också genom NIS-direktivet fått flera funktioner som kan ta tillvara erfarenheter från tillsyn i andra medlemsstater.

Under utredningens arbete har frågan om den samordnande funktionen skulle kunna utformas som tillsynsvägledning lyfts fram. Begreppet används inom miljöområdet och definieras i 3 § miljötillsynsförordningen (2011:13) som utvärdering, uppföljning och samordning av operativ tillsyn samt stöd och råd till de operativa tillsynsmyndigheterna. Tillsynsvägledning ska ges i fråga om tillämp-

ningen av miljöbalken, föreskrifter som meddelats med stöd av miljöbalken och EU-förordningar. Statskontoret har på uppdrag av regeringen analyserat den statliga tillsynsvägledningen på miljöområdet.[10]

Utredningen kan konstatera att de centrala myndigheterna med tillsynsvägledningsansvar ska ge tillsynsvägledning inom vissa av sina expertområden, t.ex. ska Affärsverket svenska kraftnät ge tillsynsvägledning i frågor om dammsäkerhet enligt 11 kap. miljöbalken (3 kap. miljötillsynsförordningen). Statskontorets utvärdering visar på att vägledningskompetensen brister och att kompetens som tidigare fanns centralt i dag är mer utspridd och decentraliserad. Statskontoret föreslår bl.a. att den frivilliga samverkan som i dag bedrivs ska utvecklas inom samverkansorganet Miljösamverkan Sverige.

Utredningens bedömning är att de tillsynsmyndigheter som utredningen föreslår är de som närmast kan motsvara de centrala myndigheterna med tillsynsvägledningsansvar. Att peka ut informationssäkerhet som ett sakområde skiljt från det område inom vilket tjänsten tillhandahålls skulle enligt utredningens bedömning snarare motverka NIS-direktivet syfte än att bidra till en hög gemensam nivå av säkerhet. Utredningen menar att tillsynsmyndigheterna besitter den djupa kunskap om verksamheten och om de risker och hot som finns i sektorn. Samtliga har också tillsynskompetens. Den samordning och metodstöd som behövs för en enhetlig tillsyn bedöms inte motsvara det som avses med tillsynsvägledning och ges därför bäst i det samarbetsforum som utredningen föreslår.

8.5.5 Myndighetssamverkan m.m.

Bedömning: I de fall en tillsynsmyndighet inte har tillräcklig kompetens avseende informationssäkerhet bör behovet av sådana resurser kunna tillgodoses genom myndighetssamverkan alternativt genom upphandling av resurser med rätt kompetens.

I utredningsarbetet har det påpekats av både deltagarna i referensgruppen och av utredningens experter att det kan komma att krävas kvalificerad informationssäkerhetskompetens för att kunna utföra

[10] Vägledning till en bättre tillsyn, En utvärdering av tillsynsvägledningen på miljöområdet, 2014:17, Statskontoret.

en effektiv tillsyn särskilt när det gäller att bedöma effekterna av de skyldigheter som åligger leverantörerna av samhällsviktiga tjänster.

Utredningens bedömning är att det kan bli svårt för samtliga tillsynsmyndigheter att initialt upprätthålla en hög specialistkompetens. Utredningen anser dock att det inom de nu berörda sektorerna är viktigt att höja informationssäkerhetskompetensen och att det därför är rimligt att tillsynsmyndigheterna skaffar den kompetens som krävs. Det kan innebära att man stärker den egna kompensen eller söker hjälp hos, alternativt samarbetar med, andra tillsynsmyndigheter.[11] Det samarbetsforum som leds av MSB fyller en viktig funktion för att utveckla och stärka kompetensen och myndighetssamarbetet, se avsnitt 8.5.4.

Utredningen anser vidare att myndighetssamarbete på detta område stärker informationssäkerheten på ett bredare område än NIS-direktivets tillämpningsområde. Det bidrar också till en allmän kompetenshöjning för både tillsynsmyndigheten och den myndighet som lämnar stöd när det gäller informationssäkerhet i samhällsviktiga tjänster och digitala tjänster. Det måste vidare anses ligga i samhällets intresse att använda den expertkompetens som finns på informationssäkerhetområdet för kvalificerade uppgifter utanför den egna myndighetens uppdrag i den utsträckning det är möjligt.

En annan lösning kan vara att anlita en extern konsult eller revisor för att under ledning av tillsynsmyndigheten utföra vissa delar i en tillsyn.

[11] 6 § förvaltningslagen (1986:223) och 6 § andra stycket myndighetsförordningen (2007:515).

9 Ingripanden och sanktioner

9.1 Inledning

I kapitel 8 behandlas tillsynsmyndigheternas befogenheter. Befogenheterna syftar till att säkerställa att berörda aktörer följer de bestämmelser som antas enligt NIS-direktivet. Medlemsstaterna ska emellertid också fastställa regler om sanktioner till följd av överträdelser av bestämmelserna och vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska anmäla dessa regler och åtgärder till kommissionen senast den 9 maj 2018 samt utan dröjsmål eventuella ändringar som berör dem. (artikel 21) I detta avsnitt behandlas frågorna om hur bestämmelser om ingripanden och sanktioner bör utformas.

9.2 Allmänt om ingripanden vid tillsyn

I regeringens skrivelse 2009/10:79, *En tydlig, rättssäker och effektiv tillsyn*, redovisar regeringen generella bedömningar för hur en tillsynsreglering bör vara utformad. När det gäller frågan om tillsyn och sanktioner anges i skrivelsen bland annat följande.

När en tillsynsmyndighet vid sin tillsyn konstaterar en brist behöver myndigheten ha möjlighet att ingripa. Ett ingripande ska vara effektivt och tydligt. Det ska ha inte bara ha ett bestraffande syfte, utan också en framåtsyftande funktion och se till att regler följs i framtiden. Ingripandemöjligheterna bör utformas efter de särskilda förutsättningar som finns inom tillsynsområdet. Om författningsreglerade möjligheter till ingripanden från tillsynsorganets sida saknas kan tillsynens effektivitet minska.

Sanktioner vid tillsyn bör vara proportionerliga i förhållande till de konstaterade bristerna. De olika möjligheter till sanktioner som

är tillgängliga för ett tillsynsorgan bör därför kunna användas vid såväl mindre som mer allvarliga brister i en verksamhet. Ingripandena kan då anpassas till den enskilda situationen. Om det saknas möjlighet till mildare ingripanden kan detta leda till att inget ingripande sker trots en konstaterad brist, eftersom den som utövar tillsynen inte vill vidta en alltför ingripande åtgärd.

Exempel på ingripandemöjligheter är varning, åtgärdsföreläggande (som ska kunna förenas med vite), rättelse på den enskildes bekostnad, återkallelse av tillstånd eller att förbud mot fortsatt verksamhet som inte kräver tillstånd samt sanktionsavgifter.

Det finns ingen rättslig definition av begreppet sanktion. Sanktioner som beslutas av förvaltningsmyndighet i förvaltningsrättslig ordning brukar benämnas administrativa sanktioner. I betänkandet *Vad bör straffas?* (SOU 2013:38) används begreppet administrativa sanktioner som samlad beteckning för sanktionsavgifter, vitesföreläggande och vitesförbud samt återkallelse av tillstånd. Beslut om sådana sanktioner kan överklagas till allmän förvaltningsdomstol.

I svensk rätt skiljs administrativa sanktioner från påföljder för och annan rättsverkan av brott. Sistnämnda frågor prövas i regel inom ramen för ett brottmål i allmän domstol, av åklagare genom strafföreläggande eller av polisman genom föreläggande av ordningsbot. Ett brott definieras i svensk rätt som en gärning som är beskriven i lag eller annan författning och för vilken straff är föreskrivet. Att en gärning är straffbelagd kan uttryckas som att gärningen är kriminaliserad.

Både fysiska och juridiska personer kan bli föremål för administrativa sanktioner, men bara fysiska personer kan begå brott och dömas till en brottspåföljd. En näringsidkare kan emellertid i vissa fall åläggas företagsbot för brott som har begåtts i utövningen av näringsverksamheten (36 kap. 7 § brottsbalken).

9.3 Administrativa sanktioner eller straffrättsliga påföljder?

Förslag: Tillsynsmyndigheten ska kunna besluta om administrativa sanktioner för överträdelser av bestämmelser i den nya lagen.

Bedömning: Det saknas anledning att införa bestämmelser om straffansvar för överträdelser av den nya lagen.

Åklagarutredningen behandlade i betänkandet *Ett reformerat åklagarväsende* (SOU 1992:61) vilka närmare kriterier som bör vara styrande för att en kriminalisering av ett visst beteende ska vara befogad. Kriterierna var följande.

1. Ett beteende kan föranleda påtaglig skada eller fara.
2. Alternativa sanktioner står inte till buds, skulle inte vara rationella eller skulle kräva oproportionerligt höga kostnader.
3. En straffsanktion krävs med hänsyn till gärningens allvar.
4. Straffsanktionen ska utgöra ett effektivt medel för att motverka det icke önskvärda beteendet.
5. Rättsväsendet ska ha resurser att klara av den eventuellt ytterligare belastning som kriminaliseringen innebär.

Regeringen och riksdagen ställde sig i allt väsentligt bakom dessa kriterier[1].

Därefter har straffrättsanvändningsutredningen i betänkandet *Vad bör straffas?* (SOU 2013:38) övervägt vilka grundläggande kriterier som ska vara uppfyllda för att kriminalisering ska övervägas[2]. Ett av kriterierna är att det inte får finnas någon alternativ metod som är tillräckligt effektiv för att komma till rätta med det oönskade beteendet. De överväganden som enligt straffrättsanvändningsutredningen bör göras är bl.a. om beteendet kan motverkas tillräckligt effektivt med en regel som inte är repressiv, t.ex. en civilrättslig regel om skadestånd. Om det är nödvändigt att införa en repressiv hand-

[1] Prop. 1994/95:23 s. 55 och bet. 1994/95:JuU2.
[2] S. 19 f.

lingsdirigerande regel ska i första hand vite, sanktionsavgift eller återkallelse av tillstånd övervägas. Straff bör väljas i sista hand.

Även inom EU har kriterier för kriminalisering diskuterats och 2009 antogs *Rådets slutsatser om modellbestämmelser som vägledning för rådets överläggningar på det straffrättsliga området*[3]. En av de slutsatserna är att straffrättsliga bestämmelser som regel ska användas enbart som en sista utväg. Om det verkar finnas behov av att anta nya straffrättsliga bestämmelser bör enligt en annan slutsats hänsyn tas till de straffrättsliga bestämmelsernas förväntade mervärde eller ändamålsenlighet i jämförelse med andra åtgärder och med beaktande av möjligheten att med rimliga insatser utreda och lagföra brottet, samt brottets svårighetsgrad och konsekvenser.

Målet med bestämmelserna i NIS-direktivet och den nya lagen är att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem. För att uppnå detta är de aktörer som omfattas av bestämmelserna skyldiga att bl.a. vidta säkerhetsåtgärder och att rapportera incidenter. Syftet med regleringen uppnås enligt utredningens bedömning minst lika effektivt med hjälp av administrativa sanktioner som genom införandet av straffansvar. Härtill kommer att en förundersökning på det aktuella området är relativt resurskrävande. Eventuella överträdelser av bestämmelserna är inte heller så allvarliga att de bör kriminaliseras. Det kan i detta sammanhang nämnas att den som uppsåtligen eller av oaktsamhet vid myndighetsutövning åsidosätter vad som gäller för uppgiften kan dömas för tjänstefel enligt 20 kap 1 § brottsbalken. En arbetstagare som åsidosätter sina skyldigheter i anställningen kan också åläggas disciplinpåföljd, dvs. löneavdrag eller varning, för tjänsteförseelse enligt lagen (1994:260) om offentlig anställning.

Med hänsyn till det nu sagda anser utredningen att de sanktioner som bör komma i fråga för överträdelser av den nya lagens bestämmelser bör vara av administrativt slag.

[3] Dok. 16542/3/09

9.4 Vilka administrativa sanktioner ska införas?

Både sanktionsavgift och återkallelse av tillstånd är i huvudsak tillbakaverkande sanktioner som är handlingsdirigerande genom att verka avskräckande. Sanktionsavgifter kan också vara vinstbegränsande. Återkallelse av tillstånd kan även ses som en framåtriktad sanktion, i den mån återkallelsen syftar till att förhindra fortsatt bristande efterlevnad av ett regelverk. Vite är däremot alltid framåtsyftande. Det syftar till att tvinga fram ett önskat agerande eller att få ett pågående oönskat agerande att upphöra. Först om den vitesålagde inte uppfyller en specificerad skyldighet döms vitet ut.

Merparten av de aktörer som omfattas av bestämmelserna i den nya lagen är inte beroende av tillstånd för att bedriva sin verksamhet. Varning eller återkallelse av tillstånd är alltså inte användbara ingripanden i de flesta fall. Med hänsyn till att ett övergripande syfte med bestämmelserna är att säkerställa kontinuiteten i samhällsviktiga tjänster är inte heller förbud mot fortsatt verksamhet ett lämpligt alternativ. De sanktioner som främst bör komma i fråga är enligt utredningens mening åtgärdsföreläggande som kan förenas med vite samt sanktionsavgifter.

9.5 Åtgärdsföreläggande i förening med vite

Förslag: Tillsynsmyndigheten får meddela de förelägganden som behövs för att leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster ska uppfylla de säkerhetskrav och krav på incidentrapportering som följer av den nya lagen och av föreskrifter som har meddelats i anslutning till den.

Innan ett föreläggande meddelas ska tillsynsmyndigheten samverka med Datainspektionen.

Ett föreläggande får förenas med vite.

Utredningen har i avsnitt 8.5.3 bedömt att tillsynsmyndigheten ska få meddela förelägganden vid vite om att den som står under tillsyn ska tillhandahålla information som behövs för tillsynen.

Utredningen bedömer att tillsynsmyndigheten bör ha möjlighet att meddela åtgärdsförelägganden i enskilda fall även när det gäller säkerhetskrav och krav på incidentrapportering.

Enligt artikel 15.4 i NIS-direktivet ska tillsynsmyndigheten samarbeta med dataskyddsmyndigheter när den hanterar incidenter hos leverantörer av samhällsviktiga tjänster som medför personuppgiftsincidenter. Innan ett föreläggande mot en leverantör av samhällsviktiga tjänster meddelas ska tillsynsmyndigheten därför samverka med Datainspektionen. Det bör t.ex. kontrolleras att ett krav på att vidta en viss säkerhetsåtgärd inte motverkar åtgärder till stöd för en säker personuppgiftsbehandling. En bestämmelse som reglerar denna samverkan bör tas in i förordning.

Mot bakgrund av NIS-direktivets krav på att det ska finnas effektiva, proportionella och avskräckande sanktioner bör åtgärdsförelägganden kunna förenas med vite.

När vite föreläggs, ska det enligt 3 § lagen (1985:206) om viten (viteslagen) 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. Med omständigheterna i övrigt avses bl.a. 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.

9.6 Sanktionsavgift

9.6.1 Sanktionsavgift införs för överträdelser av vissa bestämmelser i den nya lagen

Förslag: Sanktionsavgift ska meddelas mot den som underlåter att vidta säkerhetsåtgärder eller att incidentrapportera enligt lagen.

Avgiften ska tillfalla staten.

En sanktionsavgift är en ekonomisk sanktion som vanligen riktar sig mot en konstaterad överträdelse av en författningsbestämmelse. Sanktionsavgifter anses inte ingå i det straffrättsliga systemet och det finns därför i princip inga krav på att avgiften ska utformas i enlighet med de allmänna principer som gäller för straffrätten.

Sanktionsavgifter kan vara ett alternativ till straff. Ett system med sanktionsavgifter används ofta för att åstadkomma ett enklare och snabbare beivrande av regelbrott. Många gånger ges därför en myndighet rätt att som första instans besluta om sanktionsavgifter.

En sanktionsavgift bör knyta an till ett enkelt, objektivt och lätt konstaterbart faktum. Sanktionsavgifter bedöms inte vara lämpliga när det krävs mer omfattande bedömningar för att avgöra om lagstiftningen följs i det enskilda fallet[4].

Som huvudregel är det antingen en tillsynsmyndighet eller domstol, efter ansökan från tillsynsmyndigheten, som beslutar om uttag av sanktionsavgiften och dess storlek. Vanligtvis tillämpas ett strikt ansvar och vid fastställandet av avgiften används oftast schabloner. Sanktionsavgiften anses till följd av dessa omständigheter möjliggöra ett enklare, snabbare och effektivare beivrande av regelbrott jämfört med det straffrättsliga förfarandet.

Regleringen med en särskild avgift som tas ut av regelöverträdare har ansetts tillgodose unionsrättsliga krav på effektiva, proportionerliga och avskräckande sanktioner[5].

Utformningen av en sanktionsavgift vid tillsyn bör enligt regeringens skrivelse 2009/10:79, *En tydlig, rättssäker och effektiv tillsyn*, uppfylla de principer som angavs i förarbetena till bestämmelsen om

[4] Prop. 1981/82:142.
[5] Se prop. 2004/05:158 s. 142 f., prop. 2005/06:140 s. 75 ff. och prop. 2006/07:65 s. 226 ff.

förverkande i 36 kap. 4 § brottsbalken[6]. Enligt dessa principer bör sanktionsavgifter användas inom områden där regelöverträdelser är särskilt frekventa eller där det föreligger speciella svårigheter med att beräkna storleken av den vinst eller besparing som uppnås i det enskilda fallet. Avgifter bör vidare endast förekomma inom speciella och klart avgränsade rättsområden där det relativt lätt kan fastställas om en överträdelse skett eller inte. Sanktionsavgifter bör kunna beräknas utifrån parametrar som gör det möjligt att i förväg förutse och fastställa avgiftens storlek. Om avgiftsskyldigheten ska bygga på ett strikt ansvar bör förutsättas att det finns starkt stöd för en presumtion om att överträdelser inte kan förekomma annat än som en följd av uppsåt eller oaktsamhet. Det kan även behöva göras avsteg från principen om ett strikt ansvar.

I skrivelsen hänvisar regeringen vidare till tillsynsutredningens betänkande *Förslag om en tydligare och effektivare offentlig tillsyn* (SOU 2004:100)[7]. Där anges att sanktionsavgifter spelar en viktig roll inom de tillsynsområden där de förekommer och att avgifterna har en utformning som är specifikt avpassad till förhållandena inom respektive tillsynsområde. Det uttalas vidare att sanktionsavgifter bör ses som ett komplement till övriga ingripandemöjligheter.

Utredningen bedömer att sanktionsavgifter bör införas som ett komplement till möjligheten att meddela åtgärdsföreläggande när det gäller underlåtenhet att vidta säkerhetsåtgärder samt incidentrapportera.

Underlåtenhet att incidentrapportera är förhållandevis lätt att konstatera, även om det beträffande incidentrapporteringen krävs en bedömning av om en incident haft en betydande inverkan på kontinuiteten i den tillhandahållna tjänsten.

När det gäller skyldigheten att vidta säkerhetsåtgärder kan det vara svårare att bedöma en eventuell underlåtenhet, bl.a. eftersom en aktörs skyldighet att vidta säkerhetsåtgärder är kopplad till den risk som hotar säkerheten. Mot bakgrund särskilt av syftet med regleringen är säkerhetsbrister emellertid oacceptabla. Det är därför av stor vikt att en så pass ingripande sanktionsmöjlighet som sanktionsavgift finns att tillgå.

[6] Prop. 1981/82:142 s. 77.
[7] S. 190.

Bestämmelsen bör vara obligatorisk, dvs. utformas så att tillsynsmyndigheten ska besluta om sanktionsavgift när förutsättningarna för det är uppfyllda. Med hänsyn till principer om likabehandling, objektivitet och proportionalitet bör tillsynsmyndighetens möjligheter till mer skönsmässiga bedömningar vara begränsade.[8] Tillsynsmyndigheten bör dock ha möjlighet att under vissa förutsättningar efterge sanktionsavgiften helt eller delvis, se avsnitt 9.6.6.

Sanktionsavgiften ska tillfalla staten.

9.6.2 Sanktionsavgift och normgivning

Förslag: Bestämmelser om sanktionsavgift ska tas in i lag.

Enligt 8 kap. 2 § första stycket 2 regeringsformen ska föreskrifter meddelas genom lag om de avser förhållandet mellan enskilda och det allmänna. Detta gäller under förutsättning att föreskrifterna gäller skyldigheter för enskilda eller i övrigt avser ingrepp i enskildas personliga eller ekonomiska förhållanden. Enligt 3 § regeringsformen kan riksdagen bemyndiga regeringen att meddela föreskrifter enligt denna punkt. Föreskrifterna får dock inte avse annan rättsverkan av brott än böter.

I tidigare lagstiftningsärenden har det ansetts att sanktionsavgifter kan jämställas med böter. Detta talar för att normgivningen ska ha lagform, men med möjlighet att bemyndiga regeringen att meddela närmare föreskrifter.[9] Utredningen bedömer mot denna bakgrund att bestämmelser om sanktionsavgift ska tas in i lag.

[8] Wiweka Warnling-Nerep, Sanktionsavgifter – särskilt i näringsverksamhet, s. 192 ff.
[9] Wiweka Warnling-Nerep, Sanktionavgifter – särskilt i näringsverksamhet, s. 116; Om sanktionsavgifter vid överträdelser av import- och exportregleringar, prop. 1983/84:192 s. 44 och Sanktionsväxling – effektivare sanktioner på exportkontrollområdet, SOU 2014:83 s. 103.

9.6.3 Tillsynsmyndigheten ska besluta om sanktionsavgift

Förslag: Tillsynsmyndigheten ska besluta om sanktionsavgift.

Beslut om sanktionsavgift fattas som huvudregel av en tillsynsmyndighet eller av domstol efter ansökan från tillsynsmyndigheten.

Utredningen bedömer att det bör vara tillsynsmyndigheten som bestämmer om sanktionsavgift för överträdelse av sagda bestämmelser i den nya lagen ska tas ut i det enskilda fallet. Tillsynsmyndigheten bör också bestämma hur hög avgiften i så fall ska vara. En fördel med att myndigheten fattar beslutet är att handläggningen blir snabbare eftersom inte flera myndigheter måste involveras i hanteringen. Det är vidare tillsynsmyndigheten som har bäst förutsättningar att bedöma om en aktör har underlåtit att följa regelverket. Tillsynsmyndigheten kommer att vara väl förtrogen med det regelverk som sanktioneras och ha goda förutsättningar att upptäcka regelöverträdelser.

I detta sammanhang bör även nämnas den undersökning som krigsmaterielexportöversynskommittén har gjort av hur sanktionsavgifter fungerar i dag.[10] Kommittén konstaterar att användningsfrekvensen för sanktionsavgifter är betydligt högre hos de myndigheter som själva kan fatta beslutet jämfört med hos de myndigheter som måste ansöka hos domstol. Av de sanktionsavgiftsbeslut som meddelas direkt av en myndighet är det enligt kommittén överlag få som överklagas till domstol och i de fall överklagande sker är ändringsfrekvensen också låg.

9.6.4 Sanktionsavgiftens storlek

Förslag: Sanktionsavgiften ska bestämmas till lägst 5 000 kr och som högst till 10 miljoner kr.

Sanktionsavgifter kan vara utformade som på förhand bestämda belopp, oavsett vem som begått överträdelsen, eller vara kopplade till årsomsättning i näringsverksamhet.

[10] Sanktionsväxling – effektivare sanktioner på exportkontrollområdet (SOU 2014:83) s. 104.

De sanktioner som medlemsstaterna ska införa ska vara effektiva, proportionerliga och avskräckande. Den nya lagens bestämmelser kommer att omfatta såväl myndigheter som privata aktörer. Aktörerna kommer att skilja sig mycket från varandra vad gäller t.ex. storlek och ekonomiska förutsättningar. Detta innebär att vad som upplevs som en avskräckande avgift av en aktör med måttliga ekonomiska resurser kan framstå som i det närmaste obetydlig för en aktör med stora resurser. Skillnaderna kommer att finnas mellan aktörer i olika sektorer såväl som mellan aktörer inom samma sektor.

Med hänsyn främst till att vissa aktörer som omfattas av bestämmelserna är myndigheter bedömer utredningen att det inte är lämpligt att koppla sanktionsavgiften till omsättning, utan att ett system med bestämda beloppsintervall är att föredra. För att uppfylla kravet på effektiva, proportionerliga och avskräckande sanktioner bör intervallet för sanktionsavgiften vara förhållandevis stort. Tillsynsmyndigheten får då möjlighet att göra en nyanserad bedömning när avgiftens storlek ska bestämmas.

Vid bestämmandet av vilka beloppsintervall som bör gälla finns det skäl att titta på vad som gäller enligt andra regelverk.

Från och med den 25 maj 2018 ska EU:s medlemsstater tillämpa 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). Dataskyddsförordningen innehåller EU-gemensamma regler för personuppgiftsbehandling och kommer att utgöra grunden för generell personuppgiftsbehandling inom EU. Förordningen kommer att ersätta den svenska personuppgiftslagen. En särskild utredare har fått i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som förordning ger anledning till[11]. Uppdraget ska redovisas senast den 12 maj 2017.

Vid överträdelse av dataskyddsförordningen kan sanktionsavgift tas ut enligt två nivåer – en lägre nivå vid överträdelser som betraktas som mindre allvarliga och en högre nivå vid allvarligare överträdelser och underlåtenhet att följa förelägganden eller beslut av tillsynsmyndigheten eller att på annat sätt bistå den. För de olika nivåerna gäller maximibelopp på 10 miljoner euro respektive 20 miljoner

[11] Dataskyddsutredningen, Ju 2016:04, dir 2016:15.

euro alternativt en procentsats av den totala globala årsomsättningen. Något minimibelopp anges inte.

Även Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF ålägger medlemsstaterna att föreskriva effektiva, proportionella och avskräckande sanktioner för överträdelser av bestämmelser som antas enligt det direktivet. Direktivet innehåller regler om skydd av personuppgifter när behöriga myndigheter behandlar sådana uppgifter vid brottsbekämpning, brottmålshantering eller straffverkställighet. Regeringen har i mars 2016 tillsatt en utredning som ska föreslå hur direktivet ska genomföras i svensk rätt.[12] Ett delbetänkande, *Brottsdatalag* (SOU 2017:29), överlämnades den 5 april 2017. Uppdraget ska slutredovisas senast den 30 september 2017.

Inom svensk lagstiftning finns i dag sanktionsavgifter på bl.a. miljöområdet och arbetsmiljöområdet. De högsta respektive lägsta belopp som kan beslutas inom dessa områden är 1 000 respektive 1 miljon kr, dvs. långt ifrån de belopp som anges i dataskyddsförordningen. Ett annat exempel är att Finansinspektionen, enligt lagen (2004:297) om bank- och finansieringsrörelse, får besluta om sanktionsavgift som ska fastställas till högst tio procent av kreditinstitutets omsättning alternativt två gånger den vinst som institutet har erhållit till följd av regelöverträdelsen eller två gånger de kostnader som institutet har undvikit till följd av regelöverträdelsen.

Ytterligare en jämförelse kan göras med de belopp som gäller för företagsbot. För sådan bot är minimibeloppet 5 000 kr och maximibeloppet 10 miljoner kr. Utredningen om vissa frågor om företagsbot har emellertid i betänkandet *En översyn av lagstiftningen om företagsbot* (SOU 2016:82), föreslagit att företagsboten ska kunna uppgå till 100 miljoner kronor. Förslaget lämnas mot bakgrund av att det enligt den utredningen är uppenbart att det finns situationer där ett belopp om 10 miljoner kronor framstår som ett alldeles för lågt belopp för att vara en tillräckligt kännbar sanktion. Det framhålls också att det faktum att motsvarande maximibelopp i flera

[12] Utredningen om 2016 års dataskyddsdirektiv, Ju 2016:06, dir. 2016:21.

andra europeiska länder är avsevärt högre talar för att det svenska maximibeloppet är för lågt. Betänkandet bereds för närvarande i regeringskansliet.

Utredningen bedömer att det är rimligt att det lägsta belopp som kan beslutas i sanktionsavgift är 5 000 kr, dvs. vad som i dag utgör lägsta belopp vid åläggande av företagsbot.

För att sanktionsavgiften ska få en tillräckligt avskräckande effekt för alla aktörer som kommer att omfattas av den nya lagens bestämmelser krävs att maximibeloppet sätts relativt högt. En för låg sanktionsnivå kan t.ex. medföra att företag räknar in avgiften som en ren affärskostnad. Det är enligt utredningens menig emellertid inte aktuellt med belopp i den storleksordning som kommer att gälla för överträdelser av dataskyddsförordningen. Utredningen bedömer att beloppet i stället bör korrespondera med vad som i dag gäller i svensk rätt. Det är enligt utredningens mening rimligt att även maximibeloppet motsvarar det belopp som högst kan åläggas genom företagsbot, dvs. 10 miljoner kr.

9.6.5 Sanktionsavgiftens bestämmande i det enskilda fallet

Förslag: När sanktionsavgiftens storlek bestäms ska hänsyn tas till samtliga relevanta omständigheter. Särskild hänsyn ska tas till den skada eller risk för skada som uppstått till följd av regelöverträdelsen, om leverantören tidigare har begått en överträdelse samt de kostnader som leverantören undvikit till följd av överträdelsen.

Bedömning: Det ska inte krävas uppsåt eller oaktsamhet för att sanktionsavgift ska kunna tas ut.

Huvudregeln vid användande av sanktionsavgift är att avgiftsskyldigheten ska bygga på strikt ansvar[13]. Beträffande de aktuella överträdelserna bedömer utredningen att det finns ett starkt stöd för en presumtion om att överträdelser inte kan förekomma annat än som en följd av uppsåt eller oaktsamhet. Utredningen bedömer därför

[13] Se t.ex. betänkandet *Vad bör straffas?* SOU 2013:38 s. 544.

att det inte finns anledning att frångå huvudregeln om strikt ansvar när det gäller den nya lagen.

Lagrådet har med hänvisning till huvudregeln om strikt ansvar uttalat att lagtext inte behöver innehålla någon upplysning om att uppsåt eller oaktsamhet inte krävs för att sanktionsavgift ska kunna dömas ut. En särskild angivelse av detta, som skett i ett antal lagar, riskerar enligt lagrådet att i stället för att vara klargörande skapa osäkerhet om vad som gäller närt någon sådan angivelse inte finns[14]. Utredningen bedömer mot denna bakgrund att det inte behöver anges i lagtext att sanktionsavgift får tas ut även om en överträdelse inte har skett uppsåtligen eller av oaktsamhet.

När storleken på sanktionsavgiften ska bestämmas i det enskilda fallet bör hänsyn tas till alla relevanta omständigheter. Det är inte möjligt att i lagen ange samtliga relevanta omständigheter som kan behöva beaktas i enskilda fall. Utredningen bedömer dock att lagen bör innehålla en bestämmelse som anger omständigheter som särskilt ska beaktas. De omständigheter som är särskilt viktiga att beakta och som alltså bör tas in i lagen är enligt utredningens mening den skada eller risk för skada som uppstått till följd av överträdelsen, om aktören tidigare har begått en överträdelse samt de kostnader som aktören undvikit till följd av regelöverträdelsen.

Exempel på omständigheter som kan komma att påverka beloppets storlek men som enligt utredningens mening inte behöver tas in i lagen är hur länge överträdelsen pågått. Om aktören tidigare gjort sig skyldig till överträdelse av lagen kan det bli aktuellt att beakta om överträdelserna är likartade samt den tid som har gått mellan de olika överträdelserna. Det kan också vara relevant att beakta bestämmelsens betydelse för tillsynsområdet. Vissa omständigheter kan det finnas anledning att beakta i mildrande riktning. Att en aktör samarbetat med tillsynsmyndigheten för att komma till rätta med överträdelser kan vara en sådan omständighet[15].

[14] Prop. 2012/13:55 – *Ny lag om kontroll av ekologisk produktion* s. 139 ff.
[15] Jfr t.ex. 15 kap. lagen (2004:297) om bank- och finansieringsrörelse och prop. 2016/17:22 s. 220 f.

9.6.6 Jämkning och eftergift

Förslag: Sanktionsavgiften får efterges helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Att avgiftsskyldigheten bygger på strikt ansvar innebär mot bakgrund av de krav som följer av Europakonventionen att det behöver finnas en möjlighet för tillsynsmyndigheten att underlåta att besluta om sanktionsavgift. Det bör därför införas en bestämmelse som ger tillsynsmyndigheten utrymme att jämka eller helt efterge avgiften i fall där det inte framstår som rimligt och proportionerligt att ta ut avgift. Tillsynsmyndigheten bör i det enskilda fallet göra en nyanserad bedömning av om omständigheterna ger anledning till jämkning eller eftergift. Omständigheter som kan ha betydelse kan t.ex. vara överträdelsens allvarlighet och om aktören gjort rättelse. En annan situation som kan innebära att det framstår som oskäligt att besluta om sanktionsavgift är om en aktör drabbas av sanktionsavgift enligt något annat regelverk för i princip samma brist. Bestämmelser om säkerhetsåtgärder och sanktionsavgifter för den som bryter mot dessa bestämmelser finns t.ex. i den tidigare nämnda dataskyddsförordningen.[16] Det skulle också kunna uppstå situationer där en aktör på grund av avtal med t.ex. en underleverantör blir skyldig att betala skadestånd till följd av en brist som sanktioneras genom den nya lagens bestämmelser. Även i dessa fall skulle det kunna anses oskäligt att meddela beslut om sanktionsavgift.

9.6.7 Hinder mot sanktionsavgift

Förslag: Tillsynsmyndigheten får inte ingripa med sanktionsavgift om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

[16] 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).

Regeringen har i flera lagstiftningsärenden konstaterat att begreppet straff i den mening som avses i Europakonventionen får anses omfatta även t.ex. vite[17]. Om ett vite har dömts ut bör det därför inte vara möjligt att besluta om en sanktion – administrativ eller straffrättslig – för samma sak. Den avgörande tidpunkten för när sådant hinder uppkommer bör enligt vad regeringen nyligen uttalat anses vara när det inleds en domstolsprocess angående frågan om utdömande av vite. Ett föreläggande om vite bör därför inte hindra ett senare ingripande så länge som tillsynsmyndigheten inte har ansökt om utdömande av vitet. I den situationen bör dock tillsynsmyndigheten vara förhindrad att ingripa mot en överträdelse som omfattas av vitesföreläggandet[18]. En bestämmelse om detta bör tas in i lagen.

9.6.8 Förfarandet vid beslut om sanktionsavgift

Förslag: Ett beslut om sanktionsavgift ska vara skriftligt och innehålla skälen för beslutet.

Innan tillsynsmyndigheten beslutar om sanktionsavgift ska den som beslutet kommer att riktas mot ges tillfälle att yttra sig.

Sanktionsavgift får inte beslutas om den som anspråket riktas mot inte har getts tillfälle att yttra sig inom två år efter överträdelsen.

För att rimliga krav på rättssäkerhet ska tillgodoses ska ett beslut om sanktionsavgift inte kunna komma i fråga förrän omständigheterna kring överträdelsen har utretts och den som beslutet avser att gälla har fått möjlighet att ta del av utredningen i ärendet och yttra sig över den.[19] Aktörens möjlighet i detta avseende är en förutsättning för att relevanta omständigheter ska bli kända för tillsynsmyndigheten och därmed för materiellt riktiga beslut och för förtroende för systemet.

Ett beslut om sanktionsavgift bör vara skriftligt och innehålla skälen för beslutet.

[17] Prop. 2007/08:107 s. 24 och prop. 2012/13:143 s. 69.
[18] Prop. 2016/17:22 s. 228.
[19] Jfr 16–17 §§ förvaltningslagen (1986:223).

Det bör finnas en bortre tidsgräns för när en sanktionsavgift får beslutas. Denna tid bör vara relativt kort. Utredningen anser att sanktionsavgift inte ska få beslutas om den som anspråket riktas mot inte har getts tillfälle att yttra sig inom två år från överträdelsen.

9.6.9 Betalning, indrivning och preskription

Förslag: Sanktionsavgiften ska betalas till tillsynsmyndigheten inom trettio dagar efter det att beslutet om sanktionsavgift fått laga kraft eller annars inom den längre tid som anges i beslutet.

En sanktionsavgift får verkställas utan föregående dom eller utslag om den är obetald och förfallen till betalning.

Om sanktionsavgiften inte betalas i tid ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning.

En beslutad sanktionsavgift faller bort om beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

För att regleringen om sanktionsavgifter ska bli tillräckligt handlingsdirigerande och effektiv bör den avgift som tillsynsmyndigheten beslutat kunna drivas in utan att det krävs något domstolsavgörande. Av 3 kap. 1 § första stycket 6 utsökningsbalken (1981:774) följer att en förvaltningsmyndighets beslut får verkställas om det finns en särskild föreskrift om detta. Det bör alltså införas en bestämmelse i den nya lagen som anger att en sanktionsavgift får verkställas om den är obetald och förfallen till betalning.

Utredningen bedömer att betalning av sanktionsavgift bör ske till tillsynsmyndigheten inom trettio dagar från det att beslutet om sanktionsavgift vann laga kraft eller annars inom den längre tid som anges i beslutet. Om avgiften inte betalas inom denna tid bör tillsynsmyndigheten lämna den obetalda avgiften för indrivning. [20]

I allmänhet gäller för den här typen av avgifter att de preskriberas i den utsträckning verkställighet inte har skett inom fem år. Utredningen bedömer att det saknas anledning att införa annan pre-

[20] Jfr t.ex. prop. 2016/17:22 s. 256 och prop. 2012/13:72 s. 30 f.

skriptionstid än den som i allmänhet används. Preskriptionstiden bör därför vara fem år.

9.7 Möjligheter till mindre ingripande åtgärder

Förslag: Om tillsynsmyndigheten finner skäl att misstänka att en leverantör av samhällsviktiga tjänster inte följer lagen eller föreskrifter som har meddelats i anslutning till lagen ska myndigheten underrätta leverantören om det och ge denne möjlighet att yttra sig inom skälig tid.

Om tillsynsmyndigheten konstaterar att en leverantör av samhällsviktiga tjänster eller en leverantör av digitala tjänster inte följer lagen eller föreskrifter som har meddelats i anslutning till lagen, ska myndigheten, genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse.

En tillsynsmyndighets grundläggande uppgift är att självständigt granska aktörer för att kontrollera om dessa uppfyller krav som följer av lagar och andra bindande föreskrifter, och vid behov fatta beslut om åtgärder som syftar till att åstadkomma rättelse av aktören. För att den nya lagens syfte – en höjd nivå av säkerhet i nätverk och informationssystem – ska uppnås på ett så effektivt sätt som möjligt anser utredningen att tillsynsmyndigheternas även bör ge vägledning i frågor som har samband med verksamheten. Tillsynsmyndigheterna bör arbeta både främjande och förebyggande för att effektivt uppnå lagstiftningens mål. (jfr avsnitt 8.5).

Det är inte givet att kännbara sanktioner i alla lägen är det mest effektiva sättet att uppnå den nya lagens syfte. I de fall tillsynsmyndigheten konstaterar att en leverantör av samhällsviktiga tjänster eller en leverantör av digitala tjänster gjort sig skyldig till en överträdelse bör tillsynsmyndigheten, på lämpligt sätt, försöka förmå leverantören att vidta rättelse.

I de fall tillsynmyndigheten finner skäl att misstänka att en leverantör av samhällsviktiga tjänster överträder bestämmelserna, bör tillsynsmyndigheten underrätta leverantören om detta och ge denne tillfälle att yttra sig inom skälig tid. Vad som är skälig tid får avgöras efter omständigheterna i det enskilda fallet. Utöver möjligheten att lämna sina synpunkter får leverantören i och med underrättelsen

möjlighet att vidta åtgärder för att t.ex. leva upp till säkerhetskrav eller på andra sätt minska risker för incidenter. Att en leverantör vidtar rättelse kan ha betydelse för vilket belopp som beslutas i sanktionsavgift.

Tillsynsmyndigheten bör kunna utfärda föreläggande samt besluta om sanktionsavgift även om leverantören inte yttrar sig till följd av en underrättelse. Inte heller upprepade inlagor från leverantören bör kunna hindra myndigheten från att gå vidare i tillsynen. Att tillsynsmyndigheten ska försöka förmå en leverantör att vidta rättelse är inte heller något hinder mot utfärdande av föreläggande eller beslut om sanktionsavgift. Detta kan innebära att ett förfarande om meddelande av beslut om sanktionsavgift inleds eller föreläggande utfärdas parallellt med tillsynsmyndighetens åtgärder i syfte att förmå leverantören att rätta sig. Det bör dock vara upp till tillsynsmyndigheten att avgöra när det är lämpligt att vidta de åtgärder som står till buds.

9.8 Vitesföreläggande och sanktionsavgifter mot statliga myndigheter och kommuner

Bedömning: Även statliga myndigheter och kommuner ska kunna föreläggas vite och meddelas sanktionsavgift.

Vitesföreläggande kan i vissa fall riktas även mot staten. I förarbetena till viteslagen uttalade departementschefen att det särskilt vad gäller det marknadsrättsliga fältet kan tänkas uppkomma situationer där staten i så utpräglad grad uppträder som privaträttsligt subjekt att det skulle te sig onaturligt om möjligheten att förelägga vite inte stod till buds. Som exempel angavs ett organ som ingår i den statliga organisationen och som bedriver affärsverksamhet i konkurrens med och på liknande sätt som privata företag, mot vilka viten kan riktas enligt de marknadsrättsliga reglerna.[21]

I rättspraxis har Miljööverdomstolen i ett mål angående föreläggande mot Banverket om bullerskyddsåtgärder uttalat att det inte fanns några rättsliga hinder mot att förelägga Banverket att vid vite

[21] prop. 1984/85:96 s. 99 f.

vidta åtgärderna. Domstolen ansåg att Banverket i det sammanhanget närmast fick betraktas som affärsdrivande och att det principiellt inte fanns anledning att göra skillnad mellan Banverket och andra verksamhetsutövare och av det skälet låta bli att sätta ut vite.[22]

Frågan om sanktionsavgifter är en lämplig reaktion mot myndigheter har också behandlats i betänkandet *Brottsdatalag* (SOU 2017:29).

Utredningen bedömer med hänsyn till det anförda att vitesföreläggande och sanktionsavgifter enligt den nya lagen under motsvarande förhållanden ska kunna meddelas även mot statliga myndigheter och kommuner.

9.9 Omedelbar verkställighet och inhibition

Förslag: Tillsynsmyndigheten får bestämma att ett beslut om föreläggande ska gälla omedelbart.

Bedömning: Bestämmelser om inhibition finns i förvaltningsprocesslagen och behöver inte tas in i den nya lagen.

Om tillsynsmyndigheten har konstaterat att det finns skäl för att ingripa genom beslut om föreläggande finns det ofta ett behov av att beslutet blir gällande genast. Det kan då vara nödvändigt att beslutet verkställs omedelbart. Samma sak gäller beträffande tillsynsmyndighetens beslut att förelägga en leverantör att lämna tillträde till lokaler och att lämna upplysningar, handlingar och liknande för att tillsynen ska kunna genomföras. I sådana fall kan det vara angeläget att beslutet inte förhalas genom ett överklagande. Mot denna bakgrund bör tillsynsmyndigheten ha möjlighet att bestämma att dess beslut om föreläggande ska gälla omedelbart.

En domstol som ska pröva ett överklagande av ett förvaltningsbeslut som gäller omedelbart kan förordna att det överklagade beslutet tills vidare inte ska gälla (s.k. inhibition). Möjligheten till inhibition innebär att risken för att en aktör drabbas av skada på grund av ett felaktigt beslut av en tillsynsmyndighet minimeras. Bestämmel-

[22] MÖD 2005:12

ser om inhibition finns i 28 § förvaltningsprocesslagen (1971:291) och behöver inte tas in i den nya lagen.

9.10 Överklagande

Förslag: Tillsynsmyndighetens beslut enligt den nya lagen eller föreskrifter som meddelats i anslutning till lagen ska kunna överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Kammarrättens avgörande i ett mål enligt den nya lagen får inte överklagas.

En tillsynsmyndighets beslut om förelägganden och sanktionsavgifter måste kunna överklagas. Även beslut om förelägganden som meddelas för att tillsynsmyndigheten ska kunna fullgöra tillsynen måste kunna överklagas (se avsnitt 8.5.3). Besluten ska kunna överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Kammarrättens avgörande ska inte kunna överklagas.

10 Leverantörer av digitala tjänster

10.1 Inledning

Utöver operatörer som tillhandahåller samhällsviktiga tjänster reglerar direktivet säkerheten i nätverk och informationssystem hos sådana leverantörer av digitala tjänster som anges i bilaga 3 till direktivet. Dessa tjänster är internetbaserade marknadsplatser, internetbaserade sökmotoror och molntjänster.

I detta kapitel beskrivs NIS-direktivets bestämmelser om leverantörer av digitala tjänster med utgångspunkt främst i hur bestämmelserna skiljer sig från dem som gäller för leverantörer av samhällsviktiga tjänster. När det gäller t.ex. ingripanden och sanktioner samt hur tillsynen ska organiseras är frågorna emellertid sammankopplade på ett sådant sätt att de bör behandlas i ett sammanhang. I dessa delar hänvisas därför till de avsnitt där respektive fråga behandlas.

10.2 NIS-direktivets tillämpningsområde och definitioner

10.2.1 Definitioner

Definitionerna av internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster i NIS-direktivet är specifika för direktivet och påverkar inte andra instrument (skäl 55).

I NIS-direktivet definieras en *digital tjänst* som en tjänst i den mening som avses i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster av en typ som anges i bilaga 3 till direktivet. De kategorier av tjänster som anges i den

bilagan är internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster.

I artikel 1.1 b i direktiv (EU) 2015/1535 definieras digital tjänst enligt följande.

> [A]lla informationssamhällets tjänster, det vill säga tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. I denna definition avses med
>
> i) på distans: tjänster som tillhandahålls utan att parterna är närvarande samtidigt,
>
> ii) på elektronisk väg: en tjänst som sänds vid utgångspunkten och tas emot vid slutpunkten med hjälp av utrustning för elektronisk behandling (inbegripet digital signalkomprimering) och lagring av uppgifter, och som i sin helhet sänds, befordras och tas emot genom tråd, radio, optiska medel eller andra elektromagnetiska medel,
>
> iii) på individuell begäran av en tjänstemottagare: en tjänst som tillhandahålls genom överföring av uppgifter på individuell begäran.

Med *leverantör av digitala tjänster* avses i NIS-direktivet en juridisk person som tillhandhåller en digital tjänst (artikel 4.6).

En *internetbaserad marknadsplats* är enligt NIS-direktivet en digital tjänst som gör det möjligt för konsumenter och/eller näringsidkare (enligt definitionen i artikel 4.1 a respektive 4.1 b Europaparlamentets och rådets direktiv 2013/11/EU av den 21 maj 2013 om alternativ tvistlösning vid konsumenttvister och om ändring av förordning (EG) nr 2006/2004 och direktiv 2009/22/EG (direktivet om alternativ tvistlösning) att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare antingen på webbplatsen för den internetbaserade marknadsplatsen eller på webbplatsen tillhörande en näringsidkare där datatjänster som tillhandahålls av en internetbaserad marknadsplats används (artikel 4.17).

En *internetbaserad sökmotor* är enligt NIS-direktivet en digital tjänst som gör det möjligt för användaren att göra sökningar på i princip alla webbplatser eller webbplatser på ett visst språk eller på grundval av en förfrågan om vilket ämne som helst i form av ett nyckelord, en fras eller annan inmatning och som returnerar länkar som innehåller information om det begärda innehållet (artikel 4.18)

Molntjänster definieras i NIS-direktivet som en digital tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser (artikel 4.19).

10.2.2 Aktörer som inte omfattas av NIS-direktivet

Mikroföretag och små företag samt hård- och mjukvarutillverkare omfattas inte

Bestämmelserna i NIS-direktivet ska inte tillämpas på mikroföretag eller små företag enligt definitionen i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (artikel 16.11). Enligt den rekommendationen är ett mikroföretag ett företag med färre än 10 anställda och en årsomsättning eller balansomslutning som understiger två miljoner euro. Små företag definieras i rekommendationen som företag med färre än 50 anställda och en årsomsättning eller balansomslutning som inte överstiger 10 miljoner euro.

I NIS-direktivet anges att hårdvarutillverkare och mjukvaruutvecklare spelar en viktig roll när det gäller att möjliggöra för leverantörer av både samhällsviktiga tjänster och digitala tjänster att skydda sina nätverk och informationssystem. De omfattas emellertid av redan befintliga bestämmelser om produktansvar och träffas inte av NIS-direktivet. (skäl 50)

Övriga undantag

Angående gränsdragningen mot säkerhetskänslig verksamhet, se kapitel 5.

10.2.3 Vad är en internetbaserad marknadsplats, en internetbaserad sökmotor och molntjänster i praktiken?

Vid bedömningen av vad som i praktiken utgör en internetbaserad marknadsplats, internetbaserad sökmotor eller en molntjänst kan ledning hämtas från NIS-direktivets skäl samt från vedertagna standarder.

Internetbaserad marknadsplats

En internetbaserad marknadsplats ger enligt NIS-direktivet konsumenter och näringsidkare möjlighet att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare och är slutdestinationen för ingåendet av sådana avtal (skäl 15).

En näringsidkare som vill tillhandahålla sina varor och tjänster via internet kan göra detta genom en e-butik eller via en digital marknadsplats. Till skillnad från e-butiken är den digitala marknadsplatsen en webbplats där kunden kan ta del av flera näringsidkares utbud på samma ställe. Marknadsplatsen kan på detta sätt jämföras med ett köpcentrum. Genom att använda sig av en marknadsplats kan näringsidkaren nå ut med sina varor och tjänster utan att behöva marknadsföra sig på samma sätt som krävs för att kunderna ska hitta till den egna e-butiken.

Som exempel på internetbaserade marknadsplatser kan nämnas amazon.com, etsy.com och blocket.se.

Internetbaserad sökmotor

En sökmotor kan beskrivas som ett dataprogram som söker igenom och på något sätt katalogiserar sidor och filer på internet.

En internetbaserad sökmotor gör det möjligt för användaren att göra sökningar på i princip alla webbplatser på grundval av en sökning inom vilket ämnesområde som helst. Den kan också vara inriktad på webbplatser på ett visst språk. (skäl 16)

Exempel internetbaserade sökmotorer är google.com, yahoo.com och bing.com.

Molntjänster

Molntjänster är ett samlingsnamn för it-tjänster som ersätter program och lagringsutrymme i användarens egen dator och i stället erbjuder motsvarande funktioner i servrar via internet. Att ha sin information i ”molnet” innebär alltså att ha informationen i ”någon annans dator”.

I NIS-direktivet (skäl 17) anges att molntjänster omfattar många olika verksamheter, som kan levereras enligt olika modeller. Vid tillämpningen av direktivet omfattar termen molntjänster sådana tjänster som medger åtkomst till en skalbar och elastisk pool av delbara dataresurser. Sådana dataresurser omfattar resurser såsom nätverk, servrar eller annan infrastruktur, lagring, applikationer och tjänster. Termen skalbar avser dataresurser 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 dataresurser som avsätts 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 dataresurser 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.

SIS (Swedish Standards Institute) har definierat molnbaserade datortjänster som ”… ett koncept som möjliggör nätverksåtkomst till en skalbar och elastisk pool av delade fysiska eller virtuella resurser som via självbetjäning levereras och administreras på begäran”.

NIST (US National Institute for Standards and Technology) har definierat begreppet molntjänster som ”a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. NIST anger också fem väsentliga egenskaper hos molntjänster:

1. självbetjäning är möjlig när kunden behöver det,
2. åtkomst sker via nätet i olika klienter (exempelvis stationära datorer, mobiltelefoner och surfplattor),
3. kunden delar leverantörens resurser med andra kunder,
4. prestanda anpassas till kundens behov för stunden, och
5. tjänsterna går att mäta, bl.a. i syfte att avgöra hur mycket kunden ska debiteras för tjänsten.

NIST anger vidare tre huvudsakliga typer av molntjänster; Infrastructure as a Service, Platform as a Service och Software as a Service. Tjänstetyperna beskriver tre olika funktionsområden och tjänsterna finns i olika tekniska lager. Leverantören tillhandahåller tekniska lösningar i olika utsträckning beroende på typ av tjänst.

Molntjänster kan tillhandahållas på fyra olika sätt; privata moln, partnermoln, publika moln och hybridmoln[1].

Privata molntjänster bygger på en infrastruktur som är dedikerad åt endast en användare. Infrastrukturen kan hanteras av användaren själv eller av en annan aktör.

Partnermoln, som ibland också kallas för gemenskapsmoln eller branschmoln, erbjuds till en begränsad och väldefinierad grupp av kunder. En särskild form av partnermoln är s.k. myndighetsmoln. Ett myndighetsmoln har skapats i t.ex. Storbritannien, för att möta särskilda behov av t.ex. säkerhet.

Publika molntjänster ägs och hanteras av en molntjänstleverantör (tredje part) som säljer resurser till flera kunder i samma infrastruktur. Tjänster i publika moln är potentiellt tillgängliga för alla som så önskar. GoogleApps, iCloud och Dropbox är exempel på publika molntjänster.

Hybridmoln avser en sammansättning av två eller flera molntyper som möjliggör kopplingar mellan olika tjänster och molntyper.

10.2.4 Nationell lagstiftning saknas i dag

Leverantörer av internetbaserade marknadsplatser, internetbaserade sökmotorer eller molntjänster omfattas i dag inte av någon nationell lagstiftning motsvarande bestämmelserna i direktivet. Utredningen har i kapitel 5 bedömt att NIS-direktivet bör genomföras genom införandet av en ny lag.

[1] Molntjänster i staten – En ny generation av outsourcing, Pensionsmyndigheten.

10.2.5 Vilka leverantörer av digitala tjänster ska omfattas av den nya lagen?

Förslag: En leverantör av digitala tjänster som erbjuder digitala tjänster i Sverige men som inte har sitt huvudsakliga etableringsställe inom Europeiska unionen ska utse en företrädare i något av de länder där tjänsterna erbjuds.

Bedömning: En näringsidkare som tillhandahåller sina egna varor och tjänster på en webbplats (e-butik) är inte en leverantör av digitala tjänster i form av internetbaserad marknadsplats enligt NIS-direktivet och ska inte omfattas av lagen.

En aktör som använder sig av ett privat moln är inte en leverantör av digitala tjänster enligt NIS-direktivet och ska inte omfattas av lagen.

I kapitel 5 kommer utredningen fram till att den nya lagen ska omfatta endast sådana leverantörer som omfattas av NIS-direktivet, se avsnitt 5.4. Beträffande leverantörer av digitala tjänster ska den nya lagen alltså tillämpas på tillhandahållare av digitala tjänster i form av internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster, med undantag av leverantörer som är mikroföretag eller små företag.

Jurisdiktion m.m.

För att en leverantör av en digital tjänst ska omfattas av NIS-direktivet krävs inte att den tillhandahållna tjänsten bedöms vara samhällsviktig. Till skillnad från vad som gäller beträffande leverantörer av samhällsviktiga tjänster är medlemsstaterna inte heller skyldiga att identifiera leverantörer av digitala tjänster.

För att en leverantör av digitala tjänster ska omfattas av lagstiftningen i en medlemsstat krävs enligt NIS-direktivet att leverantören har sitt huvudsakliga etableringsställe i det landet. Det huvudsakliga etableringsstället ska anses vara där leverantören har sitt huvudkontor. Det krävs att leverantören utför en faktisk och reell verksamhet med hjälp av en stabil struktur för att den ska anses vara etablerad. Den rättsliga formen, dvs. om det är fråga om en filial eller ett dotter-

bolag, bör inte vara avgörande. Att nätverk och informationssystem är fysiskt belägna på en viss plats innebär inte att det är fråga om ett huvudsakligt etableringsställe. (skäl 64)

Om leverantören inte är etablerad i unionen, men erbjuder tjänster här, ska leverantören utse en företrädare i någon av de medlemsstater där tjänsterna erbjuds. Leverantören ska i de fallen omfattas av lagstiftningen i det land där företrädaren finns. För att fastställa om en leverantör av digitala tjänster erbjuder tjänster inom unionen bör det kontrolleras om det är uppenbart att leverantören planerar att erbjuda tjänster till personer i en eller flera medlemsstater. Att kontaktuppgifter eller en webbplats tillhörande leverantören är tillgängliga i unionen, eller att ett språk används som allmänt används i det tredjeland där leverantören är etablerad är inte tillräckligt för att fastställa en sådan avsikt. Företrädaren bör agera på leverantörens vägnar och det bör vara möjligt för behöriga myndigheter eller CSIRT-enheterna att kontakta företrädaren. Företrädaren bör utses uttryckligen genom en skriftlig fullmakt från leverantören av digitala tjänster att agera på dess vägnar med avseende på leverantörens skyldigheter enligt NIS-direktivet. (skäl 65)

Som tidigare nämnts anger NIS-direktivet att bestämmelserna om leverantörer av digitala tjänster inte ska tillämpas på mikroföretag eller små företag.

Bestämmelser som genomför NIS-direktivet i dessa delar ska införas i den nya lagen.

Den nya lagen ska inte tillämpas på jämförelsesajter

En *internetbaserad marknadsplats* ger konsumenter och näringsidkare möjlighet att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare och är slutdestinationen för ingåendet av sådana avtal. Datatjänster som tillhandahålls av den internetbaserade marknadsplatsen kan enligt direktivet inbegripa behandling av transaktioner, sammanställning av data eller profilering av användare. Applikationsbutiker, som fungerar som onlinebutiker och möjliggör digital distribution av applikationer eller programvara från tredje part, ska betraktas som en typ av internetbaserad marknadsplats. Onlinetjänster som jämför priset på vissa varor eller tjänster från olika näringsidkare och sedan leder användaren vidare till den näringsidkare som valts

för köp av varan omfattas emellertid inte av begreppet. Sådana onlinetjänster, t.ex. pricerunner.se och prisjakt.nu, fungerar endast som mellanhand för tredjepartstjänster genom vilka ett avtal slutligen kan ingås. (skäl 15). Sistnämnda jämförelsesajter är inte heller att betrakta som sådana *internetbaserade sökmotorer* som omfattas av NIS-direktivet. Sökfunktioner som begränsas till innehållet på en särskild webbplats omfattas inte heller av direktivet. Det gäller oavsett om sökfunktionen tillhandahålls av en extern sökmotor. (skäl 16)

Den nya lagen ska inte tillämpas på näringsidkare som tillhandahåller egna varor och tjänster på en webbplats i egen regi (e-butiker) eller på användare av privata moln

Bakgrunden till regleringen avseende leverantörer av digitala tjänster är att många företag i unionen är beroende av leverantörer av digitala tjänster för att tillhandahålla sina tjänster. Eftersom vissa digitala tjänster skulle kunna utgöra en viktig resurs för sina användare, inklusive leverantörer av samhällsviktiga tjänster, och dessa användare inte alltid har alternativ tillgängliga, har det bedömts att NIS-direktivet bör gälla också för leverantörer av sådana tjänster. För många företag är säkerheten, kontinuiteten och tillförlitligheten hos den typ av digitala tjänster som avses i NIS-direktivet av avgörande betydelse för att företaget ska fungera väl. En störning i en sådan digital tjänst kan hindra tillhandahållandet av andra tjänster som är beroende av den och därmed påverka viktig ekonomisk och samhällelig verksamhet i unionen. Sådana digitala tjänster skulle därför kunna vara av avgörande betydelse för att företag som är beroende av dem ska fungera väl och för dessa företags deltagande i den inre marknaden och den gränsöverskridande handeln inom unionen. Leverantörer av digitala tjänster som omfattas av NIS-direktivet är sådana som anses erbjuda digitala tjänster som många företag i unionen i allt högre grad är beroende av. (skäl 48)

Det står klart att tillhandahållare (leverantörer) av internetbaserade marknadsplatser där användaren (kunden) kan sluta avtal med ett flertal näringsidkare omfattas av bestämmelserna i NIS-direktivet. Detsamma gäller en leverantör som tillhandahåller molntjänster åt någon annan.

Det förekommer emellertid också att näringsidkare tillhandahåller varor och tjänster på webbplatser i egen regi genom e-butiker.

När en aktör tillhandahåller egna varor eller tjänster genom en e-butik är det inte fråga om tillhandahållande av en digital tjänst i form av en internetbaserad marknadsplats. Näringsidkaren är inte en leverantör av en digital tjänst i NIS-direktivets mening, utan en användare av webbplatsen i syfte att tillhandahålla andra varor och tjänster än digitala tjänster. En webbplats som drivs i egen regi tillhandahålls inte heller av någon annan, varför det inte kan sägas vara fråga om en tjänst. En incident med effekter på en sådan aktörs webbplats påverkar dessutom endast aktörens egen verksamhet och har ingen inverkan på andra aktörers möjligheter att tillhandahålla sina varor eller tjänster.

Samma resonemang kan appliceras på situationen med privata moln. En användare av privata moln är inte en leverantör av en digital tjänst och omfattas därmed inte av NIS-direktivets bestämmelser. Det gäller oavsett om infrastrukturen hanteras av användaren själv eller om användaren överlåtit det uppdraget till någon annan. I det sistnämnda fallet kan dock uppdragstagaren omfattas av bestämmelserna såsom leverantör av en digital tjänst.

10.3 Säkerhetskrav och krav på incidentrapportering

Förslag: Leverantörer av digitala tjänster ska utarbeta och vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder när de tillhandahåller internetbaserade marknadsplatser, internetbaserade sökmotorer eller molntjänster inom unionen. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till den föreliggande risken, varvid hänsyn ska tas till

1. säkerheten i system och anläggningar,
2. incidenthantering,
3. hantering av driftskontinuitet,
4. övervakning, revision och testning och
5. efterlevnad av internationella standarder.

Leverantörer av digitala tjänster ska vidta åtgärder för att förebygga och minimera den inverkan som incidenter som påverkar säkerheten i deras nätverk och informationssystem har på internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster och som erbjuds inom unionen, i syfte att säkerställa kontinuiteten i dessa tjänster.

Leverantörer av digitala tjänster ska utan onödigt dröjsmål rapportera alla incidenter som har en avsevärd inverkan på tillhandahållandet av en internetbaserad marknadsplats, internetbaserad sökmotor eller molntjänst till CSIRT-enheten (Myndigheten för samhällsskydd och beredskap). Rapporterna ska innehålla information som gör det möjligt för CSIRT-enheten att fastställa vilken betydelse eventuell gränsöverskridande inverkan har.

Rapporteringen ska inte medföra ökat ansvar för den rapporterande parten.

För att fastställa om en incident har en avsevärd inverkan ska hänsyn framför allt tas till följande faktorer.

1. Det antal användare som påverkas av incidenten, framför allt användare som är beroende av tjänsten för att kunna tillhandahålla sina egna tjänster.
2. Hur länge incidenten varar.
3. Hur stort geografiskt område som påverkas av incidenten.
4. I vilken utsträckning incidenten stör tjänstens funktion.
5. I vilken utsträckning incidenten inverkar på den ekonomiska och samhälleliga verksamheten.

Skyldigheten att rapportera en incident ska gälla endast om leverantören har tillgång till den information som behövs för att bedöma en incidents inverkan mot bakgrund av angivna faktorer.

Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om rapportering av incidenter.

Bedömning: Utredningens förslag i dessa delar kan komma att behöva justeras med hänsyn till ännu inte antagna genomförandeakter.

10.3.1 NIS-direktivets krav

Säkerhetskrav

Leverantörer av digitala tjänster ska utarbeta och vidta tekniska och organisatoriska åtgärder för att hantera säkerhetsrisker i nätverk och informationssystem (artikel 16.1). De ska också vidta tekniska och organisatoriska åtgärder för att förebygga och minimera inverkan av incidenter (artikel 16.2). Begreppet tekniska och organisatoriska åtgärder behandlas i avsnitt 7.3.1.

De tekniska och organisatoriska åtgärder som leverantörerna ska utarbeta och vidta ska, med beaktande av den senaste tekniska utvecklingen, säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till den föreliggande risken, varvid hänsyn ska tas till a) säkerheten i system och anläggningar, b) incidenthantering, c) hantering av driftskontinuitet, d) övervakning, revision och testning och e) efterlevnad av internationella standarder. (artikel 16.1). Kommissionen ska anta genomförandeakter för att ytterligare specificera de element som avses. Genomförandeakterna ska antas i enlighet med det granskningsförfarande som avses i artikel 22.2 senast den 9 augusti 2017. (artikel 16.8)

Incidentrapportering

Leverantörer av digitala tjänster ska, liksom leverantörer av samhällsviktiga tjänster, utan onödigt dröjsmål rapportera incidenter till den behöriga myndigheten eller CSIRT-enheten. För leverantörer av digitala tjänster gäller att alla incidenter som har en avsevärd inverkan på tillhandahållandet av en digital tjänst enligt direktivets bilaga 3 som de erbjuder inom unionen. Rapporterna ska innehålla information som gör det möjligt för den behöriga myndigheten eller CSIRT-enheten att fastställa vilken betydelse eventuell gränsöverskridande inverkan har. Rapportering ska inte medföra ökat ansvar för den rapporterande parten.

För att fastställa om en incident har en avsevärd inverkan ska hänsyn tas till vissa angivna faktorer, bl.a. det antal användare som påverkas av incidenten, hur länge incidenten varar, hur stort geografiskt område som påverkas och i vilken utsträckning incidenten inverkar på den ekonomiska och samhälleliga verksamheten. Skyldigheten

att rapportera ska gälla endast om leverantören har tillgång till den information som behövs för att bedöma incidentens inverkan mot bakgrund av de angivna faktorerna. (artikel 16.3–4)

Kommissionen får anta genomförandeakter som fastställer format och förfaranden tillämpliga på rapporteringskrav. Sådana genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 22.2. (artikel 16.9)

10.3.2 Vilka krav ska ställas i den nya lagen?

NIS-direktivets bestämmelser om säkerhetsåtgärder och incidentrapportering ser annorlunda ut för leverantörer av digitala tjänster jämfört med leverantörer av samhällsviktiga tjänster. När det gäller säkerhetsåtgärder ska medlemsstaterna se till att leverantörer av digitala tjänster bland annat utarbetar åtgärder för att hantera risker i nätverk och informationssystem. Till skillnad från vad som gäller för leverantörer av samhällsviktiga tjänster är det alltså leverantörerna själva som ska identifiera dessa åtgärder.

Beträffande incidentrapporteringen ska leverantörer av digitala tjänster åläggas att rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av tjänsten, medan leverantörer av samhällsviktiga tjänster ska rapportera incidenter som har betydande inverkan. Leverantörer av digitala tjänster är skyldiga att rapportera en incident endast om leverantören har tillgång till den information som behövs för att bedöma incidentens inverkan.

Rapportering ska inte medföra ökat ansvar för den rapporterande parten. Det går därmed inte att ställa krav på att leverantören ska utreda händelsen åt någon annan, t.ex. CSIRT-enheten. Leverantörens skyldigheter beträffande rapporteringen upphör alltså i och med att rapporten har lämnats.

Enligt artikel 16.10 i NIS-direktivet får medlemsstaterna inte införa ytterligare säkerhets- eller rapporteringskrav för leverantörer av digitala tjänster utöver de som anges i direktivet. I skälen anges bl.a. att graden av risk för leverantörer av samhällsviktiga tjänster, som ofta är viktiga för att upprätthålla kritisk samhällelig och ekonomisk verksamhet, i praktiken är högre än för leverantörer av digitala tjänster. Leverantörer av digitala tjänster bör fritt kunna vidta de åtgärder som de anser lämpliga för att hantera risker för säker-

heten i sina nätverk och informationssystem. På grund av den gränsöverskridande arten bör dessa leverantörer omfattas av ett mer harmoniserat tillvägagångssätt på unionsnivå. Genomförandeakter bör underlätta i detta avseende. (skäl 49)

Bestämmelser som motsvarar NIS-direktivets bestämmelser om säkerhetskrav och incidentrapportering bör införas i den nya lagen.

Med hänsyn till att kommissionen senast den 9 augusti 2017 ska anta genomförandeakter för att specificera dels de element som ska ligga till grund för bedömningen av vilka tekniska och organisatoriska åtgärder som ska utarbetas och vidtas för att hantera risker i nätverk och informationssystem, dels de faktorer som ska ligga till grund vid bedömningen av om en incident har en avsevärd inverkan, kan utredningens förslag i dessa delar komma att behöva justeras. Samma sak gäller till följd av den möjlighet som kommissionen har att i genomförandeakter reglera format och förfaranden avseende incidentrapporteringen (artikel 16.9). I NIS-direktivets skäl 69 anges att kommissionen, när den antar genomförandeakter om säkerhetskraven, uppmuntras att beakta

- fysisk säkerhet och miljösäkerhet, funktionssäkerhet, kontroll av åtkomst till nätverks- och informationssystem samt nätverks- och informationssystemens integritet när det gäller systems och anläggningars säkerhet,
- incidenthanteringsförfaranden, kapacitet att upptäcka incidenter, incidentrapportering och kommunikation när det gäller incidenthantering,
- strategier för tjänstekontinuitet samt beredskapsplaner, kapacitet för katastrofberedskap när det gäller driftskontinuitetshantering och
- strategier för övervakning och loggning, beredskapsövningar, testning av nätverk och informationssystem, säkerhetsbedömningar och övervakning av efterlevnaden när det gäller övervakning, revision och testning.

Antagandet av en genomförandeakt får till följd att svensk lagstiftning som står i strid med genomförandeakten måste ändras i enlighet med denna.

Att regelverket för leverantörer av digitala tjänster inte innehåller mer långtgående eller specificerade säkerhetskrav hindrar inte att sådana krav kan ställas genom avtalsförpliktelser aktörerna emellan. Ett exempel på när detta kan aktualiseras är då offentliga förvaltningar använder tjänster som erbjuds av leverantörer av digitala tjänster, särskilt molntjänster (skäl 54).

Myndigheten för samhällsskydd och beredskap bör, till dess att eventuella genomförandeakter antas enligt artikel 16.9, få meddela föreskrifter om på vilket sätt skyldigheten att rapportera incidenter ska fullgöras och om incidentrapportens utformning. Skälen för detta utvecklas i avsnitt 7.3.2.

10.4 Tillsyn

Förslag: Tillsynsåtgärder beträffande leverantörer av digitala tjänster får vidtas endast när tillsynsmyndigheten har fått kännedom om att leverantören inte uppfyller de krav som lagen ställer.

Vid tillsyn ska en leverantör av digitala tjänster tillhandahålla tillsynsmyndigheten den information som behövs för en bedömning av säkerheten i leverantörernas nätverk och informationssystem, inbegripet dokumenterade säkerhetsprinciper.

När det gäller tillsyn över leverantörer av digitala tjänster ska den behöriga myndigheten inte ha någon allmän skyldighet att utöva tillsyn, vilket är en skillnad mot vad som gäller beträffande leverantörer av samhällsviktiga tjänster. Bakgrunden är att leverantörer av digitala tjänster bör omfattas av mindre ingripande, reaktiv efterhandstillsyn som är anpassad till deras tjänsters och verksamheters art. Medlemsstaterna ska säkerställa att de behöriga myndigheterna vid behov vidtar åtgärder genom tillsynsåtgärder i efterhand, när de har mottagit bevis på att en leverantör av digitala tjänster inte uppfyller kraven i NIS-direktivet. Sådana bevis får läggas fram av en behörig myndighet i en annan medlemsstat där tjänsten tillhandahålls. Tillsynsmyndigheten kan också få kännedom om att leverantören inte uppfyller kraven från leverantören av digitala tjänster själv, från en annan tillsynsmyndighet eller från en tjänsteanvändare, särskilt efter en incident (skäl 60). Även incidentrapporteringen till CSIRT-enheten kan leda till att tillsynsmyndigheten får sådana bevis.

De behöriga myndigheterna ska ha de befogenheter och medel som krävs för att ålägga leverantörer av digitala tjänster att a) tillhandahålla den information som behövs för en bedömning av säkerheten i deras nätverk och informationssystem, inbegripet dokumenterade säkerhetsprinciper, och b) åtgärda varje underlåtenhet att uppfylla kraven. (artikel 17.1–17.2 b)

Bestämmelser motsvarande NIS-direktivets bestämmelser bör tas in i den nya lagen.

Frågan om vilken myndighet som ska utöva tillsyn över leverantörer av digitala tjänster samt tillsynsmyndighetens befogenheter behandlas i kapitel 8.

10.5 Sanktioner

NIS-direktivet ålägger medlemsstaterna att fastställa regler om sanktioner för överträdelse av nationella bestämmelser som har antagits enligt direktivet och vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska anmäla dessa regler och åtgärder till kommissionen senast den 9 maj 2018 samt utan dröjsmål eventuella ändringar som berör dem. Frågan om sanktioner behandlas i kapitel 9.

10.6 Information till andra medlemsstater och allmänheten samt frivillig incidentrapportering

Frågorna om skyldigheten att lämna information till andra medlemsstater och allmänheten om en incident (artikel 16.6–7) samt frågan om frivillig incidentrapportering (artikel 20.1) behandlas i avsnitt 11.2.3 och 7.3.4.

11 Nationell kontaktpunkt, CSIRT-enhet och samarbetsgrupp

11.1 Nationell kontaktpunkt

11.1.1 Inledning

Enligt NIS-direktivet ska det utses en gemensam nationell kontaktpunkt för säkerhet i nätverk och informationssystem. Rollen kan tilldelas en befintlig myndighet och om bara en behörig myndighet utses ska den behöriga myndigheten också vara gemensam kontaktpunkt (artikel 8.3).

Enligt kommittédirektiven ska Myndigheten för samhällsskydd och beredskap (MSB) anförtros rollen som nationell kontaktpunkt.

11.1.2 Nationell kontaktpunkt i Sverige

Förslag: Myndigheten för samhällsskydd och beredskap ska utses till nationell kontaktpunkt.

Syftet med NIS-direktivet är att förbättra den inre marknadens funktion genom att skapa tillit och förtroende. Därför måste den nationella kontaktpunkten kunna samarbeta effektivt med ekonomiska aktörer och ha en struktur som är förenlig med detta.

Mot bakgrund av det uppdrag som MSB har i dag på informationssäkerhetsområdet samt den kompetens som finns inom myndigheten kan det konstateras att MSB har den struktur som krävs för att samordna frågor angående säkerhet i nätverk informationssystem samt ansvara för kommunikation och gränsöverskridande samarbete i anslutning till detta, se avsnitt 11.1.5. MSB ska därför ha rollen som nationell kontaktpunkt.

11.1.3 Den nationella kontakpunktens uppgift

Förslag: Myndigheten för samhällsskydd och beredskap ska fullgöra de uppgifter som åligger den nationella kontaktpunkten enligt NIS-direktivet samt de uppgifter som regeringen bestämmer.

Den nationella kontaktpunkten ska underlätta gränsöverskridande samarbete och kommunikation samt göra det möjligt att genomföra NIS-direktivet på ett effektivt sätt. Den nationella kontaktpunkten ska ha ansvar för samordningen av frågor angående säkerhet i nätverk informationssystem och gränsöverskridande samarbete på unionsnivå.

Medlemsstaterna ska säkerställa att den nationella kontaktpunkten samarbetar på ett effektivt och säkert sätt i samarbetsgruppen (artikel 8.5), se avsnitt 11.3.

Sambandsfunktion

Den nationella kontaktpunkten ska utöva en sambandsfunktion för att säkerställa gränsöverskridande samarbete mellan medlemsstaternas myndigheter och med de berörda myndigheterna i andra medlemsstater samt med den samarbetsgrupp som inrättas genom NIS-direktivet, se avsnitt 11.3, och CSIRT-nätverket, se avsnitt 11.2.5 (artiklarna 11, 12 och 8.4). Den gemensamma nationella kontaktpunkten ska när det är lämpligt och förenligt med svensk rätt samråda och samarbeta med relevanta nationella rättsvårdande myndigheter och med dataskyddsmyndigheter (artikel 8.6).

Incidentrapportering

Den gemensamma nationella kontaktpunkten ska på begäran av CSIRT-enheten vidarebefordra incidentrapporter till gemensamma nationella kontaktpunkter i andra medlemsstater som påverkats av en incident hos en leverantör av samhällsviktiga tjänster (artikel 14.5).

11.1.4 Samarbetet mellan ansvariga myndigheter

Förslag: Myndigheten för samhällsskydd och beredskap ska årligen lämna en sammanfattande rapport till samarbetsgruppen om de incidentrapporter som mottagits. Av rapporten ska framgå antalet mottagna incidentrapporter, incidenternas art och vidtagna säkerhetsåtgärder.

Tillsynsmyndigheterna, den gemensamma nationella kontaktpunkten och CSIRT-enheten ska samarbeta när det gäller fullgörandet av NIS-direktivet (artikel 10.1).

Den gemensamma nationella kontaktpunkten ska senast den 9 augusti 2018, och därefter en gång om året, lämna en sammanfattande rapport till samarbetsgruppen om de rapporter som mottagits, inklusive antalet rapporter och de rapporterade incidenternas art, samt om vilka åtgärder som vidtagits i enlighet med artiklarna 14.3, 14.5, 16.3 och 16.6 (artikel 10.3).

Rapporten ska säkerställa att medlemsstaterna och kommissionen får information avseende incidentrapporteringen på ett ändamålsenligt sätt. Den sammanfattande rapporten bör utöver uppgifter om antalet mottagna incidentrapporter samt information om de rapporterade incidenternas art, även innehålla information om vilka typer av säkerhetsöverträdelser det rör sig om eller hur allvarliga eller långvariga de varit. Rapporten bör vara anonymiserad för att bevara rapporternas konfidentialitet och identiteten på leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, eftersom information om de rapporterande enheternas identitet inte krävs för utbyte av bästa praxis inom samarbetsgruppen. (skäl 33)

11.1.5 Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskaps uppdrag regleras i förordningen (2008:1002) med instruktion för Myndigheten för samhällskydd och beredskap.

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 eller en kris. Myndigheten ska

- utveckla och stödja samhällets beredskap mot olyckor och kriser och vara pådrivande i arbetet med förebyggande och sårbarhetsreducerande åtgärder,
- arbeta med samordning mellan berörda aktörer i samhället för att förebygga och hantera olyckor och kriser,
- bidra till att minska konsekvenser av olyckor och kriser,
- följa upp och utvärdera samhällets krisberedskapsarbete, och
- se till att utbildning och övningar kommer till stånd inom myndighetens ansvarsområde.

När det gäller förebyggande och förberedande arbete ska myndigheten enligt 2 § i samverkan med myndigheter, kommuner, landsting, 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 § ha förmågan att bistå med stödresurser i samband med allvarliga olyckor och kriser samt stödja samordningen av berörda myndigheters åtgärder vid en kris. Myndigheten ska se till att berörda aktörer vid en kris får tillfälle att

- samordna krishanteringsåtgärderna,
- samordna information till allmänhet och media,
- effektivt använda samhällets samlade resurser och internationella förstärkningsresurser, och
- samordna stödet till centrala, regionala och lokala organ i fråga om information och lägesbilder.

Myndigheten ska ha förmågan att bistå Regeringskansliet med underlag och information i samband med allvarliga olyckor och kriser.

För uppföljning, utvärdering och lärande ska myndigheten enligt 10 § såväl områdesvis som på en övergripande samhällsnivå följa upp och utvärdera krisberedskapen och bedöma om vidtagna åtgärder fått önskad effekt. Vidare ska myndigheten kunna göra en samlad bedömning av olycksutvecklingen och det säkerhetsarbete som är kopplat till den.

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.

När det gäller informationssäkerhet ska myndigheten enligt 11 a § 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 landsting samt företag och organisationer. Myndigheten ska årligen lämna en rapport till regeringen med en sammanställning av de incidenter som rapporterats in till myndigheten enligt 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (KBF). Inför sammanställning av rapporten ska myndigheten inhämta upplysningar från Säkerhetspolisen och Försvarsmakten om de incidenter som rapporterats in till de myndigheterna enligt 10 a § säkerhetsskyddsförordningen (1996:633). Myndigheten ska även rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder inom olika nivåer och områden i samhället. Myndigheten ska enligt 11 b § ansvara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. Myndigheten ska i detta arbete

- 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,
- samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, och

- vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.

Myndigheten ska enligt 17 a § vara Sveriges kontaktpunkt för skydd av europeisk kritisk infrastruktur enligt artikel 10.1 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.

Myndigheten får med stöd av 21 § 1 KBF meddela föreskrifter som behövs för verkställigheten av 8 § KBF om risk- och sårbarhetsanalyser. Enligt 19 § KBF ansvarar varje myndighet för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Därvid ska behovet av säkra ledningssystem särskilt beaktas. Myndigheten får enligt 21 § 2 KBF meddela föreskrifter om sådana säkerhetskrav som avses i 19 § med beaktande av nationell och internationell standard. MSB har utfärdat uppdaterade föreskrifter om statliga myndigheters systematiska informationssäkerhetsarbete i april 2016. I de nya föreskrifterna skärptes kraven på myndigheterna på en rad punkter. Förändringen föranleddes av att en genomförd undersökning av statliga myndigheters informationssäkerhetsarbete påvisat brister. (MSB, En bild av myndigheternas informationssäkerhet, 2014)

I april 2016 infördes ett krav i 20 § KBF på att statliga myndigheter skyndsamt ska rapportera it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandhåller åt en annan organisation. Rapporteringen ska ske till MSB. Myndigheten får med stöd av 21 § 4 KBF, efter att ha gett Polismyndigheten, Säkerhetspolisen och Försvarsmakten tillfälle att yttra sig, meddela de ytterligare föreskrifter som behövs för verkställighet av 20 § första stycket KBF om rapportering av it-incidenter.

Arbetet med informationssäkerhet bedrivs vid *avdelningen för utveckling av samhällskydd* som inbegriper Verksamhet för cybersäkerhet och skydd av samhällsviktig verksamhet. Verksamheten är indelad i fyra enheter.

Enheten för verksamhetssamordning och strategisk analys ansvarar för stöd avseende verksamhetens planering och uppföljning, budgetarbete samt rapportering. Enheten har det sammanhållande ansvaret för att samordna och stödja arbetet med remisser, uppdrag och utredningar samt kommunikations-, forsknings- och studiefrågor, nationell och internationell samverkan. Enheten ansvarar också för att analysera och bedöma omvärldsutvecklingen på området. I detta arbete ingår den årliga rapporten till regeringen samt verksamhetens stöd till bl.a. myndighetens centrala analysprocess.

Enheten för skydd av kritisk infrastruktur och cybersäkerhet ska driva och hålla samman arbetet med skydd av samhällsviktig verksamhet och ansvara för myndighetens uppgifter att vara Sveriges kontaktpunkt för skydd av europeisk kritisk infrastruktur. I detta ingår att stödja och utveckla samhällets arbete med kontinuitetshantering och kritiska beroenden samt att arbeta med rymdvädersamordning. Enheten ska, med fokus på kritisk informationsinfrastruktur, lämna råd och stöd till tekniskt förebyggande arbete inom området till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. Bland annat erbjuds vägledningar som stöd för säkerhet i industriella kontroll- och informationssystem liksom tillgång till övningsverksamhet. Enheten svarar för myndighetens arbete med säkra kryptografiska funktioner för det civila samhället och för arbetet med myndighetens uppdrag vad avser eter- och medieberedskap. Enheten leder och samordnar arbetet med informationssäkerhet i myndighetens externa kommunikationstjänster för ledning och samverkan så att den externa kravställningen tillgodoses. Enheten ansvarar vidare för att analysera och bedöma omvärldsutvecklingen inom sitt område.

Enheten för operativ cybersäkerhet och it-incidenthantering ska upprätthålla funktionen CERT-SE, som är en del av det internationella nätverket av Computer Emergency Response Teams (CERT). Enheten ska vara den operativa kontaktpunkten gentemot motsvarande funktioner i andra länder. Enheten ska säkerställa att verksamheten i sin helhet kan agera skyndsamt vid inträffade it-incidenter genom att sprida information samt vid behov samordna åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade. Enheten tar emot de rapporter som statliga myndigheter lämnar in med anledning av den obligatoriska it-incidentrapporteringen i 20 § KBF. Enheten har ansvar för att operativt stödja

arbetet med it-säkerhet i de av myndighetens externa kommunikationstjänster för ledning och samverkan som kräver detta. Enheten ansvarar för webbplatsen CERT.se. Enheten ansvarar för att analysera och bedöma omvärldsutvecklingen inom sitt område. I detta ingår löpande omvärldsbevakning, att producera och delge anpassad information till relevanta aktörer.

Enheten för systematiskt informationssäkerhetsarbete ska lämna råd och stöd om förebyggande informationssäkerhetsarbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. I detta ingår att lämna råd och stöd till statliga myndigheter, kommuner och landsting i arbetet med risk- och sårbarhetsanalyser samt kontinuitetshantering på området informationssäkerhet. Enheten ansvarar för webbplatsen www.informationssäkerhet.se och förvaltar även det metodstöd som har tagits fram för att underlätta för organisationer att etablera ett systematiskt informationssäkerhetsarbete i enlighet med ISO-standarderna på området. Metodstödet, liksom en rad vägledningar och annat stöd, finns publicerat på www.informationssäkerhet.se. Webbplatsen är ett samarbetsprojekt mellan SAMFI-myndigheterna. Enheten ansvarar för att analysera och bedöma omvärldsutvecklingen inom sitt område.

Myndigheten deltar i nationella samarbeten på informationssäkerhetsområdet och driver ett antal forum i flera sektorer, i syfte att dela information mellan stat, näringsliv och andra relevanta organisationer avseende informationssäkerhetsaspekter (hälso- och sjukvård, finans, drift, telekom och SCADA). Myndigheten driver också mediernas beredskapsråd där målet är att medieföretagen kan förmedla nyheter, samhällsinformation och viktigt meddelande till allmänheten (VMA) i krissituationer och ytterst i krig. Myndigheten driver vidare ett nätverk för myndighetsansvariga i statliga myndigheter (SNITS) i syfte att stödja myndigheterna i deras arbete med informationssäkerhet. Svenskt CERT-forum är ett annat forum som myndigheten driver i syfte att bl.a. diskutera förhållningssätt runt aktuella it-säkerhetshändelser. Utöver de ovan nämnda forumen deltar myndigheten i KIS (kommunnätverket, NIS (Landstingsnätverket) och SWITS som är ett forskningsnätverk. Myndigheten arbetar också med standardisering och ingår i en teknisk standardiseringskommitté.

Myndigheten har, i sin samordningsroll på informationssäkerhetsområdet, knutit till sig ett *informationssäkerhetsråd* med bred

representation från både offentlig förvaltning och näringslivet. Informationssäkerhetsrådet ska i huvudsak bistå myndigheten med

- information om utvecklingstrender inom området informationssäkerhet, det vill säga skydd av information och säkring av informationssystem,
- synpunkter på inriktning, prioritering och genomförande av MSB:s arbete inom området,
- kvalitetssäkring och trovärdighet till MSB:s arbete genom att vara rätt sammansatt och ha koppling till vitala samhällsfunktioner och
- att bidra till spridning av information om MSB:s arbete med informationssäkerhet i omvärlden.

SAMFI är en grupp bestående av myndigheter med särskilda uppgifter inom området informationssäkerhet. Gruppen träffas sex gånger per år och syftet är att underlätta samarbetet genom informationsutbyte och samverkan. I gruppen ingår Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Post- och telestyrelsen, Polismyndigheten, Säkerhetspolisen och MSB. SAMFI bildades 2003 i samband med en framtagen strategi för samhällets informationssäkerhet. SAMFI verkar för säkra informationstillgångar i samhället avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet samt genom informationsutbyte och samverkan stödja de medverkande myndigheternas arbete avseende samhällets informationssäkerhet i syfte att uppfylla visionen. Myndigheten har ansvaret för SAMFI.

Myndigheten deltar i internationella samarbeten som rör informations- och cybersäkerhet, t.ex. policyutveckling, operativt samarbete och informationsdelning. MSB deltar i enlighet med kommittédirektiven i CSIRT-nätverket och samarbetsgruppen som etablerats med anledning av NIS-direktivet. MSB:s övriga internationella samarbete inbegriper bland annat samarbete mellan nordiska nationella CERT-funktioner och samarbete inom nätverket European Governmental CERT:s (EGC), samt internationell samverkan kring säkerhet i itprodukter, säkerhet i industriella informations- och styrsystem, cybersäkerhet i finansiella tjänster och standardisering kopplad till informationssäkerhet (ISO). Myndigheten deltar i den privat-offent-

liga plattformen för nät- och informationssäkerhet (NIS-plattformen) samt representerar Sverige i Natos planeringsgrupp för industriella resurser och kommunikationer (IRCSG). Myndigheten deltar också i internationell övningsverksamhet som exempelvis EU:s Cyber Europe, Natos Cyber Coalition och USA:s Cyber Storm. I flera av dessa övningar arrangerar MSB en nationell övning i anslutning till de nämnda övningarna med ytterligare deltagare.

11.2 Enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet)

11.2.1 Inledning

Varje medlemsstat ska utse en eller flera incidenthanteringsorgan, CSIRT-enheter[1], som ska ansvara för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande. En CSIRT-enhet får inrättas inom en behörig myndighet som uppfyller kraven i bilaga 1 till NIS-direktivet. (artikel 9.1) CSIRT-enheten ska uppfylla grundläggande krav för att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker samt säkerställa ett effektivt samarbete på unionsnivå.

För att alla typer av leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster ska kunna dra nytta av sådan kapacitet och sådant samarbete bör medlemsstaterna säkerställa att alla typer av leverantörer omfattas av en utsedd CSIRT-enhet.

Genom NIS-direktivet har Europarlamentet och rådet inrättat ett nätverk för nationella CSIRT-enheter, CSIRT-nätverket (artikel 1.2 c).

Med tanke på vikten av internationellt samarbete på området cybersäkerhet, bör CSIRT-enheterna kunna delta i andra internationella samarbetsnätverk utöver det CSIRT-nätverk som inrättats genom NIS-direktivet (skäl 34).

CSIRT-enheten ska ha tillgång till lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur på nationell nivå (artikel 9.3).

[1] CSIRT=Computer Security Incident Response Team.

Enligt kommittédirektiven bör Sveriges CSIRT-organisation finnas hos Myndigheten för samhällsskydd och beredskap.

11.2.2 CSIRT-enhet i Sverige

Förslag: Myndigheten för samhällsskydd och beredskap ska utses till CSIRT-enhet.

Kraven på CSIRT-enheten framgår av artikel 9 i NIS-direktivet samt i punkt 1 i bilaga 1 till direktivet. Det är bland annat krav på kommunikationstjänster, säkerhet avseende lokaler och informationssystem, driftskontinuitet och möjligheter till internationellt samarbete.

Myndigheten för samhällsskydd och beredskap (MSB) svarar 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 MSB/CERT-SE:s uppgifter 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 informationssäkerhetsområdet. MSB/CERT-SE är Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder och mot den CERT-organisation som ansvarar för it-incidenthantering inom EU:s institutioner, CERT-EU, och ska utveckla samarbetet och informationsutbytet med dessa funktioner. Det är också MSB/CERT-SE som tar emot de rapporter som statliga myndigheter lämnar med anledning av den obligatoriska it-incidentrapporteringen (20 § KBF). I avvaktan på att ett tekniskt rapporteringsverktyg är driftssatt tillhandahåller MSB/CERT-SE i dag en kryptolösning för säker kommunikation vid överföring av it-incidentrapporterna. Rapporteringsverktyget är tänkt att tas i bruk under 2017.

Mot bakgrund av det uppdrag MSB har på informationssäkerhetsområdet och den kompetens som finns inom myndigheten be-

[2] Computer Emergency Response Team.

dömer utredningen att MSB ska ha rollen som Sveriges CSIRT-enhet. MSB/CERT-SE har också tillgång till sådan lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur som avses i NIS-direktivet (artikel 9.4).

11.2.3 CSIRT-enhetens uppgift

Förslag: Myndigheten för samhällsskydd och beredskap ska fullgöra de uppgifter som åligger CSIRT-enheten enligt NIS-direktivet och punkt 2 i bilaga 1 till NIS-direktivet.

CSIRT-enheten ska ta emot de incidentrapporter som lämnas enligt den nya lagen.

CSIRT-enheten ska informera den eller de andra berörda medlemsstaterna, om en incident som rapporterats av leverantörer av samhällsviktiga tjänster har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i den medlemsstaten.

CSIRT-enheten ska, om det är lämpligt, informera andra medlemsstater som påverkats av en incident som rapporterats av en leverantör av digitala tjänster.

Efter samråd med den rapporterande leverantören av samhällsviktiga tjänster får CSIRT-enheten informera allmänheten om enskilda incidenter. En förutsättning för detta är att allmänheten behöver känna till incidenten för att det ska vara möjligt att förhindra en incident eller åtgärda en pågående incident.

CSIRT-enheten får, efter samråd med den berörda leverantören av digitala tjänster, förplikta leverantören av digitala tjänster att informera allmänheten om enskilda incidenter. En förutsättning för detta är att allmänheten behöver känna till incidenten för att det ska vara möjligt att förhindra en incident eller åtgärda en pågående incident eller om incidentens avslöjande på annat sätt omfattas av allmänintresset.

CSIRT-enheten ska när det är möjligt överlämna relevant information som kan bidra till en effektiv hantering av incidenten och det förebyggande arbetet till den rapporterande leverantören av samhällsviktiga tjänster.

MSB svarar 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.

CSIRT-enhetens uppgift anges i NIS-direktivet samt i punkt 2 i bilaga 1 till NIS-direktivet. Det är bland annat uppgifter som rör incidentrapporteringen, samverkan med privat sektor och gemensam praxis för att underlätta samarbete avseende incidenthantering.

Utredningen har i avsnitt 7.3.2 kommit fram till att CSIRT-enheten ska ta emot de incidentrapporter som upprättas till följd av NIS-direktivet.

Ta emot incidentrapporter

Till CSIRT-enhetens uppgifter hör bland annat att ta emot rapporter om incidenter samt fastställa incidentens eventuella gränsöverskridande verkningar (artiklarna 14.3 och 16.3). Närmare bestämmelser om CSIRT-enhetens uppgifter i samband med incidentrapportering framgår av punkt 2 i bilaga 2 till NIS-direktivet.

Närmare bestämmelser om när leverantörer av samhällsviktiga tjänster är skyldiga att rapportera incidenter samt vilka faktorer som ska användas för att fastställa om en incident har en betydande inverkan enligt artikel 14.4 får meddelas i myndighetsföreskrifter (artikel 14.7), se avsnitt 7.3.2.

Närmare bestämmelser om format och förfarande avseende rapporteringskraven för leverantörer av digitala tjänster ska fastställas i genomförandeakter som antas av kommissionen (artikel 16.9). Medlemsstaterna får inte införa ytterligare rapporteringskrav för leverantörer av digitala tjänster (artikel 16.10).

CSIRT-enheten kommer genom sitt uppdrag att hantera uppgifter om incidenter från leverantörer som tillhandahåller samhällsviktiga tjänster och digitala tjänster. Dessutom hanteras incidenter från statliga myndigheter. Uppgifterna tillsammans kan komma att ge information om sårbarheter i det svenska samhället som kan utgöra information som är av betydelse för Sveriges säkerhet. Vilka krav på som ska ställas på hanteringen av uppgifterna bör bedömas i MSB:s säkerhetskyddsanalys.

Information till andra medlemsstater

CSIRT-enheten eller den behöriga myndigheten ska, mot bakgrund av informationen i rapporten från leverantören av den samhällsviktiga tjänsten, informera den eller de andra berörda medlemsstaterna, om incidenten har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i den medlemsstaten. På begäran av CSIRT-enheten eller den behöriga myndigheten ska den gemensamma kontaktpunkten vidarebefordra rapporterna till gemensamma kontaktpunkter i andra medlemsstater som påverkats av incidenten (artikel 14.5).

När det gäller incidenter som rapporterats av leverantörer av digitala tjänster ska, om så är lämpligt, och särskilt om incidenten berör två eller flera medlemsstater, CSIRT-enheten eller den behöriga myndigheten informera andra medlemsstater som har påverkats (artikel 16.6).

Vid sådan rapportering ska CSIRT-enheten eller den behöriga myndigheten och den nationella kontaktpunkten, i enlighet med unionsrätten eller med nationell lagstiftning som är förenlig med unionsrätten, bevara nämnda leverantörs säkerhetsintressen och kommersiella intressen samt konfidentialiteten hos informationen i leverantörens rapport (artiklarna 14.5 och 16.6). När det gäller uppgifter om produkters sårbara aspekter ska dessa hållas strikt konfidentiella till dess lämpliga säkerhetslösningar har släppts (skäl 59), se kapitel 12.

Utredningen bedömer att CSIRT-enheten ska ha uppgiften att informera andra medlemsstater i samband med rapporterade incidenter.

Information till leverantören

När omständigheterna tillåter ska den behöriga myndigheten eller CSIRT-enheten förse den rapporterande leverantören av samhällsviktiga tjänster med relevant information om uppföljningen av rapporten, såsom information som skulle kunna bidra till effektiv hantering av incidenten (artikel 14.5). En väl fungerande incidenthantering är en viktig del i det förebyggande informationssäkerhetsarbetet och skapar förutsättningar för att anpassa säkerhetsåtgärder allteftersom hot och risker förändras, se avsnitt 7.3.1.

Utredningen bedömer att uppgiften att förse leverantören med information ska anförtros CSIRT-enheten.

Information till allmänheten

Efter samråd med den rapporterande leverantören av samhällsviktiga tjänster får den behöriga myndigheten eller CSIRT-enheten informera allmänheten om enskilda incidenter, om allmänheten behöver känna till dem för att det ska vara möjligt att förhindra en incident eller åtgärda en pågående incident (artikel 14.6).

Efter samråd med den berörda leverantören av digitala tjänster får den behöriga myndigheten eller CSIRT-enheten och, om så är lämpligt, CSIRT-enheter eller behöriga myndigheter i andra berörda medlemsstater, informera allmänheten om enskilda incidenter eller kräva att leverantören av digitala tjänster gör det, om allmänheten behöver känna till dem för att det ska vara möjligt att förhindra en incident eller åtgärda en pågående incident eller om incidentens avslöjande på annat sätt omfattas av allmänintresset (artikel 16.7). Bestämmelsen innebär bl.a. att en leverantör av digitala tjänster kan förpliktas att uppfylla denna informationsskyldighet.

Utredningen bedömer att uppgiften att lämna information till allmänheten bör åligga CSIRT-enheten.

Utredningen ser i och för sig inget hinder mot att CSIRT-enheten eller en behörig myndighet i en annan medlemsstat informerar allmänheten i Sverige om inträffade incidenter så länge det inte är fråga om uppgifter som omfattas av sekretess. Situationen är en annan i det fall CSIRT-enheten eller en behörig myndighet i en annan medlemsstat kräver att en leverantör av digitala tjänster under svensk jurisdiktion själv lämnar information enligt bestämmelsen. I dessa fall bör kravet mot leverantören framställas av den svenska CSIRT-enheten efter samråd inom CSIRT-nätverket eller med den behöriga myndigheten i den andra medlemsstaten.

En bestämmelse om att CSIRT-enheten får förplikta en leverantör av digitala tjänster att informera allmänheten om enskilda incidenter, om allmänheten behöver känna till dem för att det ska vara möjlighet att förhindra en incident eller åtgärda en pågående incident eller om incidentens avslöjande på annat sätt omfattas av allmänintresset, bör införas i den nya lagen.

Vid offentliggörande av incidenter som rapporteras till CSIRT-enheten bör allmänhetens intresse av att få information om hot vägas mot eventuell renomméskada och kommersiell skada för de leve-

rantörer av samhällsviktiga tjänster och de leverantörer av digitala tjänster som rapporterar incidenter (skäl 59).

CSIRT-enheter som deltar i CSIRT-nätverket uppmanas att på frivillig grund tillhandahålla den information som ska offentliggöras på den webbplats som CSIRT-nätverket föreslås upprätta, utan att inkludera konfidentiell eller känslig information (skäl 40).

11.2.4 Brottslig verksamhet

Förslag: CSIRT-enheten ska skyndsamt uppmana leverantörer av samhällsviktiga tjänster och digitala tjänster att anmäla incidenter som har sin grund i en brottslig gärning till polisen.

Incidenter kan vara en följd av brottslig verksamhet, vars förebyggande, utredning och lagföring stöds av samordning och samarbete mellan leverantörer av samhällsviktiga tjänster, leverantörer av digitala tjänster, behöriga myndigheter och rättsvårdande myndigheter. Om en incident misstänks ha samband med allvarlig brottslig verksamhet enligt unionsrätt eller nationell rätt, bör medlemsstaterna uppmuntra leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster att rapportera incidenter som misstänks vara av allvarlig brottslig art till de relevanta rättsvårdande myndigheterna. När så är lämpligt är det önskvärt att samordningen mellan behöriga myndigheter och rättsvårdande myndigheter i olika medlemsstater underlättas av Europeiska it-brottscentrumet (EC3) och Enisa. (skäl 62)

När det gäller statliga myndigheters incidentrapportering ska MSB, om det kan antas att incidenten har sin grund i en brottslig gärning, skyndsamt uppmana den rapporterande myndigheten att anmäla incidenten till polisen (20 § fjärde stycket KBF).

Frågan om hur polisens tillgång till information om vissa it-incidenter ska öka har behandlats i departementspromemorian *Polisens tillgång till information om vissa it-incidenter* (Ds 2016:22). I promemorian förslås när det gäller statliga myndigheters incidentrapportering en skyldighet för MSB att lämna uppgift om sådana incidenter som rapporterats enligt 20 § första stycket KBF till Polismyndigheten om det finns anledning att anta att incidenten har sin grund i en brottslig gärning. Alternativt framhålls en möjlighet att regeringen

genom myndighetsstyrning säkerställer att ett effektivt och ändamålsenligt informationssamarbete etableras mellan myndigheterna.

Det har kommit till utredningens kännedom att MSB och Polismyndigheten nu har träffat en överenskommelse om informationsutbytet.

I departementspromemorian görs också bedömningen att varken bestämmelser om sekretess eller bestämmelser om behandling av personuppgifter normalt utgör ett hinder mot att MSB lämnar information om rapporterade it-angrepp till Polismyndigheten. Vidare framgår att bestämmelserna om sekretess i de brottsbekämpande myndigheternas verksamhet och regelverket i övrigt ger myndigheterna goda förutsättningar att skydda skyddsvärda uppgifter om it-incidenter under utredningen och i domstol vid ett eventuellt åtal.

Utredningens bedömning är att MSB, som föreslås vara CSIRT-enhet, skyndsamt ska uppmana leverantörer av samhällsviktiga tjänster och digitala tjänster att anmäla incidenten som har sin grund i en brottslig gärning till polisen. I kravet på att uppmana leverantören ingår, enligt utredningens uppfattning, att i samtliga fall där leverantören inte själv anmält incidenten till polisen kontakta leverantören och undersöka orsaken till att incidenten inte polisanmälts.

När det gäller polisens tillgång till information om incidenter som har sin grund i en brottslig gärning bör informationssamarbetet mellan MSB och Polismyndigheten hanteras på samma sätt som information om incidenter som rapporteras av statliga myndigheter.

Utredningen anser att det är viktigt att alla it-incidenter som kan antas utgöra ett brott anmäls och utreds samt att individer som begår denna typ av brott lagförs. I samband med tillkomsten av den bestämmelse som reglerar förutsättningarna för myndigheter att utan hinder av sekretess lämna information om misstänkta brott till brottsutredande myndigheter, 10 kap. 24 § OSL, uttalas i förarbetena följande (prop. 1983/84:142 s. 19 och 21).

> För att ett rättssamhälle skall fungera på ett tillfredsställande sätt fordras att samhället ingriper mot brott. Uppgiften att bekämpa brottsligheten ligger i första hand på polisen och åklagarna.
>
> – – –
>
> Brottsbekämpningen bygger […] inte enbart på polisens övervakande och brottsspanande verksamhet. En solidarisk medverkan från allmänheten utgör en förutsättning för att brottsligheten skall kunna bekämpas effektivt. Även insatser från andra myndigheter är betydelse-

> fulla. Andra myndigheter har i många fall en rätt och ibland t.o.m. en skyldighet att lämna ut uppgifter om brott till polis eller åklagare. Detta gäller inte sällan även om uppgifterna i övrigt är skyddade av sekretess.
>
> – – –
>
> Myndigheterna kan delta i kampen mot brottsligheten på många olika sätt. En betydelsefull form av medverkan består i att lämna uppgifter om brott till de direkt brottsbekämpande myndigheterna.

Att it-brott inte beivras kan på sikt leda till stora kostnader och konsekvenser för samhället. Regeringen bör därför noga följa upp i vilken utsträckning leverantörerna själva anmäler incidenter som kan antas utgöra brott till polisen samt utvärdera hur informationsutbytet mellan MSB och Polismyndigheten påverkar brottsbekämpningen när det gäller incidenter som rapporterats med stöd av den nya lagen.

11.2.5 CSIRT-nätverket

Bedömning: I MSB:s roll som Sveriges CSIRT-enhet ingår att delta i CSIRT-nätverket. MSB ska samarbeta i nätverket på ett ändamålsenligt, effektivt och säkert sätt.

CSIRT-nätverket ska bidra till utveckling av förtroende och tillit mellan medlemsstaterna och främja ett snabbt och effektivt operativt samarbete (artikel 12.1).

CSIRT-nätverket ska bestå av företrädare för medlemsstaternas CSIRT-enheter och CERT-EU. Kommissonen ska delta i CSIRT-nätverket som observatör. Enisa (Europeiska unionens byrå för nät- och informationssäkerhet) ska tillhandahålla sekretariat och aktivt stödja samarbetet mellan CSIRT-enheterna. (artikel 12.2)

CSIRT-nätverket ska ha de uppgifter som följer av artikel 12.3–5 i NIS-direktivet.

CSIRT-nätverket ska informera samarbetsgruppen om sin verksamhet (artikel 12.2 g). Med avseende på den översyn som kommissionen ska göra ska CSIRT-nätverket, senast den 9 augusti 2018 och därefter med 1,5 års mellanrum, utarbeta en rapport med en bedömning av erfarenheterna av det operativa samarbetet enligt artikel 12,

inklusive slutsatser och rekommendationer. Rapporten ska även överlämnas till samarbetsgruppen.

Information om incidenter blir allt mer värdefull för allmänheten och företag, särskilt för små och medelstora företag. I vissa fall tillhandahålls sådan information redan via webbplatser på nationell nivå, på ett specifikt lands språk, och är främst inriktad på incidenter och händelser med en nationell dimension. Eftersom företag i allt större utsträckning bedriver gränsöverskridande verksamhet och medborgare använder onlinetjänster, bör information om incidenter tillhandahållas i samlad form på unionsnivå. CSIRT-nätverkets sekretariat uppmuntras att upprätta en webbplats eller upplåta utrymme åt en särskild sida på en befintlig webbplats, där allmän information om allvarliga incidenter i unionen görs tillgänglig för allmänheten. Informationen ska vara särskilt inriktad på företags intressen och behov. (skäl 40)

Övningar där incidentscenarier simuleras i realtid är viktiga för att testa medlemsstaternas beredskap och samarbete när det gäller säkerhet i nätverk informationssystem. Övningsserien CyberEurope, som samordnas av Enisa med deltagande av medlemsstaterna är ett användbart verktyg för att testa och utarbeta rekommendationer för hur incidenthanteringen på unionsnivå bör förbättras med tiden. Med tanke på att medlemsstaterna för närvarande inte har någon skyldighet att vare sig planera eller delta i övningar, bör inrättandet av CSIRT-nätverket enligt NIS-direktivet göra det möjligt för medlemsstaterna att delta i övningar på grundval av noggrann planering och strategiska val. Den samarbetsgrupp som inrättas enligt NIS-direktivet bör diskutera de strategiska besluten om övningar, särskilt men inte enbart, när det gäller övningarnas regelbundenhet och utformningen av scenarierna. MSB representerar Sverige i samarbetsgruppen. Enisa bör i enlighet med sitt mandat stödja anordnandet och genomförandet av unionsomfattande övningar genom att tillhandahålla expertis och rådgivning till samarbetsgruppen och CSIRT-nätverket (skäl 42).

I MSB:s roll som Sveriges CSIRT-enhet ingår att delta i det CSIRT-nätverk som inrättats. MSB ska samarbeta i nätverket på ett ändamålsenligt, effektivt och säkert sätt (artikel 9.2).

11.2.6 Samarbetet mellan ansvariga myndigheter

Förslag: CSIRT-enheten ska skyndsamt överlämna incidentrapporterna till den tillsynsmyndighet som utövar tillsyn över den rapporterande leverantören.

Tillsynsmyndigheten, den nationella kontaktpunkten och CSIRT-enheten ska samarbeta när det gäller fullgörandet av NIS-direktivet (artikel 10.1).

CSIRT-enheten ska informera den nationella kontaktpunkten om de incidentrapporter som lämnats in enligt NIS-direktivet samt de övriga uppgifter som den nationella kontaktpunkten behöver för sin rapportering till samarbetsgruppen. (artikel 10.3). Detta ankommer på MSB i rollen som både nationell kontaktpunkt och CSIRT-enhet.

Incidentrapporteringen är ett viktigt underlag för de tillsynsmyndigheter som övervakar tillämpningen av den nya lagen. Det möjliggör både utövandet av en effektiv tillsyn och identifiering av brister som behöver åtgärdas genom t.ex. förelägganden och nya föreskrifter.

Mot bakgrund av att incidentrapporteringen ska göras till CSIRT-enheten behövs det en bestämmelse som reglerar skyldigheten för CSIRT-enheten att överlämna relevanta incidentraporter till respektive tillsynsmyndighet. När det är möjligt ska CSIRT-enheten också förse den rapporerande leverantören med annan relevant information.

11.3 Samarbetsgrupp

11.3.1 Inledning

Europaparlamentet och rådet inrättar genom NIS-direktivet en samarbetsgrupp i syfte att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna och att utveckla förtroende och tillit mellan dem i syfte att uppnå en hög gemensam nivå på säkerheten i nätverk informationssystem i unionen (artiklarna 1.2 b och 11.1).

I kommittédirektiven anges att Myndigheten för samhällsskydd och beredskap (MSB) ska delta i den samarbetsgrupp som skapats.

11.3.2 Företrädare för Sverige i samarbetsgruppen

Bedömning. Myndigheten för samhällsskydd och beredskap ska företräda Sverige i samarbetsgruppen.

Mot bakgrund av det uppdrag som MSB har i dag på informationssäkerhetsområdet samt den kompetens som finns inom myndighet ska MSB företräda Sverige i samarbetsgruppen.

11.3.3 Samarbetsgruppens uppgifter

Bedömning. Myndigheten för samhällsskydd och beredskap ska fullgöra de uppgifter som ankommer på den som företräder Sverige i samarbetsgruppen enligt NIS-direktivet samt de uppgifter som regeringen bestämmer.

Samarbetsgruppen ska ha de uppgifter som följer av artikel 11.3 i NIS-direktivet och ska utföra sina uppgifter på grundval av tvååriga arbetsprogram (artikel 11.1 och 11.3 andra stycket). Arbetsprogrammet med åtgärder som ska vidtas för att genomföra gruppens mål och uppgifter ska överensstämma med målen för NIS-direktivet. Arbetsprogrammen utarbetas av samarbetsgruppen och det första ska vara klart senast den 9 februari 2018.

Samarbetsgruppen består av företrädare för medlemsstaterna, kommissionen och Enisa (Europeiska unionens byrå för nät- och informationssäkerhet). När det är lämpligt får samarbetsgruppen bjuda in företrädare för de berörda parterna att delta i arbetet. Kommissionen tillhandhåller sekretariat. (artikel 11.2)

Förfarandet för samarbetsgruppens verksamhet framgår av genomförandeakter som ska antas av kommissionen (artikel 11.5).

Samarbetsgruppen ska också hjälpa medlemsstaterna att tillämpa ett enhetligt tillvägagångssätt i förfarandet för identifieringen av leverantörer av samhällsviktiga tjänster (artiklarna 5.6 och 11.3 l). För att samarbetsgruppen ska få information om incidenter ska den nationella kontaktpunkten lämna en sammanfattande rapport till samarbetsgruppen, se avsnitt 11.1.4. CSIRT-nätverket ska informera samarbetsgruppen om sin verksamhet samt delge rapport om erfarenheter och samarbetet i CSIRT-nätverket, se avsnitt 11.2.5.

Eftersom de flesta nätverk och informationssystem drivs privat är det mycket viktigt med samarbete mellan offentlig och privat sektor. Leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster bör uppmuntras att upprätta egna informella samarbetsmekanismer för att säkerställa säkerheten i nätverk informationssystem. Samarbetsgruppen bör vid behov kunna bjuda in berörda parter till diskussionerna. För att effektivt uppmuntra utbyte av information och bästa praxis är det mycket viktigt att säkerställa att samarbetet inte leder till nackdelar för de leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster som deltar i sådana utbyten. (skäl 35)

För att bygga upp kapacitet och kunskap bland medlemsstaterna bör samarbetsgruppen också fungera som ett instrument för utbyte av bästa praxis, diskussioner om medlemsstaternas kapacitet och beredskap och, på frivillig grund, bistå medlemmarna vid utvärdering av nationella strategier för säkerhet i nätverk informationssystem, vid kapacitetsuppbyggnad och utvärderingar av övningar som avser säkerheten i nätverk informationssystem. (skäl 36)

Samarbetsgruppens och Enisas respektive uppgifter är beroende av och kompletterar varandra. Enisa bör generellt bistå samarbetsgruppen i utförandet av dess uppgifter i enlighet med Enisas mål enligt Europaparlamentets och rådets förordning (EU) nr 526/2013[3], nämligen att bistå unionens institutioner, organ och byråer samt medlemsstaterna med att genomföra de strategier som krävs för att uppfylla rättsliga och regleringsmässiga krav på säkerhet i nätverk informationssystem i befintliga och framtida unionsrättsakter. Enisa bör särskilt tillhandahålla bistånd på de områden som motsvarar dess egna uppgifter enligt förordning (EU) nr 526/2013, nämligen att analysera strategier för säkerhet i nätverk informationssystem, stödja anordnandet och genomförandet av övningar på unionsnivå som avser säkerhet i nätverk informationssystem samt utbyta information och bästa praxis vad gäller åtgärder för ökad medvetenhet och utbildning. Enisa bör också delta i utarbetandet av riktlinjer för sektorspecifika kriterier för fastställande av hur betydande en incidents inverkan är. (skäl 38)

[3] Europaparlamentets och rådets förordning (EU) nr 526/2013 av den 21 maj 2013 om Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och om upphävande av förordning (EG) nr 460/2004.

I syfte att främja avancerad säkerhet i nätverk informationssystem bör samarbetsgruppen vid behov samarbeta med berörda unionsinstitutioner, -organ, och -byråer för att utbyta sakkunskap och bästa praxis samt ge råd om säkerhetsaspekter på nätverk informationssystem som kan påverka deras arbete, samtidigt som befintliga arrangemang för utbyte av konfidentiell information respekteras. Vid samarbete med rättsvårdande myndigheter om säkerhetsaspekter på nätverk informationssystem som kan påverka deras arbete bör samarbetsgruppen respektera befintliga informationskanaler och etablerade nätverk. (skäl 39)

Övningar där incidentscenarier simuleras i realtid är viktiga för att testa medlemsstaternas beredskap och samarbete när det gäller säkerhet i nätverk informationssystem. Övningsserien CyberEurope, som samordnas av Enisa med deltagande av medlemsstaterna är ett användbart verktyg för att testa och utarbeta rekommendationer för hur incidenthanteringen på unionsnivå bör förbättras med tiden. Med tanke på att medlemsstaterna för närvarande inte har någon skyldighet att vare sig planera eller delta i övningar, bör inrättandet av CSIRT-nätverket enligt NIS-direktivet göra det möjligt för medlemsstaterna att delta i övningar på grundval av noggrann planering och strategiska val. Den samarbetsgrupp som inrättas enligt NIS-direktivet bör diskutera de strategiska besluten om övningar, särskilt men inte enbart när det gäller övningarnas regelbundenhet och utformningen av scenarierna. Enisa bör i enlighet med sitt mandat stödja anordnandet och genomförandet av unionsomfattande övningar genom att tillhandahålla expertis och rådgivning till samarbetsgruppen och CSIRT- nätverket. (skäl 42)

Mot bakgrund av samarbetsgruppens uppgifter kommer Sveriges företrädare, MSB, behöva samverka med övriga ansvariga myndigheter enligt NIS-direktivet och övriga som berörs av NIS-direktivet. Det ankommer på MSB att fullgöra de uppgifter som följer av denna samverkan (artikel 8.5).

12 Sekretess

12.1 Inledning

Utredaren ska ta ställning till om bestämmelserna i offentlighets- och sekretesslagen (2009:400) (OSL) innebär ett tillräckligt skydd för uppgifter som kan komma att rapporteras med anledning av en it-incident eller om nuvarande lagstiftning behöver ändras och vid sådant behov föreslå författningsändringar.

Utredaren ska vidare undersöka om det behövs en uppgiftsskyldighet för att uppgifter som följer av direktivet ska kunna delas mellan de svenska aktörer som träffas av direktivet och Myndigheten för samhällsskydd och beredskap (MSB) och vid behov föreslå författningsändringar. Utredaren ska också ta ställning till behovet av författningsändringar för att möjliggöra utbyte av andra uppgifter än sådana som rör rikets säkerhet med andra medlemsstater och kommissionen och vid behov föreslå sådana ändringar.

De bestämmelser som av intresse är bestämmelser om sekretess till skydd främst för intresset av att förebygga eller beivra brott (18 kap. OSL), sekretess till skydd för det allmännas ekonomiska intresse (19 kap. OSL), sekretess till skydd för enskild i verksamhet som avser tillsyn m.m. i fråga om näringslivet (30 kap. OSL), bestämmelser om utlämnande (8 kap. OSL), sekretess till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer (15 kap. OSL) och sekretessbrytande bestämmelser (10 kap. OSL).

Offentlighetsprincipen

Offentlighetsprincipen har olika beståndsdelar. Bestämmelserna i regeringsformen (RF) om yttrande- och informationsfrihet gäller för dem som är verksamma hos det allmänna – de s.k. offentliga funktionärerna – lika väl som för medborgarna i allmänhet. I RF slås också

principen om domstolsförhandlingars offentlighet fast. Tryckfrihetsförordningen (TF) innehåller å sin sida bestämmelser om – förutom tryckfriheten – allmänna handlingars offentlighet samt om den s.k. meddelarfriheten, som innebär stora möjligheter att lämna information för publicering i tidningar och andra tryckta skrifter. Såvitt gäller andra grundlagsskyddade medier än tryckta skrifter finns bestämmelser om meddelarfrihet i yttrandefrihetsgrundlagen (YGL).

Med handling förstås enligt 2 kap. 3 § första stycket TF en framställning i skrift eller bild eller en upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. En handling är allmän om den förvaras hos en myndighet och enligt 6 eller 7 §§ TF är att anse som inkommen till eller upprättad hos en myndighet.

Bestämmelserna om allmänna handlingars offentlighet finns i 2 kap. TF. Enligt 2 kap. 2 § andra stycket TF ska varje begränsning i rätten att ta del av allmänna handlingar anges noga i en särskild lag eller i en annan lag som den förstnämnda lagen hänvisar till. Den särskilda lag som åsyftas är OSL.

Bestämmelser om sekretess

Rätten att ta del av allmänna handlingar får enligt 2 kap. 2 § TF begränsas endast när det är påkallat med hänsyn till sju olika uppräknade intressen. Flertalet punkter avser det allmännas intressen, bl.a. det allmännas ekonomiska intresse (p. 5). Punkten 6 avser enskildas intressen, nämligen skyddet för enskilds personliga eller ekonomiska förhållanden.

Sekretess innebär ett förbud att röja en uppgift, oavsett om det sker genom utlämnande av en handling eller genom att röja uppgiften muntligen eller på något annat sätt (3 kap. 1 § OSL). Sekretessen innebär dels handlingssekretess, dels tystnadsplikt. Till den del sekretessen innebär tystnadsplikt innebär den en begränsning av yttrandefriheten enligt regeringsformen, och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Förbudet att röja eller utnyttja en uppgift enligt OSL eller annan lagstiftning som OSL hänvisar till gäller för myndigheter. Det finns dock kompletterande bestämmelser om tystnadsplikt i en-

skilda verksamheter, t.ex. 16 § elberedskapslagen (1997:288) och 6 kap. 12 § patientsäkerhetslagen (2010:659).

Sekretess gäller som huvudregel inte bara i förhållande till enskilda utan också mellan myndigheter och inom en myndighet, om det där finns olika verksamhetsgrenar som är att betrakta som självständiga i förhållande till varandra (8 kap. 1 och 2 §§ OSL). I vissa fall måste dock myndigheter kunna utbyta uppgifter för att kunna utföra sina uppgifter. Sekretessregleringen innehåller därför särskilda sekretessbrytande bestämmelser (10 kap. OSL). Dessa har utformats efter en intresseavvägning mellan myndigheternas behov av att utbyta uppgifter och det intresse som den aktuella sekretessbestämmelsen avser att skydda.

Sekretessens styrka bestäms i regel med hjälp av s.k. skaderekvisit. Man skiljer mellan raka och omvända skaderekvisit. Vid *raka skaderekvisit* är utgångspunkten att uppgifterna är offentliga och att sekretess bara gäller om det kan antas att en viss skada uppkommer om uppgiften röjs. Det *omvända skaderekvisitet* har den omvända utgångspunkten, dvs. det uppställer sekretess som huvudregel. Vid ett omvänt skaderekvisit gäller således sekretess om det inte står klart att uppgiften kan röjas utan att viss skada uppstår. En del bestämmelser innehåller ett *kvalificerat rakt skaderekvisit*, dvs. det krävs särskilt mycket för att sekretessen ska gälla. Sekretessen enligt en bestämmelse kan även vara *absolut*. Vid absolut sekretess ska uppgifter som omfattas av bestämmelsen hemlighållas oavsett skada. Någon skadeprövning ska inte göras i dessa fall.

Utbyte av uppgifter med krav på bevarande av konfidentialiteten enligt NIS-direktivet

Utan att det påverkar tillämpningen av artikel 346 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) får information som är konfidentiell enligt unionsbestämmelser och nationella bestämmelser, såsom bestämmelser om affärshemligheter, utbytas med kommissionen och andra relevanta myndigheter endast när sådant utbyte är nödvändigt för att tillämpa NIS-direktivet. Den information som utbyts ska begränsas till vad som är relevant och proportionellt för ändamålet med utbytet. Vid sådant utbyte ska informationens konfidentialitet bevaras och säkerhetsintressen och kommersiella

intressen hos leverantörer av såväl samhällsviktiga tjänster som digitala tjänster skyddas. (artikel 1.5)

Av artikel 346 EUF-fördraget framgår följande.

> 1. Bestämmelserna i fördragen ska inte hindra tillämpningen av följande regler:
>
> a) Ingen medlemsstat ska vara förpliktad att lämna sådan information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen.
>
> b) Varje medlemsstat får vidta åtgärder, som den anser nödvändiga för att skydda sina väsentliga säkerhetsintressen i fråga om tillverkning av eller handel med vapen, ammunition och krigsmateriel; sådana åtgärder får inte försämra konkurrensvillkoren på den inre marknaden vad gäller varor som inte är avsedda speciellt för militärändamål.
>
> 2. Rådet får på förslag från kommissionen genom enhälligt beslut ändra den lista som rådet den 15 april 1958 fastställde över varor på vilka bestämmelserna i punkt 1b ska tillämpas.

Leverantörer av samhällsviktiga tjänster ska rapportera incidenter som har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänster de tillhandahåller till CSIRT-enheten vid MSB. Mot bakgrund av informationen i rapporten ska CSIRT-enheten informera andra berörda medlemsstater, om incidenten har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i den medlemsstaten. Därvid ska CSIRT-enheten, i enlighet med unionsrätten eller med nationell lagstiftning som är förenlig med unionsrätten, bevara nämnda leverantörs säkerhetsintressen och kommersiella intressen samt konfidentialiteten hos informationen i leverantörens rapport. (artikel 14.3 och 14.5). CSIRT-enheten ska enligt den förordning som utredningen föreslår också skyndsamt överlämna incidentrapporterna till den tillsynsmyndighet som utövar tillsyn över den rapporterande leverantören. När det är möjligt ska CSIRT-enheten också förse den rapporterande leverantören med annan relevant information.

Leverantören kan åläggas att tillhandahålla tillsynsmyndigheten information som är nödvändig för att bedöma säkerheten i nätverk och informationssystem, inklusive dokumenterade säkerhetsprinciper, liksom information om resultaten av en genomförd säkerhetsrevision inklusive de underliggande dokumenten (artikel 15.2).

Leverantörer av digitala tjänster ska rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av tjänsten till CSIRT-enheten. Om det är lämpligt, och särskilt om incidenten berör två eller fler medlemsstater, ska CSIRT-enheten informera andra med-

lemsstater som påverkats. Därvid ska CSIRT-enheten, i enlighet med unionsrätten eller nationell lagstiftning som är förenlig med unionsrätten, bevara leverantören av digitala tjänsters säkerhetsintressen och kommersiella intressen samt den tillhandahållna informationens konfidentialitet (artikel 16.2 och 16.6).

Leverantören kan åläggas att tillhandahålla tillsynsmyndigheten information som är nödvändig för att bedöma säkerheten i nätverk och informationssystem inklusive dokumenterade säkerhetsprinciper (artikel 17.2).

12.2 Behövs ett starkare skydd för uppgifter som ska rapporteras med anledning av en incident eller som ska tillhandahållas i samband med tillsyn?

Förslag: En ny punkt ska införas i bilagan till offentlighets- och sekretessförordningen (2009:641): tillsyn enligt lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster.

Bedömning: Skyddet för uppgifter som ska rapporteras och delas med anledning av incidenter samt tillhandahållas i samband med tillsyn enligt lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster samt förordningen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster är tillgodosett genom bestämmelserna i OSL förutom när det gäller skyddet för enskilds affärs- eller driftförhållande.

Nuvarande sekretesskydd i 18 kap. 8 § 3 OSL är tillräckligt för att skydda uppgifter i incidentrapporteringen.

Leverantörer av samhällsviktiga tjänster och digitala tjänster är enligt NIS-direktivet skyldiga att rapportera incidenter. Det kan röra sig om uppgifter om namn och kontaktuppgifter på den som rapporterat, beskrivning av incidenten, när den inträffat, uppgift om incidenten är pågående eller avslutad, vilken kategori incidenten tillhör samt bedömning av omfattning och konsekvenser av incidenten.

Leverantörer av samhällsviktiga tjänster och digitala tjänster kan även behöva lämna känslig information om bl.a. säkerhets- och bevakningsåtgärder till tillsynsmyndigheten, såsom uppgifter om säkerheten i nätverk och informationssystem samt uppgifter om säkerhetsprinciper. Leverantörer av samhällsviktiga tjänster ska även tillhandahålla uppgifter om genomförda säkerhetsrevisoner.

Uppgifterna som rapporteras eller tillhandhålls kan även röra den rapporterande aktörens ekonomiska verksamhet.

Nedan följer en genomgång av bestämmelser i OSL som kan vara aktuella.

Sekretess till skydd för säkerhets- eller bevakningsåtgärd

I 18 kap. 8 § OSL finns bestämmelser om sekretess för olika brottsförebyggande åtgärder som i huvudsak hänför sig till annan verksamhet än polisens.

Vissa av åtgärderna syftar endast mera indirekt till att förebygga brott. De åtgärder som aktualiseras i samband med incidentrapporteringen återfinns i punkterna 3 och 4. Bestämmelserna är tillämpliga både hos den myndighet som upprättar och skickar in en incidentrapport och hos den myndighet som tar emot rapporten. Motsvarande gäller när uppgifter tillhandahålls i samband med en tillsyn.

Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser telekommunikation eller system för automatiserad behandling av information, (tredje punkten) eller behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling (fjärde punkten) (18 kap. 8 § 3 och 4 OSL).

Som exempel på säkerhets- eller bevakningsåtgärder nämns i förarbetena[1] funktioner för användning av lösenord, loggning och kryptering, installation av brandväggar och antivirusprogram samt administrativa rutiner för t.ex. utdelning av lösenord eller bevakning av loggar och larm. Både uppgifter som direkt lämnar upplysningar om säkerhets- eller bevakningsåtgärder avseende sådana system och uppgifter som kan bidra till att lämna upplysningar om sådana åt-

[1] Prop. 2003/04:93 s 82 f.

gärder kan hemlighållas om det kan antas att syftet med de vidtagna åtgärderna motverkas om uppgifterna röjs. Som exempel på uppgifter som kan bidra till att lämna upplysningar om säkerhets- eller bevakningsåtgärder nämns t.ex. i förarbetena uppgift om vilken typ och version av operativsystem som använts. Sådana uppgifter kan hemlighållas om t.ex. en viss version av ett operativsystem har visat sig ha svagheter som gör att det är lätt att olovligen ta sig in i systemet trots de vidtagna skyddsmekanismerna. En uppgift om vilket operativsystem som används skulle i ett sådant fall indirekt innebära en anvisning för den datatekniskt kunnige om hur man kringgår de vidtagna skyddsåtgärderna. Beskrivningar av hur ett program fungerar i stora drag och vilka typer av uppgifter som bearbetas i ett program bör dock alltid kunna lämnas utan att det kan antas att vidtagna säkerhetsåtgärder motverkas.

Den för incidentrapporteringen mest relevanta sekretessbestämmelsen är bestämmelsen i tredje punkten, angående system för automatiserad behandling av information. Med system för automatiserad behandling av information avses system där datorer, telekommunikation eller annan teknisk utrustning samverkar för att insamla, ordna, bearbeta, söka och distribuera information. Om en myndighets informationssystem har slutat att fungera eller om vissa svagheter i systemet har upptäckts och en incidentrapport lämnas till tillsynsmyndigheten eller till myndighet som tar emot rapporten kan uppgiften om vem som har lämnat rapporten utgöra en säkerhetsrisk, eftersom uppgiften innebär en upplysning om att den aktuella organisationens säkerhetssystem är sårbart. Även en sådan uppgift kan falla under bestämmelsen under förutsättning att skaderekvisitet är uppfyllt.

Sekretessen enligt fjärde punkten, avseende uppgift om åtgärd som avser behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling, gäller i första hand uppgifter om behörighetskoder och behörighetsnycklar samt arrangemang och fördelning av dessa, däremot inte generellt program för hemliga upptagningar. Bestämmelsen gäller inte bara behörighet avseende upptagningar som utgör hemliga, allmänna handlingar i tryckfrihetsförordningens mening, utan gäller behörighet avseende alla typer av handlingar.

Sekretess till skydd för chiffer, kod m.m.

Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod, om det kan antas att syftet med metoden motverkas om uppgiften röjs och metoden har till syfte att antingen underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, eller göra det möjligt att kontrollera om data i elektronisk form har förvanskats (18 kap. 9 § OSL). Sekretessen gäller oberoende av hos vilken myndighet uppgifterna finns. Inom ramen för it-incidentrapporteringen och en tillsyn eller säkerhetsrevision kan uppgifter om chiffer, kod eller liknande metoder som används av informationssäkerhetsskäl komma att hanteras i samband med en teknisk analys av en incident och i tillsynsarbetet.

Sekretess till skydd för det allmännas ekonomiska intresse

Sekretess gäller i en myndighets affärsverksamhet för uppgift om myndighetens affärs- eller driftförhållanden, om det kan antas att någon som driver likartad rörelse gynnas på myndighetens bekostnad om uppgiften röjs. Under motsvarande förutsättning gäller sekretess hos en myndighet för uppgift om affärs- eller driftförhållanden hos bolag, förening, samfällighet eller stiftelse som driver affärsverksamhet och där det allmänna genom myndigheten utövar ett bestämmande inflytande eller bedriver revision (19 kap. 1 § första stycket).

Med affärs- eller driftförhållanden avses förvärv, överlåtelser, upplåtelser eller användning av egendom, tjänster eller annat. Vidare omfattas affärshemligheter av mera allmänt slag, marknadsundersökningar, marknadsplaneringar, prissättningskalkyler och planer rörande reklamkampanjer. Nämnas kan också sådant som konstruktionsarbeten, utredningar av annat slag, prov, förhandlingar och andra affärshändelser.[2] Som exempel kan nämnas att Luftfartsverkets drifthandböcker har ansetts omfattas av sekretess.[3]

Av förarbetena till sekretesslagen framgår att bestämmelsen i första hand tar sikte på att skydda uppgifter hos de affärsdrivande verken men det nämns också att begreppet affärsverksamhet inte

[2] Prop. 1979/80:2 del A s. 145.
[3] Kammarrätten i Jönköpings dom den 15 november 2011, mål nr 2662-11.

får fattas alltför snävt. Enligt vad som uttalas i förarbetena är det utmärkande för affärsverksamhet i allmänhet att verksamheten bedrivs under krav på viss vinst eller åtminstone att den går ihop ekonomiskt, låt vara att den kan vara delvis subventionerad. Det är vidare i allmänhet fråga om verksamhet som inte kan sägas bestå i fullgörande av förvaltningsuppgift i snäv bemärkelse.[4] Enligt vad regeringen uttalade i prop. 1992/93:43 s. 12 f. om ökad konkurrens i kommunal verksamhet får de delar av kommunernas och landstingens verksamheter som är konkurrensutsatta anses utgöra annat än fullgörande av förvaltningsuppgifter i snäv bemärkelse. Regeringen bedömde att sekretessbestämmelsen därför torde kunna vara tillämplig på sådan konkurrensutsatt verksamhet hos kommunerna och landstingen.[5]

Får en myndighet en uppgift som är sekretessbelagd enligt 19 kap. 1 § från en annan myndighet blir 1 § tillämplig på uppgiften också hos den mottagande myndigheten under förutsättning att uppgiften inte ingår i ett beslut av den mottagande myndigheten.

Sekretess till skydd för enskilds affärs- eller driftförhållanden

Uppgifter kan även vara känsliga med hänsyn till leverantörernas ekonomiska verksamhet. Utredningen ska analysera om det befintliga sekretesskyddet för uppgifter om enskilds affärs- och driftförhållanden är tillräckligt.

Enligt 30 kap. 23 § OSL gäller sekretess i en statlig myndighets verksamhet som består i utredning, planering, prisreglering, tillståndsgivning, tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt, för uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgiften röjs (första punkten), och för uppgift om andra ekonomiska eller personliga förhållanden än som avses i första punkten för den som har trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet (andra punkten). Bestämmelsen ger inte i sig själv upphov till någon sekretess utan förut-

[4] Prop. 1979/80:2 del A s. 144 f.
[5] Prop. 1993/94:188 sida 89.

sätter att regeringen föreskriver om sekretess. Regeringen har med stöd av första stycket meddelat föreskrifter om sekretess i 9 § offentlighets- och sekretessförordningen (2009:641) (OSF) i den utsträckning som anges i bilagan till OSF. I p. 13 i bilagan anges bl.a. utredning, planering, tillsyn och stödverksamhet hos MSB, i p. 17 tillståndsgivning och tillsyn hos Transportstyrelsen, i p. 26 tillsyn enligt lagen (2012:806) om beredskapsplanering av olja eller enligt motsvarande äldre föreskrifter, p. 28 tillsyn enligt livsmedelslagen (2006:804) och livsmedelsförordningen (2006:813), p. 33 tillsyn enligt lagen (1993:584) om medicintekniska produkter, p. 58 tillsyn enligt patientsäkerhetslagen (2010:659) och p. 99 tillsyn hos Post- och telestyrelsen.

Begreppet affärs- eller driftförhållande har beskrivits ovan. Ordet tillsyn ska inte ges en alltför snäv tolkning utan får anses omfatta alla de fall där en myndighet har en övervakande eller styrande funktion i förhållande till näringslivet. Under begreppet tillsyn faller också sådan rådgivning som sker som ett led i en myndighets tillsynsverksamhet.[6] Den typ av uppgifter som det i första hand handlar om att sekretessbelägga är enskildas affärs- och driftförhållanden, dvs. uppgifter som typiskt sett kan vara av intresse för konkurrenter och som skulle skada verksamheten om de blev kända.

För sekretess i första punkten gäller rakt skaderekvisit och för andra punkten gäller absolut sekretess.

Sekretessen gäller oberoende av hos vilken myndighet uppgifterna finns.

Försvars- och utrikessekretess

I 15 kap. 1–2 §§ OSL regleras utrikes- och försvarssekretessen samt sekretess i det internationella arbetet. Där finns regler om sekretess till skydd för Sveriges säkerhet och Sveriges förhållande till andra stater eller mellanfolkliga organisationer.

Utrikessekretess gäller uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller stats-

[6] Prop. 1979/80:2 del A s. 235–236.

lös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs (15 kap. 1 § OSL).

Sekretess gäller för uppgift som en myndighet har fått från ett utländskt organ på grund av en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal med en annan stat eller med en mellanfolklig organisation, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs (15 kap 1 a § OSL). I denna bestämmelse regleras sekretess för uppgifter som har lämnats till eller inhämtats av en myndighet på grund av en bindande EU-rättsakt. Med bindande EU-rättsakt avses förordning, direktiv eller beslut.[7]

Försvarssekretess gäller uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs. Förekommer sådana uppgifter, t.ex. uppgifter om funktionssätt och säkerhet i system som har betydelse för samhällets försörjning eller infrastruktur, omfattas de av bestämmelsen. Bestämmelsen gäller oberoende av hos vilken myndighet uppgifterna finns (15 kap. 2 § OSL).

Behov av starkare sekretess i 18 kap. 8 § 3 OSL?

Bestämmelsen i 18 kap. 8 § 3 OSL är utrustad med ett s.k. rakt skaderekvisit. Vid införandet förordade dock flera remissinstanser i stället ett omvänt skaderekvisit.[8] I samband med att betänkandet *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten* (SOU 2015:23) remitterades pekade flera remissinstanser på att sekretesskyddet för aktuella uppgifter behöver ses över. MSB framförde i det sammanhanget att det kan finnas anledning att överväga möjligheten att föreskriva om absolut sekretess för it-incidentrapporter.

Utredningen ska enligt kommittédirektiven analysera om det nuvarande sekretesskyddet i 18 kap. 8 § 3 OSL är tillräckligt för att skydda de uppgifter som ska rapporteras till MSB och övriga tillsyns-

[7] Prop. 2012/13:192 s. 43.
[8] Prop. 2003/04:93 s. 78 f.

myndigheter eller om det finns behov av ett starkare sekretesskydd. Det som kan komma ifråga är att införa ett omvänt skaderekvisit eller absolut sekretess.

När bestämmelsen infördes gjorde regeringen bedömningen att ett rakt skaderekvisit innebär att skyddsvärda uppgifter får ett tillfredställande skydd samtidigt som insynen i myndigheternas verksamhet inte inskränks mer än nödvändigt.[9]

Kammarrätten i Göteborg har prövat om uppgifter om it-incidenter i incidentrapporter omfattas av sekretess enligt 18 kap. 8 § 3 OSL.[10] I samtliga avgöranden beslutade kammarrätten att inte lämna ut uppgifterna eftersom de bedömdes vara sådana att de lämnade eller kunde bidra till upplysning om säkerhets- eller bevakningsåtgärd och att det kunde antas att syfte med åtgärden motverkades om uppgifterna röjdes.

I skälen till NIS-direktivet (skäl 40–41) konstateras att information om incidenter blir allt mer värdefull för allmänheten och företag, särskilt små och medelstora företag. I vissa fall tillhandahålls sådan information redan via webbplatser på nationell nivå, på ett specifikt lands språk, och är främst inriktad på incidenter och händelser med en nationell dimension. Eftersom företag i allt större utsträckning bedriver gränsöverskridande verksamhet och medborgare använder onlinetjänster, bör information om incidenter tillhandahållas i samlad form på unionsnivå. CSIRT-nätverkets sekretariat uppmuntras i direktivet att upprätta en webbplats eller upplåta utrymme åt en särskild sida på en befintlig webbplats, där allmän information om allvarliga incidenter i unionen görs tillgänglig för allmänheten. Informationen ska vara särskilt inriktad på företags intressen och behov. CSIRT-enheter som deltar i CSIRT-nätverket uppmanas att på frivillig grund tillhandahålla den information som ska offentliggöras på denna webbplats, utan att därvid inkludera konfidentiell eller känslig information. I fall då information anses vara konfidentiell enligt unionsbestämmelser och nationella bestämmelser om affärshemligheter, bör konfidentiell behandling säkerställas vid genomförande av verksamhet och uppfyllande av mål enligt direktivet. Vid genomförandet av rapporteringsskyldigheterna bör CSIRT-enheterna särskilt ta hänsyn till behovet av att hålla uppgifter om produkters

[9] Prop. 2003/04:93 s. 82.
[10] Kammarrätten i Göteborg, mål nr 2972-16; 5858-16 och 5032-16.

sårbara aspekter strikt konfidentiella till dess att lämpliga säkerhetslösningar släpps. (skäl 59)

För att det ska vara möjligt att vägra lämna ut en uppgift i en allmän handling måste det enligt svensk rätt finnas en sekretessbestämmelse som omfattar den aktuella uppgiften. Gör det inte det är uppgiften offentlig och ska lämnas ut. Finns det en sekretessbestämmelse som uppgiften omfattas av ska myndigheten göra en skadeprövning. Det innebär att det ska ske en prövning av om uppgiften kan lämnas ut i just den aktuella situationen. Vid *raka skaderekvisit* är utgångspunkten att uppgiften är offentlig och att sekretess bara gäller om det kan antas att en viss skada uppkommer om uppgiften röjs. Det *omvända skaderekvisitet* har den omvända utgångspunkten, dvs. det uppställer sekretess som huvudregel. Vid ett omvänt skaderekvisit gäller således sekretess om det inte står klart att uppgiften kan röjas utan att viss skada uppstår. Omfattas uppgiften av *absolut sekretess* saknas skaderekvisit och uppgiften får då inte lämnas ut oavsett skada. Någon skadeprövning behöver alltså inte göras i dessa fall. Det är alltid förbjudet att sprida uppgifter som omfattas av absolut sekretess. Det spelar ingen roll om en uppgift i och för sig bedöms som harmlös.

MSB:s erfarenhet från tillämpningen av 20 § KBF om krav på incidentrapportering för statliga myndigheter är att redan det faktum att en sekretessprövning ska ske utgör ett sådant osäkerhetsmoment för många aktörer att aktörerna underlåter att rapportera in incidenter eller rapporterar endast övergripande eller bristfällig information. Vissa myndigheter har uppgett till MSB att sekretessfrågan utgör ett problem för rapportering. Enligt MSB finns denna problematik i en ännu större utsträckning när det gäller privata aktörer. Dessa aktörer vill ha en garanti på förhand om att känsliga uppgifter inte kommer att lämnas ut. Avsaknaden av en sådan garanti utgör enligt MSB ett starkt hinder mot att rapportera incidenter. MSB bedömer att det inte är möjligt att lämna en sådan garanti utan regler om absolut sekretess.

I utredningens arbete har framkommit att det i ett tidigt skede inte alltid står klart att uppgifterna är säkerhetskänsliga. Röjs säkerhetskänsliga uppgifter kan det svårligen repareras i efterhand.

Det som nu sagts skulle kunna utgöra skäl för att införa absolut sekretess för aktuella uppgifter i incidentrapporteringen.

Slutsatser

Utredningens bedömning är att befintliga bestämmelser om sekretess i OSL omfattar uppgifter som ska rapporteras och delas med anledning av incidenter samt tillhandahållas i samband med tillsyn.

När det gäller skyddet för enskilds affärs- eller driftförhållande ger däremot bestämmelsen i 30 kap. 23 § OSL i sig själv inte upphov till någon sekretess utan förutsätter att regeringen föreskriver om sekretess. Det ska därför införas en ny punkt i bilagan till OSF: tillsyn enligt lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster.

När det gäller frågan om det finns skäl att införa starkare sekretess för uppgifter som omfattas av bestämmelserna i 18 kap. 8 § 3 OSL konstaterar utredningen det inte framförts något exempel på brister i tillämpningen som skulle kunna motivera en starkare sekretess. Tvärtom har de avgöranden som rör incidentrapportering visat att bestämmelsen tillämpats på det sätt som avsetts.

Det har framförts att det finns anledning att anta att vissa statliga myndigheter underlåter att följa bestämmelserna om it-incidentrapportering på grund av osäkerhet kring sekretessbestämmelsernas räckvidd. Det har också framförts att privata aktörer vill ha en garanti för att känsliga uppgifter inte kommer att lämnas ut av CSIRT-enheten.

Utredningen konstaterar att det alltid måste göras en bedömning av om det finns någon sekretessbestämmelse som den aktuella uppgiften omfattas av. Det är därför omöjligt för CSIRT-enheten att lämna en garanti om att en uppgift inte ska lämnas ut. Det gäller oavsett om det införs absolut sekretess eller om nuvarande bestämmelse lämnas oförändrad. Det har inte framkommit något exempel på uppgifter om incidenter som skulle innebära skada om de röjs men som i dag inte omfattas av någon sekretessbestämmelse.

Utredningen anser därför att bestämmelserna i 18 kap. 8 § 3 OSL innebär ett tillräckligt skydd för uppgifter som kan komma att rapporteras vid en incident. Det saknas därför skäl att införa en bestämmelse om omvänt skaderekvisit eller absolut sekretess.

Under utredningens arbete har det dock framkommit att det finns brister i kunskapen om offentlighets- och sekretesslagstiftningen. Utredningen anser att detta bör kunna avhjälpas genom tydlig

information till leverantörer som kommer att omfattas av det nya regelverket.

I vissa fall kan uppgifter som omfattas av 18 kap. 8 § 3 OSL även omfattas av försvarssekretess enligt 15 kap. 2 § OSL. Den föreslagna lagen ska inte tillämpas på verksamhet som är av betydelse för Sveriges säkerhet. Det innebär att incidenter som rör Sveriges säkerhet inte ska rapporteras enligt den föreslagna lagen, utan enligt 10 a § säkerhetskyddsförordningen (1996:633), se avsnitt 5.4. Se även avsnitt 11.2.3. angående aggregerade uppgifter.

12.3 Behövs en uppgiftsskyldighet för att information ska kunna delas mellan de svenska aktörerna?

Bedömning: Genom att det i lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster införs krav på leverantörerna att dels incidentrapportera, dels tillhandahålla uppgifter vid tillsyn, införs också en sekretessbrytande uppgiftsskyldighet.

Leverantörer av samhällsviktiga tjänster och digitala tjänster är enligt NIS-direktivet skyldiga att rapportera it-incidenter. Dessa ska rapporteras till MSB som föreslås bli CSIRT-enhet. Leverantörerna kan även behöva lämna annan känslig information om bl.a. säkerhets- och bevakningsåtgärder till tillsynsmyndigheten. I båda fallen kan det förekomma uppgifter om affärs- eller driftförhållanden.

Utredningen ska enligt kommittédirektiven analysera om det finns behov av bestämmelser om sekretessbrytande uppgiftsskyldighet för att berörda leverantörer ska kunna uppfylla sin rapporteringsskyldighet.

Allmänt

En grundläggande princip är att myndigheter är skyldiga att samarbeta och bistå varandra i den utsträckning som kan ske. Principen kommer till uttryck i bl.a. 6 § förvaltningslagen (1986:223). En precisering av bestämmelsen finns i 6 kap. 5 § OSL, som innebär att en myndighet på begäran ska lämna uppgift som den förfogar över om

inte uppgiften är sekretessbelagd, eller det skulle hindra arbetets behöriga gång. Är någon sekretessbrytande bestämmelse tillämplig, även generalklausulen 10 kap. 27 § OSL, ska uppgiften lämnas ut enligt denna bestämmelse. En myndighets beslut att inte lämna ut en uppgift kan överklagas.

I många fall måste myndigheter kunna utbyta information för att kunna utföra sina uppgifter. För att tillgodose myndigheters behov av information och informationsutbyte i sin verksamhet finns flera undantag från huvudregeln om sekretess mellan myndigheter. Sådana sekretessbrytande bestämmelser och bestämmelser om undantag från sekretess finns i 10 kap. OSL. Sekretessbrytande bestämmelser finns även i andra författningar som OSL hänvisar till, eller som en uppgiftsskyldighet varvid 10 kap. 28 § OSL blir tillämplig. Nedan följer en redogörelse för de sekretessbrytande bestämmelser i OSL som är av intresse när det gäller förutsättningar att lämna ut uppgifter om rapporterade it-incidenter, om säkerhets- och bevakningsåtgärder och om affärs- och driftförhållanden.

Nödvändigt utlämnande

Sekretess enligt 10 kap. 2 § OSL hindrar inte att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen kan vara tillämplig i fall där någon av de övriga sekretessbrytandereglerna inte gäller, men ska tillämpas restriktivt. En uppgift får lämnas ut med stöd av bestämmelsen bara när utlämnandet av uppgiften är en nödvändig förutsättning för att myndigheten ska kunna fullgöra ett visst åliggande. Bara bedömningen att effektiviteten i myndighetens handlande sätts ned genom en föreskriven sekretess får inte leda till att sekretessen åsidosätts.

Tillsyn eller revision

Sekretess hindrar inte att en uppgift lämnas till en myndighet, om uppgiften behövs där för tillsyn över eller revision hos den myndighet där uppgiften förekommer (10 kap. 17 §). Får en myndighet i verksamhet som avser tillsyn eller revision en sekretessreglerad uppgift överförs sekretessen till den mottagande myndigheten om upp-

giften inte ingår ett beslut hos den mottagande myndigheten (11 kap. 1 § OSL).

Generalklausulen

Enligt den s.k. generalklausulen (10 kap. 27 § OSL) får en sekretessbelagd uppgift lämnas till en annan myndighet om det är uppenbart att intresset av att lämna uppgiften har företräde framför det intresse som sekretessen har att skydda. Generalklausulen tillkom mot bakgrund av att sekretess inte bör hindra myndigheter från att utväxla uppgifter i situationer där intresset av att uppgifterna lämnas ut bör ha företräde framför intresset av att uppgifterna inte lämnas ut.

Generalklausulen kan inte tillämpas om utlämnandet strider mot lag eller förordning eller föreskrift som har meddelats med stöd av personsuppgiftslagen. Har det t.ex. i en lag föreskrivits att en viss myndighet för sin verksamhet på vissa villkor kan få ta del av även hemliga uppgifter hos en annan myndighet, kommer det givetvis inte på fråga att, när de angivna villkoren inte är uppfyllda, lämna ut uppgifterna med stöd av generalklausulen i stället. Om det i en lag eller förordning uttömmande anges i vilka fall uppgifter får lämnas mellan myndigheter kan generalklausulen inte heller tillämpas i andra fall.

Bestämmelsen är subsidiär i förhållande till andra sekretessbrytande bestämmelser och ska alltså inte tillämpas om någon annan sekretessbrytande bestämmelse kan tillämpas.

Möjligheten att utväxla sekretessbelagda uppgifter får utnyttjas mera sparsamt och med större försiktighet om informationen inte är sekretessbelagd hos den mottagande myndigheten. Detta gäller särskilt i fråga om uppgifter som är sekretessbelagda av hänsyn till enskildas intressen. Om den uppgift som överlämnandet gäller inte blir sekretessbelagd hos den mottagande myndigheten kan risken för att skada ska uppkomma vara så stor att uppgiften inte bör lämnas ut. Att sekretessen hos den mottagande myndigheten är något svagare än hos den utlämnande myndigheten har inte ansetts spela så stor roll i praktiken.

Vid prövningen av en utlämnandefråga enligt generalklausulen ska en avvägning göras mellan den mottagnade myndighetens behov av uppgifterna och det intresse som sekretesskyddet typiskt sett till-

godoser. Ytterligare omständigheter som är av betydelse är uppgifternas art och i vilket syfte de ska användas.

Generalklausulen hindrar inte att utbyte av uppgifter mellan myndigheter sker rutinmässigt även utan särskild författningsreglering, även om det i förarbetena uttalas att rutinmässigt uppgiftsutbyte i regel ska vara författningsreglerat. I de fall där ett rutinmässigt uppgiftslämnande inte är författningsreglerat men ändå kan anses tillräckligt motiverat måste den intresseavvägning som ska göras ske på förhand. Den behöver då inte avse prövning av individuella fall. Bedömningen kan i så fall göras på ett sätt som liknar den som ska ske i fråga om massuttag. I situationen med massuttag kan emellertid den berörde tjänstemannen av naturliga skäl inte bilda sig en uppfattning om den särskilda skaderisk som kan vara förbunden med en enskild uppgift. Å andra sidan har tjänstemannen alltid kännedom om beställarens identitet och oftast också om beställarens avsikt med uppgifterna. Dessa kunskaper i förening med en bedömning av den skaderisk som typiskt sett är förbunden med uppgifter av det slag som avses med beställningen bör enligt förarbetsuttalanden i de allra flesta fall ge fullt tillräckligt underlag för bedömningen av om sekretessregleringen ska anses hindra ett utlämnande eller inte.

Sekretess vid uppgiftsskyldighet

Sekretess hindrar inte att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Sekretessbrytande bestämmelser finns också i anslutning till berörda sekretessbestämmelser. (10 kap. 28 § OSL)

Genom 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (KBF) har en sådan uppgiftsskyldighet som avses i 10 kap. 28 § OSL införts. Myndigheterna kan alltså med stöd av förordningen överlämna de uppgifter som avses till MSB, även om uppgifterna omfattas av sekretess hos myndigheterna.

Slutsatser

Utredningen konstaterar att det finns flera sekretessbrytande bestämmelser som kan tillämpas för att uppgifter som omfattas av sekretess ska kunna delas mellan myndigheter i samband med tillsyn och incidentrapportering. Mot bakgrund av att direktivet omfattar sju olika sektorer är det svårt att överblicka vilken typ av uppgifter som kommer att omfattas av kravet att incidentrapportera. Eftersom enskilda inte omfattas av OSL:s bestämmelser om utlämnande måste det i den nya lagen finnas bestämmelser om krav på incidentrapportering och att tillhandahålla uppgifter vid tillsyn. Genom införandet av sådana bestämmelser införs också en sekretessbrytande uppgiftsskyldighet för de aktörer som omfattas av OSL.

12.4 Behövs nya bestämmelser för att uppgifter ska kunna lämnas till andra medlemsstater eller kommissionen?

Bedömning. De befintliga bestämmelserna i OSL tillgodoser NIS-direktivets krav på utlämnande av uppgifter till andra medlemsstater och till kommissionen.

NIS-direktivets bestämmelser om samarbete mellan medlemsstaterna kan innebära att information som helt eller delvis omfattas av sekretess behöver utlämnas till annan medlemsstat eller till kommissionen. En förutsättning för ett sådant utlämnande är enligt 8 kap. 3 § OSL att utlämnandet sker i enlighet med särskilda föreskrifter i lag eller förordning, eller att uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

Slutsatser

I den föreslagna förordningen anges att den gemensamma nationella kontaktpunkten (MSB) ska lämna uppgifter om incidenter till samarbetsgruppen och att CSIRT-enheten vid MSB ska informera andra medlemsstater om vissa incidenter. I CSIRT-nätverket ska sekretessbelagda uppgifter inte utbytas (artikel 12.3).

Utredningen bedömer att ett sådant utbyte av sekretessbelagda uppgifter som följer av NIS-direktivet kan göras med stöd av 8 kap. 3 § 1 och 2. Något behov av ytterligare reglering finns inte.

I de fall en leverantör felaktigt rapporterar incidenter som rör Sveriges säkerhet i enlighet med bestämmelserna i den föreslagna lagen ankommer det på CSIRT-enheten att uppmärksamma detta. Eftersom sådana incidenter inte omfattas av rapporteringsplikten i den föreslagna lagen ska de inte heller rapporteras till andra medlemsstater eller till kommissionen. Detsamma gäller uppgifter i incidentrapporter som var för sig inte rör Sveriges säkerhet, men som tillsammans utgör en ny uppgift som rör Sveriges säkerhet (aggregerad information).

12.5 Hantering av information som mottagits från andra medlemsstater

Bedömning: De befintliga bestämmelserna om sekretess i OSL tillgodoser NIS-direktivets krav på konfidentialitet beträffande information som svenska myndigheter tar emot från andra medlemsstater i den Europeiska unionen till följd av NIS-direktivets bestämmelser.

När det gäller incidentrapporter från leverantörer av samhällsviktiga tjänster ska den behöriga myndigheten eller CSIRT-myndigheten, mot bakgrund av informationen i rapporten, informera den eller de andra berörda medlemsstaterna, om incidenten har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i den medlemsstaten. Därvid ska den behöriga myndigheten eller CSIRT-enheten, i enlighet med unionsrätten eller med nationell lagstiftning som är förenlig med unionsrätten, bevara nämnda leverantörs säkerhets-

intressen och kommersiella intressen samt konfidentialiteten hos informationen i leverantörens rapport (artikel 14.5).

Beträffande incidentrapporter från leverantörer av digitala tjänster ska den behöriga myndigheten eller CSIRT-enheten, om så är lämpligt, och särskilt om incidenten berör två eller flera medlemsstater, informera andra medlemsstater som påverkats. Därvid ska de behöriga myndigheterna, CSIRT-enheter och gemensamma kontaktpunkter, i enlighet med unionsrätten eller nationell lagstiftning som är förenlig med unionsrätten, bevara leverantören av digitala tjänsters säkerhetsintressen och kommersiella intressen samt den tillhandahållna informationens konfidentialitet (artikel 16.6).

Sekretess gäller enligt 15 kap. 1 a § OSL för uppgift som en myndighet har fått från ett utländskt organ på grund av en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal med en annan stat eller med en mellanfolklig organisation, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs. I bestämmelsen regleras sekretess för uppgifter som har lämnats till eller inhämtats av en myndighet på grund av en bindande EU-rättsakt. Med bindande EU-rättsakt avses förordning, direktiv eller beslut.[11]

Slutsatser

Utredningens bedömning är att information som tas emot till följd av bestämmelserna i NIS-direktivet omfattas av 15 kap. 1 a § OSL. Befintliga regler säkerställer därmed leverantörens säkerhetsintressen och kommersiella intressen samt konfidentialiteten hos informationen i leverantörens incidentrapport.

[11] Prop. 2012/13:192 s. 43.

13 Konsekvensanalys

13.1 Konsekvensutredningens innehåll

I utredningens uppdrag ingår att beskriva konsekvenserna av lämnade förslag i enlighet med 14–15 a §§ i kommittéförordningen (1998:1474). När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller landsting, ska kommittén föreslå en finansiering.

Eftersom utredningen lämnar författningsförslag ska konsekvensutredningen också göras i enlighet med 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Utredningen bedömer att följande områden inte berörs av förslagen.

- sysselsättning och offentlig service i olika delar av landet
- jämställdheten mellan kvinnor och män
- möjligheterna att nå de integrationspolitiska målen

I regeringens budgetproposition 2016/17:1, utgiftsområde 6 s. 73 och 80 f. framförs följande när det gäller NIS-direktivet. Det krävs ett fortsatt arbete för att stärka informationssäkerheten i samhället där MSB har en viktig samordnande roll. För att hålla jämna steg med den digitala utvecklingen och skydda samhällsviktig verksamhet behöver alla aktörer i samhället fortlöpande stärka förmågan att förebygga och hantera it-incidenter. För aktörer som bedriver samhällsviktig verksamhet kommer genomförandet av NIS-direktivet att innebära höjda krav på en god informationssäkerhet, vilket i sin tur gynnar hela samhället. Det förändrade omvärldsläget gör att samhällets behov av informations- och cybersäkerhet har ökat påtagligt. Digitaliseringen i samhället har bland annat inneburit nya former av kommunikation, datahantering och datalagring, vilket medfört nya risker och

sårbarheter. För att den digitala utvecklingen ska kunna fortsätta på ett säkert sätt behöver alla aktörer, såväl privata som offentliga, mer aktivt arbeta med informations- och cybersäkerhet. Regeringen avser därför att utarbeta en nationell strategi som omhändertar olika perspektiv för att kunna identifiera och möta utmaningar mot samhällets informations- och cybersäkerhet. Det är också av central betydelse att genomföra EU-direktivet om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem (NIS-direktivet). Direktivet innebär bl.a. högre krav på enskilda aktörer som bedriver samhällsviktig verksamhet och som är beroende av informationssystem.

NIS-direktivets genomförande nämns även under utgiftsområde 22 s. 106.

13.1.1 Regleringsalternativ

Utredningens huvudsakliga uppdrag har varit att genomföra NIS-direktivet genom att bland annat fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen i syfte att förbättra den inre marknadens funktion. Direktivet är bindande för medlemsstaterna med avseende på det resultat som ska uppnås och måste genomföras i nationell rätt oavsett kostnaderna.

Medlemsstaterna har mycket olika beredskapsnivåer när det gäller säkerhet i nätverk och informationssystem vilket lett till skilda tillvägagångssätt i unionen. Resultatet blir olika skyddsnivåer för konsumenter och företag vilket undergräver den allmänna nivån på säkerhet i nätverk och informationssystem i unionen. Avsaknaden av gemensamma krav gör det i sin tur omöjligt att inrätta en övergripande och effektiv mekanism för samarbete på unionsnivå. Effektiva åtgärder för att lösa problemen förutsätter ett övergripande angreppssätt på unionsnivå som omfattar en gemensam miniminivå för kapacitetsuppbyggnad och planering, utbyte av information, samarbete och gemensamma säkerhetskrav.

I vissa delar medger direktivet valmöjlighet vid genomförandet. När det gäller leverantörer av samhällsviktiga tjänster kan medlemsstaterna anta eller behålla bestämmelser som syftar till att uppnå en högre nivå på säkerheten i nätverk och informationssystem. Medlemsstaterna kan också utse en eller flera myndigheter för att över-

vaka tillämpningen av NIS-direktivet på nationell nivå. NIS-direktivet ger också medlemsstaterna möjlighet att införa frivillig incidentrapportering.

Förslagen överensstämmer med EU-rätten m.m.

Den föreslagna regleringen är i princip uteslutande en konsekvens av Sveriges medlemskap i den Europeiska unionen. Regleringen överensstämmer med Sveriges skyldigheter som följer av anslutningen till den Europeiska unionen och går inte utöver dessa skyldigheter. Förslagen innehåller inga krav som syftar till att uppnå en högre nivå av säkerhet i nätverk och informationssystem än de som anges i NIS-direktivet. Utredningen har dock, enligt uppdraget i kommittédirektiven, föreslagit att det ska inrättas en samordnande funktion mellan tillsynsmyndigheterna. Även den föreslagna tidpunkten för ikraftträdande följer direkt av NIS-direktivets bestämmelser. Effekten av om någon reglering inte kommer till stånd blir således att Sverige inte följer skyldigheterna enligt EU-rätten.

13.1.2 Vem berörs av förslagen

Lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster med tillhörande förordning kommer att omfatta leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster oavsett i vilken form verksamheten bedrivs. I dag tillhandahålls dessa tjänster av statliga myndigheter, kommuner, landsting eller företag.

Användare av samhällsviktiga tjänster och digitala tjänster finns i hela samhället men konsekvenserna av ett bortfall i tjänsten beror på vem som är användare.

Ett antal myndigheter föreslås också få särskilda uppdrag till följd av NIS-direktivet. Enligt direktivet ska det utses behöriga myndigheter (tillsynsmyndigheter), nationell kontaktpunkt och CSIRT-enhet. Sverige ska också utse representanter i den samarbetsgrupp som inrättats enligt NIS-direktivet samt deltagare i CSIRT-nätverket. Kommittédirektiven anger också att det ska finnas en samordnande funktion mellan tillsynsmyndigheterna.

13.2 Ekonomiska konsekvenser

Medlemsstaterna ska enligt NIS-direktivet säkerställa att de behöriga myndigheterna och de nationella kontaktpunkterna har tillräckliga resurser för att på ett effektivt sätt kunna utföra de uppgifter de tilldelas och därigenom uppnå målen med direktivet (artikel 8.5).

I NIS-direktivet finns inga bestämmelser om hur åtgärderna ska finansieras.

Enligt kommittédirektiven ska utredningen bedöma de ekonomiska konsekvenserna av förslagen för enskilda och det allmänna. Leder förslagen till kostnadsökningar för det allmänna ska utredningen föreslå hur dessa ska finansieras.

13.2.1 Konsekvenser för Myndigheten för samhällsskydd och beredskap, behöriga myndigheter och domstolar

Ekonomiska konsekvenser för Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap (MSB) föreslås vara nationell kontaktpunkt, CSIRT-enhet och ingå i CSIRT-nätverket. MSB föreslås också vara Sveriges representant i samarbetsgruppen.

Medlemsstaterna ska säkerställa att CSIRT-enheten har de resurser som behövs för att effektivt utföra sina uppgifter enligt bilaga 1 p. 2 till NIS-direktivet (artikel 9.2). CSIRT-enheten ska ha tillgång till lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur på nationell nivå (artikel 9.3). Den nationella kontaktpunkten bör enligt NIS-direktivet förses med de tekniska och finansiella resurser och personalresurser som den behöver för att på ett effektivt sätt kunna utföra de uppgifter som den tilldelas och därmed uppnå målen med direktivet. Eftersom syftet med direktivet är att förbättra den inre marknadens funktion genom att skapa tillit och förtroende, måste medlemsstaternas organ kunna samarbeta effektivt med ekonomiska aktörer och ha en struktur som är förenlig med detta (skäl 31).

MSB har redan i dag uppdraget att ta emot och hantera statliga myndigheters incidentrapportering. I det uppdraget har också ingått att ta fram en säker kommunikations- och informationsstruktur samt tillhandhålla tjänster som att analysera inrapporterade incidenter och

vid behov varna andra aktörer. Genom utredningens förslag kommer antalet incidenter som rapporteras att öka liksom kraven på MSB. Hur stor den ökningen kommer att bli är i dag svårt att bedöma liksom i vilken utsträckning en ökning medför behov av utökade resurser. Utredningens bedömning är att även om antalet rapporter ökar bör ökningen kunna finansieras inom befintliga budgetmedel.

MSB ska enligt utredningens förslag representera Sverige i samarbetsgruppen och leda ett samarbetsforum för tillsynsmyndigheter samt lämna olika former av stöd till tillsynsmyndigheterna. MSB ska vidare utfärda föreskrifter som behövs för arbetet med ett systematiskt och riskbaserat informationssäkerhetsarbete samt om tillämpningen av standarder och specifikationer vid utformningen av säkerhetsåtgärder. Dessa uppgifter ligger väl i linje med MSB:s nuvarande uppdrag. Detsamma gäller uppdraget att få en samlad bild genom att ta emot samlade bedömningar av tillsynsresultat m.m. från tillsynsmyndigheterna. Utredningens bedömning är att stöd i form av metodutveckling avseende tillsyn, utbildning och informationsinsatser till tillsynsmyndigheterna bör finansieras av medel från anslaget 2:4 Krisberedskap för utgiftsområde 6.[1] Sådant stöd ryms under åtgärder för funktionalitet och kontinuitet i samhällsviktig verksamhet och samhällsviktig informationsinfrastruktur.[2] När det gäller övriga uppdrag anser utredningen att dessa i den utsträckning det inte anses ingå i Myndigheten för samhällsskydd och beredskaps nuvarande uppdrag, se avsnitt 11.1.5, ska finansieras inom utgiftsområdet.

Ekonomiska konsekvenser för behöriga myndigheter (tillsynsmyndigheterna)

Tillsynsmyndigheterna ska enligt NIS-direktivet ha tillräckliga resurser för att på ett effektivt sätt kunna utföra tillsyn och uppnå målen med direktivet (artikel 8.5).

Medlemsstaterna ska säkerställa att tillsynsmyndigheterna har de befogenheter och medel de behöver för att bedöma huruvida leve-

[1] Under vissa förutsättningar och under en begränsad period kan särskilda medel beviljas för att förstärka effekten av samhällets samlade krisberedskap eller den samlade förmågan att hantera kriser. Riksdagen anslår därför årligen i bugetpropositionen för utgiftsområde 6 cirka en miljard kronor till sådana insatser genom anslag 2:4 Krisberedskap.
[2] Inriktning för att söka medel från anslag 2:4 Krisberedskap 2017, MSB dnr 2015:5690.

rantörer av samhällsviktiga tjänster uppfyller sina skyldigheter och effekterna därav på säkerheten i nätverk och informationssystem (artikel 14).

Medlemsstaterna ska också säkerställa att tillsynsmyndigheterna har de befogenheter och medel som krävs för att ålägga leverantörer av samhällsviktiga tjänster att tillhandahålla den information som är nödvändig för att bedöma säkerheten i deras nätverk och informationssystem. Detta inbegriper dokumenterade säkerhetsprinciper samt att tillhandhålla bevis för ett effektivt genomförande av säkerhetsprinciper, såsom resultaten av en säkerhetsrevision utförd av den behöriga myndigheten eller en auktoriserad revisor. I det senare fallet innebär detta också att ge den behöriga myndigheten tillgång till resultaten, inklusive de underliggande bevisen (artikel 15.1–2).

Medlemsstaterna ska säkerställa att tillsynsmyndigheten vid behov vidtar åtgärder genom tillsynsåtgärder i efterhand, när de har mottagit bevis på att en leverantör av digitala tjänster inte uppfyller kraven i artikel 16. Tillsynsmyndigheterna ska ha de befogenheter och medel som krävs för att ålägga leverantörer av digitala tjänster att tillhandahålla den information som behövs för en bedömning av säkerheten i deras nätverk och informationssystem, inbegripet dokumenterade säkerhetsprinciper, och för att åtgärda varje underlåtenhet att uppfylla kraven i artikel 16 (artikel 17.2).

Detta innebär enligt utredningens mening att tillsynsmyndigheterna bör förses med de tekniska och finansiella resurser och personalresurser som de behöver för att på ett effektivt sätt kunna utföra de uppgifter som de tilldelas och därmed uppnå målen med direktivet. Eftersom syftet med direktivet är att förbättra den inre marknadens funktion genom att skapa tillit och förtroende, måste medlemsstaternas organ kunna samarbeta effektivt med ekonomiska aktörer och ha en struktur som är förenlig med detta (skäl 31).

De föreslagna tillsynsmyndigheterna utövar redan i dag tillsyn av något slag men för några tillsynsmyndigheter innebär utredningens förslag ett nytt tillsynsområde, säkerhet i nätverk och informationssystem.

Transportstyrelsen och Post- och telestyrelsen utfärdar föreskrifter och är tillsynsmyndigheter enligt säkerhetsskyddslagen, där en viktig del är informationssäkerhet. Post- och telestyrelsen utfärdar föreskrifter och utövar tillsyn även enligt annan lagstiftning på området elektronisk kommunikation. Finansinspektionen utövar

redan i dag tillsyn och utfärdar föreskrifter inom de områden som den föreslagna lagen omfattar. Inom de flesta sektorerna måste dock nya föreskrifter utfärdas och ett nytt system för tillsyn byggas upp alternativt arbetas in i befintligt. Vidare behöver ny kompetens utvecklas eller nyrekryteras. Dessutom bör leverantörer inom de olika sektorerna informeras om den nya lagstiftningen. Inom några sektorer behöver tillsynsmyndigheten identifiera i vilken utsträckning lex specialis-bestämmelser ska tillämpas. Samtliga tillsynsmyndigheter har god kunskap om verksamheten i sin respektive sektor.

Kostnader tillsyn

Utredningens bedömning är att förslagen kommer att innebära ökade kostnader för tillsynsmyndigheterna. Hur stora kostnaderna blir är till viss del beroende av om den aktuella tillsynsmyndigheten redan i dag utövar en likartad tillsyn över leverantörerna. En annan viktig faktor är hur många leverantörer som kommer att bli föremål för tillsyn.

Utredningens bedömning är att oavsett antalet slutligt identifierade leverantörer uppkommer kostnader för att utfärda nya föreskrifter, bygga upp ett nytt system för tillsyn alternativt komplettera ett system som redan används, rekrytera eller utveckla ny kompetens inom informationssäkerhetsområdet samt att utöva tillsyn. Vidare måste leverantörer inom de olika sektorerna informeras om det nya regelverket. Inom några sektorer behöver tillsynsmyndigheten identifiera i vilken utsträckning lex specialis-bestämmelser ska tillämpas. Kostnaderna kommer därför bli högre i en initial fas. Utredningens bedömning är att samtliga tillsynsmyndigheters resurser bör förstärkas tillfälligt med två årsarbetskrafter under 2018.

Den löpande kostnaden för tillsyn och kostnaden för att besluta om administrativa sanktioner och åtgärdsföreläggande kommer till skillnad från de initiala kostnaderna att variera beroende på antalet leverantörer som kommer att omfattas av den nya lagens krav på tillsyn samt frekvensen i tillsynen.

Utredningen anser att kostnaderna till viss del, i vart fall på lång sikt, kan finansieras genom de samhällsekonomiska vinster som en hög gemensam nivå av säkerhet i nätverk och informationssystem

medför för respektive sektor, men att det inledningsvis måste tillföras medel.

Kostnader som kan uppkomma för tillsynsmyndigheterna för nationell samverkan ska finansieras inom befintlig budget. Det får anses ingå i myndigheters uppdrag att samverka med andra myndigheter.

När det gäller tillsynsmyndigheternas kostnader för den löpande tillsynen och för att besluta om sanktioner och åtgärdsföreläggande är dessa, enligt utredningens mening, till stor del beroende av hur många leverantörer som kommer att omfattas av regelverket. Kostnaderna för ett tillsynsuppdrag som omfattar ett fåtal leverantörer blir avsevärt lägre än ett uppdrag som omfattar flera hundra leverantörer. Att i dag fastställa antalet leverantörer av samhällsviktiga tjänster är dock förenat med stora svårigheter bland annat på grund av att det saknas bedömning av om en incident skulle medföra en betydande störning i tjänstens kontinuitet och eftersom tröskelvärden för de faktorer som ska användas för att göra denna bedömning ännu inte tagits fram för samtliga sektorer. Utredningen kan därför inte bedöma de framtida löpande kostnaderna för tillsyn och beslut om administrativa sanktioner samt åtgärdsföreläggande.

Utredningen föreslår att Myndigheten för samhällsskydd och beredskap med stöd av tillsynsmyndigheterna ges i uppdrag att göra en uppskattning av hur många leverantörer av samhällsviktiga tjänster som finns inom varje sektor.

En annan faktor som inverkar på kostnaden för löpande tillsyn och beslut om administrativa sanktioner samt åtgärdsföreläggande är hur tillsynen genomförs samt vilken informationssäkerhetskompetens som finns på tillsynsmyndigheten. Det är endast sådan utveckling och förstärkning av kompetens som föranleds av den föreslagna lagens genomförande som bör kostnadsberäknas. Utredningens uppfattning är att samtliga tillsynsmyndigheter i dag granskar verksamhet som är beroende av nätverk och informationssystem och utgår därför att det redan finns viss kompetens inom informationssäkerhetsområdet. Det måste också beaktas att förstärkningen av kompetens kommer andra områden, såsom samhällets krisberedskap och planering för höjd beredskap tillgodo. När det gäller kostnader för löpande tillsyn samt för kompetensförsörjning föreslår utredningen att Statskontoret ges i uppdrag att lämna ett förslag på genomförande och finansiering.

Avgiftsfinansierad tillsyn

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 bl.a. att tillsyn i normalfallet bör finansieras genom avgifter.[3] 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. Avgifterna bör vara lättbegripliga och förutsebara för de objektsansvariga och ge incitament till avsedda beteenden hos tillsynsorganen och de objektsansvariga.

Avgiftsfinansiering av tillsyn finns inom en rad olika områden och även inom de sektorer som omfattas av den föreslagna lagen. Inom transportsektorn tas bland annat ut avgift när det gäller yrkestrafik för tillsyn av den som har trafiktillstånd enligt taxitrafiklagen (2012:2111) och yrkestrafiklagen (2012:10), för tillsyn av sjöfartsskydd i hamnanläggningar enligt lagen (2004:487) om sjöfartsskydd och tillsyn av hamnskydd i hamnar enligt lagen (2006:1209) om hamnskydd. Finansinspektionens kostnader för bland annat regelgivning och tillsyn täcks av årliga avgifter enligt förordningen (2007:1135) om årliga avgifter för finansiering av Finansinspektionens verksamhet.

I betänkandet *En översyn inom Sevesområdet – förslag till en förstärkt organisation för att förebygga och begränsa följderna av allvarliga kemikalieolyckor* (SOU 2013:14) görs i avsnitt 5 en genomgång av förutsättningarna för att avgiftsfinansiera tillsyn av Sevesoverksamheter.

När det gäller sådan verksamhet som omfattas av den föreslagna lagen är det i nuläget svårt att bedöma omfattningen av de tillsyner som ska genomföras. Sektorernas verksamhet skiljer sig åt liksom komplexiteten i de olika nätverken och informationssystemen. Den snabba tekniska utvecklingen liksom samhällets digitalisering kan få

[3] Regeringens skrivelse 2009/10:79, En tydlig, rättssäker och effektiv tillsyn, s. 19.

stora effekter på tillsynsverksamhetens omfattning och innehåll. Den verksamhet som kommer att bli föremål för tillsyn finns inom staten, kommuner, landsting och enskild verksamhet och är till viss del skattefinansierad. Förutsättningar för en avgiftsfinansierad tillsyn är enligt utredningens mening att det är känt vilka leverantörer som omfattas och att kontroller sker hos samtliga leverantörer som betalar tillsynsavgift. Av kapitel 6, 10 och 11 framgår att bedömningen av vilka leverantörer som omfattas är beroende av flera omständigheter och att vilka leverantörer som omfattas kan variera över tid. Förteckningen över samhällsviktiga tjänster ska uppdateras årligen.

Vidare kommer inte samtliga leverantörer av den aktuella tjänsten att omfattas. Detta kan medföra att en avgiftsfinansierad tillsyn kan få en negativ påverkan på konkurrensen. När det gäller till exempel digitala tjänster kan en avgiftsfinansiering också påverka var leverantören etablerar sin verksamhet om finansieringen skiljer sig åt i de olika medlemsstaterna. I sektorer som regleras eller kan komma att regleras av andra EU-rättsakter, exempelvis finans- och sjöfartssektorn, ska den föreslagna lagen endast tillämpas i den utsträckning kraven på leverantörerna enligt EU-rättsakten inte motsvarar kraven i lagen.

Utredningen bedömer att det är svårt att bestämma en avgift som ska täcka de kostnader som uppstår innan leverantörerna av de samhällsviktiga tjänsterna och digitala tjänsterna har identifierats. Det är i nuläget svårt att både bedöma antalet leverantörer som kommer omfattas och komplexiteten i den verksamhet som ska granskas. Inom några sektorer görs redan i dag tillsyn och i vissa fall är den tillsynen avgiftsfinansierad. Utredningens förslag är därför att tillsynsverksamheten, i vart fall inledningsvis, ska vara anslagsfinansierad och fördelas på de utgiftsområden som respektive sektor tillhör.

När leverantörer av samhällsviktiga tjänster och digitala tjänster har identifierats kan en ny utredning göras för att bedöma om det är möjligt att införa ett system med tillsynsavgifter som är förutsägbara, konkurrensneutrala och står i proportion till motprestationen. Det bör även vägas in i vilken utsträckning verksamheten är statligt eller kommunalt finansierad och att en avgift inte ska innebära höga administrativa kostnader för tillsynsmyndigheten eller för leverantörer som ska granskas. Vidare bör erfarenheterna från den avgiftsfinansierade livsmedelskontrollen tas tillvara. Statskontoret har i rapporten *Avgifter i livsmedelskontrollen, Förslag på en mer*

effektiv avgiftsfinansiering, 2015:17, gjort en utvärdering av avgiftsfinansieringen av den offentliga livsmedelskontrollen. I rapporten framhålls till exempel att avgiftsmodellen måste vara begriplig, tillämpas på ett enhetligt sätt och att kontroller faktiskt genomförs.

Ekonomiska konsekvenser för domstolar

Tillsynsmyndighetens beslut om förelägganden eller sanktionsavgift får överklagas till allmän förvaltningsdomstol vilket kan medföra en ökning av antalet mål där. Det bedöms dock i så fall endast bli fråga om ett fåtal ytterligare beslut som kommer under prövning i domstol, se avsnitt 9.6.3. De ekonomiska konsekvenserna för domstolarna bedöms därför kunna hanteras inom befintliga budgetramar.

13.2.2 Konsekvenser för leverantörer

Utredningen har bedömt i vilken utsträckning förslagen påverkar kostnaderna för statliga myndigheter, kommuner, landsting och företag. För leverantörerna av samhällsviktiga tjänster och digitala tjänster är utredningens bedömning att konsekvenserna av förslagen sammantaget är positiva. Det förebyggande säkerhetsarbetet innebär att skadekonsekvenserna av en incident blir begränsade för den leverantör där incidenten inträffat men även för samhället i stort.

Ekonomiska konsekvenser för leverantörer

Leverantörerna finns inom sju olika sektorer samt inom tre typer av digitala tjänster.

Den föreslagna regleringens krav på säkerhetsåtgärder och incidentrapportering medför för de flesta leverantörer ingen större förändring jämfört med vad som gäller i dag även om det inom vissa sektorer inte finns några uttryckliga krav på säkerhetsåtgärder eller incidentrapportering. Utredningen anser att det i de fall det saknas bestämmelser måste anses ingå i uppdraget att tillhandahålla en samhällsviktig tjänst att också vidta grundläggande säkerhetsåtgärder för de nätverk och informationssystem som tjänsten är beroende av. Däremot kommer kravet att rapportera incidenter till CSIRT-en-

heten vara en ny uppgift för andra leverantörer än statliga myndigheter.

För att undvika oproportionella finansiella och administrativa bördor för leverantörerna bör kraven enligt skälen i NIS-direktivet stå i proportion till den risk som det berörda nätverk och informationssystemet utgör, med beaktande av den senaste tekniska utvecklingen. När det gäller leverantörer av digitala tjänster gäller dessa krav inte för mikroföretag och små företag, se avsnitt 10.2.2.

Utredningens förslag kommer att ställa högre krav på dokumentation och administrativ hantering när det gäller identifiering av leverantörer av samhällsviktiga tjänster, bedömning av lämpliga säkerhetsåtgärder samt incidentrapportering. Förslagen om tillsyn kommer också att medföra administrativa kostnader för den leverantör som blir föremål för tillsyn.

Däremot kommer enhetliga regler, standardisering av säkerhetskrav, tillsyn och möjligheten att få upplysningar av tillsynsmyndigheterna bidra till minskade kostnader både vad gäller teknik och personella resurser. Information om incidenter kommer genom direktivets genomförande att bli mer tillgänglig både allmänt och riktat till sektorer samt enskilda leverantörer. De erfarenheter som kan dras från inträffade incidenter både nationellt och inom unionen kommer att kunna användas i det förebyggande och systematiska informationssäkerhetsarbetet. En hög nivå av säkerhet i nätverk och informationssystem kommer att väsentligt minska både kostnader för och andra konsekvenser av en eventuell incident.

Vissa leverantörer kan också ha fått ersättning för säkerhetsåtgärder som även kan främja säkerheten i samhällsviktiga tjänster enligt till exempel elberedskapslagen (1997:288) för att vidta beredskapsåtgärder och förordningen (2003:396) om elektronisk kommunikation för att beakta totalförsvarets behov. Här bör nämnas att flera myndigheter även har tilldelats medel från anslaget 2:4 Krisberedskap, utgiftsområde 6 i budgetpropositionen, för projekt som angränsar till de åtgärder som ska vidtas med stöd av den föreslagna lagen.

Utredningens bedömning är att förslagen inte kommer innebära några ekonomiska konsekvenser för leverantörer av samhällsviktiga och digitala tjänster. Kostnadsmässiga och andra konsekvenser av myndighetsföreskrifter som meddelas i anslutning till den nya lagen

ska utredas enligt förordningen (2007:1244) om konsekvensutredning vid regelgivning.

13.2.3 Konsekvenser för konsumenter och andra användare

Förslagen innebär krav på leverantörer av samhällsviktiga tjänster och digitala tjänster. Utredningen har konstaterat att det måste anses ingå i uppdraget att tillhandahålla en samhällsviktig tjänst att också vidta grundläggande säkerhetsåtgärder för de nätverk och informationssystem som tjänsten är beroende av. I de fall sådana grundläggande åtgärder inte vidtagits kan det inte uteslutas att kostnader för säkerhetsåtgärder skulle kunna komma att avspegla sig i priset på sådana tjänster som inte skattefinansieras eller skattesubventioneras, t.ex. dricksvatten- och elförsörjning. Detta ska dock vägas mot de kostnader som kan uppkomma på grund av brister i säkerheten i nätverk och informationssystem.

13.2.4 Samhällsekonomiska konsekvenser

Bakgrunden till NIS-direktivet är att nätverk och informationssystem spelar en allt viktigare roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och i synnerhet för Sveriges och den inre marknadens funktion. Säkerhetsincidenter, som blir allt mer omfattande och vanliga får allt större inverkan, utgör ett allvarligt hot mot nätverkens och informationssystemens funktion. Systemen kan också bli föremål för avsiktligt sabotage i syfte att skada dem eller förorsaka driftsavbrott. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande ekonomiska förluster, undergräva användarnas förtroende och medför allvarliga konsekvenser för Sveriges och unionens ekonomi. Incidenterna kan också medföra allvarliga konsekvenser för invånarna i Sverige.

Nätverk och informationssystem, i synnerhet internet, spelar en viktig roll genom att underlätta både den gränsöverskridande rörligheten för varor, tjänster och personer och rörligheten för varor, tjänster och personer inom landet. På grund av denna transnationella natur kan allvarliga störningar av dessa system, vare sig de är avsiktliga eller oavsiktliga och oberoende av var de förekommer påverka

enskilda medlemsstater och unionen som helhet. Säkerheten i nätverk och informationssystem är därför avgörande för att den inre marknaden och den svenska marknaden ska fungera väl.

Utredningens förslag syftar till att säkerställa kontinuiteten i samhällsviktiga tjänster och digitala tjänster vilket är till fördel för både företag, myndigheter, kommuner, landsting och konsumenterna eftersom försörjningstryggheten ökar. Tillförlitliga nätverk och informationssystem skapar därför samhällsekonomiska vinster på både kort och lång sikt.

13.3 Övriga konsekvenser

13.3.1 Förslagens konsekvenser för den kommunala självstyrelsen

Det finns ett antal värden som kan tillgodoses genom kommunal självstyrelse. Det handlar främst om demokrativärden och effektivitetsvärden. Det avser beslutsfattande nära medborgarna, flexibilitet och effektivt resursutnyttjande, lokal och regional anpassning samt medborgarnas inflytande över beslut.

Följande frågor kan användas vid analysen av konsekvenser för den kommunala självstyrelsen.

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?

Det finns även lagstiftning som över huvud taget inte påverkar den kommunala självstyrelsen på det sätt som avses här. Vissa lagbestämmelser berör kommuner och landsting i deras egenskap av arbetsgivare, måltidsproducent, fastighetsägare etc. Här omfattas kommu-

ner och landsting av samma lagstiftning som andra arbetsgivare, måltidsproducenter etc. Vidare måste kommuner och landsting kunna omfattas av säkerhetsföreskrifter m.m. av produktionsmässig karaktär. I dessa situationer blir det inte aktuellt att göra en prövning av den föreslagna lagstiftningen utifrån de värden som den kommunala självstyrelsen är satt att värna.

Utredningens bedömning är att förslagen inte påverkar den kommunala självstyrelsen på sätt som avses i 15 § kommittéförordningen (1998:1474). Förslagen avser krav på säkerhetsåtgärder och it-incidentrapportering som omfattar kommuner och landsting i deras egenskap av tillhandahållare av en samhällsviktig tjänst på samma sätt som andra leverantörer av samhällsviktiga tjänster.

13.3.2 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

Utredningens förslag om krav på säkerhetssåtgärder och incidentrapportering förebygger både avsiktliga angrepp och s.k. handhavandefel. Förslagen bör enligt utredningens mening leda till att it-relaterade brott förebyggs och förhindras.

Förslaget om att leverantörerna av samhällsviktiga och digitala tjänster ska uppmanas att anmäla incidenter som har sin grund i en brottslig gärning till polisen bör leda till att ett större antal it-brott utreds och beivras.

13.3.3 Särskild hänsyn till små företag

Enligt artikel 16.11 i direktivet ska säkerhets- och rapporteringskraven beträffande leverantörer av digitala tjänster inte tillämpas på mikroföretag eller små företag enligt definitionen i kommissionens rekommendation 2003/361/EG[4].

Mot bakgrund av att utredningen inte har identifierat vilka leverantörer som kommer omfattas av förslagen är det svårt att bedöma vilka konsekvenser de föreslagna reglerna kan komma att få för små företag. Krav på dokumentation och administration kan innebära

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

en större börda för små företag. Genom utredningens förslag att tillsynsmyndigheterna ska lämna råd och upplysning till leverantörerna inom den sektor över vilken de utövar tillsyn bedömer utredningen att de behov som små företag kan ha tillgodoses.

När det gäller konkurrensförmåga innebär NIS-direktivet att reglerna om säkerhet i nätverk och informationssystem för samhällsviktiga tjänster och digitala tjänster blir enhetliga i hela unionen. Förslaget bör därför underlätta för alla typer av företag som vill verka på den inre marknaden och därmed förbättra konkurrensen.

14 Ikraftträdande

14.1 Förslaget till ny lag om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster

Förslag: Lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster ska träda i kraft den 10 maj 2018.

Enligt artikel 25 i NIS-direktivet ska medlemsstaterna senast den 9 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att uppfylla direktivet. Vidare anges att bestämmelserna ska tillämpas från och med den 10 maj 2018. Det är alltså nödvändigt att bestämmelserna träder i kraft den 10 maj 2018 och detta datum bör därför anges i lagen.

14.2 Övrigt

Mot bakgrund av att det i flertalet sektorer krävs myndighetsföreskrifter för att den föreslagna lagen ska kunna tillämpas enligt NIS-direktivet bör regeringen ge Myndigheten för samhällsskydd och beredskap (MSB) och tillsynsmyndigheterna i uppdrag att påbörja arbetet med myndighetsföreskrifter så att de kan träda ikraft samtidigt som lagen. Det bör också övervägas om berörda myndigheters instruktioner behöver ändras.

MSB bör ges i uppdrag att påbörja identifiering och bedömning av samhällsviktiga tjänster. Föreskriften om samhällsviktiga tjänster bör meddelas senast den 10 maj 2018.

MSB bör ges i uppdrag att vidta förberedelseåtgärder med anledning av kravet på incidentrapportering som träder i kraft den 10 maj 2018.

MSB bör ges i uppdrag att utforma och leda det samarbetsforum för tillsynsmyndigheterna som beskrivs i avsnitt 8.5.4.

MSB bör ges i uppdrag att ta fram vägledningar och riktlinjer för standarder och specifikationer.

Post- och telestyrelsen, Transportstyrelsen och Finansinspektionen bör ges i uppdrag att utreda vilka enheter som omfattas av annan lag eller andra bindande unionsrättsakter med säkerhetskrav eller krav på incidentrapportering vars verkan minst motsvarar verkan av dessa skyldigheter i lagen.

15 Författningskommentar

15.1 Förslaget till lag (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster

Inledande bestämmelser

1 §

Paragrafen genomför artikel 1.1 i NIS-direktivet.

Första stycket innehåller syftet med lagen.

Av *andra stycket* framgår att genom lagen och de föreskrifter som avses komplettera lagen genomförs NIS-direktivet utom vad gäller en nationell strategi.

Bakgrunden till paragrafen behandlas i kapitel 3.

Lagens tillämpningsområde

2 §

Paragrafen genomför artiklarna 5.1, 16.11 och 18.1–2 i NIS-direktivet.

Under a) anges vilka leverantörer av samhällsviktiga tjänster som omfattas av lagen. Med etablerad avses att leverantören utför en faktisk och reell verksamhet med hjälp av en stabil struktur. Den rättsliga formen för en sådan struktur bör enligt skälen till NIS-direktivet inte vara den avgörande faktorn. Hur leverantörer av samhällsviktiga tjänster ska identifieras beskrivs närmare i 8 § samt i 3 § förordningen.

Under b) anges vilka leverantörer av digitala tjänster som omfattas av lagen. I motsats till vad som gäller för leverantörer av sam-

hällsviktiga tjänster ska någon identifiering av leverantörer av digitala tjänster inte ske.

Lagen ska inte tillämpas på leverantörer av digitala tjänster som är mikroföretag eller små företag. Hårdvarutillverkare och mjukvaruutvecklare omfattas av redan befintliga bestämmelser om produktansvar och träffas inte heller av lagen. Näringsidkare som tillhandahåller egna varor och tjänster på en webbplats (e-butik) eller aktörer som använder sig av privata moln är inte leverantörer av digitala tjänster enligt lagen. Lagen ska inte heller tillämpas på jämförelsesajter.

För att en leverantör av digitala tjänster ska omfattas av svensk jurisdiktion krävs att leverantören har sitt huvudsakliga etableringsställe i Sverige, eller har utsett en företrädare här. Det huvudsakliga etableringsstället ska anses vara där leverantören har sitt huvudkontor. Det krävs att leverantören utför en faktisk och reell verksamhet med hjälp av en stabil struktur för att den ska anses vara etablerad. Den rättsliga formen är inte avgörande. Att nätverk och informationssystem är fysiskt belägna på en viss plats innebär inte att det är fråga om ett huvudsakligt etableringsställe. Om leverantören inte är etablerad i unionen, men erbjuder tjänster här, ska leverantören utse en företrädare i något av de länder i Europeiska unionen där tjänsterna erbjuds. Leverantören ska i de fallen omfattas av lagstiftningen i det land där företrädaren finns. Företrädaren bör utses uttryckligen genom en skriftlig fullmakt från leverantören av digitala tjänster att agera på dess vägnar med avseende på leverantörens skyldigheter enligt NIS-direktivet (se 9 §).

Bakgrunden till paragrafen behandlas i kapitel 6 och avsnitt 10.2.5.

Undantag från lagens tillämpningsområde

Elektronisk kommunikation

3 §

Paragrafen genomför första ledet i artikel 1.3 i NIS-direktivet.

Genom paragrafen undantas företag som omfattas av artiklarna 13a och 13b i Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv) från

lagens tillämpningsområde, dock inte företag som tillhandahåller internetknutpunkter.

Säkerhets- och rapporteringskraven i NIS-direktivet ska enligt artikel 1.3 inte tillämpas på företag som omfattas av artiklarna 13a och 13b i ramdirektivet. Internetknutpunkter anses i svensk rätt som sådana allmänna kommunikationsnät som omfattas av 5 kap. 6 b och c §§ lagen (2003:389) om elektronisk kommunikation, som genomför artiklarna. Med hänsyn till att internetknutpunkter är en av de enheter som uttryckligen ska regleras enligt NIS-direktivet ska undantaget för företag som omfattas av artiklarna inte gälla tillhandahållare av internetknutpunkter. Undantaget i denna bestämmelse omfattar alltså inte tillhandahållare av internetknutpunkter. Artiklarna 13a och 13b i ramdirektivet innehåller dock krav på säkerställande av säkerheten i nätverk och informationssystem samt på incidentrapportering. Om verkan av de kraven minst motsvarar verkan av skyldigheterna i denna lag ska bestämmelserna i ramdirektivet tillämpas enligt principen om lex specialis till följd av bindande EU-rättsakter, se 5 § första stycket. Lagen blir i så fall inte tillämplig på tillhandahållare av internetknutpunkter.

Bakgrunden till paragrafen behandlas i avsnitt 5.4.

Betrodda tjänster

4 §

Paragrafen genomför andra ledet i artikel 1.3 i NIS-direktivet.

Säkerhets- och rapporteringskraven i NIS-direktivet ska enligt direktivets artikel 1.3 inte tillämpas på leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 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. Genom paragrafen undantas dessa leverantörer från lagens tillämpningsområde.

Bakgrunden till paragrafen behandlas i avsnitt 5.4.

Avvikande bestämmelser i EU-rättsakter eller i annan författning

5 §

Första stycket genomför artikel 1.7 i NIS-direktivet.

Stadgandet innebär att lagen inte ska tillämpas om det i en bindande EU-rättsakt finns bestämmelser om krav på säkerhetsåtgärder eller incidentrapportering vars verkan minst motsvarar verkan av skyldigheterna enligt lagen (lex specialis). Det innebär t.ex. att identifieringsförfarandet för leverantörer av samhällsviktiga tjänster inte ska genomföras. Någon tillsyn av leverantörerna eller incidentrapportering ska heller inte att ske enligt lagen. Bestämmelser som kan utgöra lex specialis finns t.ex. inom sjöfartssektorn, banksektorn, sektorn för finansmarknadsinfrastruktur och sektorn för digital infrastruktur.

Andra stycket innebär att bestämmelser om säkerhetskrav eller krav på incidentrapportering i nationell lag, som inte grundas på EU-rättsakter, ska tillämpas i stället för lagens bestämmelser om kraven minst motsvarar skyldigheterna i lagen. För att NIS-direktivet ska anses korrekt genomfört krävs dock att lagens bestämmelser tillämpas i den utsträckning det saknas andra bestämmelser. Skulle det t.ex. finnas bestämmelser om krav på tekniska och organisatoriska åtgärder i en särskild lag, men saknas bestämmelser om t.ex. incidentrapportering, tillsyn eller sanktioner, ska lagen tillämpas i sistnämnda delar.

Bakgrunden till paragrafen behandlas i avsnitt 5.4.

Sveriges säkerhet

6 §

Paragrafen genomför artikel 1.6 i NIS-direktivet.

Genom paragrafen undantas verksamhet som är av betydelse för Sveriges säkerhet från lagens tillämpningsområde.

NIS-direktivet påverkar enligt artikel 1.6 inte medlemsstaternas åtgärder för att skydda sina väsentliga statliga funktioner, särskilt för att skydda den nationella säkerheten, inklusive åtgärder för skydd av information vars avslöjande medlemsstaterna anser strida mot sina väsentliga säkerhetsintressen och för att upprätthålla lag och ordning, särskilt för att möjliggöra utredning, upptäckt och lagföring

av brott. När det gäller åtgärder för att upprätthålla lag och ordning finns inte sådan verksamhet inom de sektorer som enligt bilaga 2 till NIS-direktivet omfattas av direktivet.

Verksamhet som är av betydelse för Sveriges säkerhet regleras i säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Enligt det regelverket åligger det den som ansvarar för en verksamhet att undersöka vilka uppgifter i verksamheten som ska hållas hemliga med hänsyn till rikets säkerhet (säkerhetsanalys, 5 § säkerhetsskyddsförordningen), och om verksamheten till följd av förekomsten av sådana uppgifter är av betydelse för Sveriges säkerhet.

Som exempel på hemliga uppgifter kan anges uppgifter som omfattas av försvarssekretess. Försvarssekretess gäller för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs. Förekommer uppgifter om funktionssätt och säkerhet i system som har betydelse för samhällets försörjning eller infrastruktur, omfattas de av bestämmelsen om försvarssekretess. Bestämmelsen gäller oberoende av hos vilken myndighet uppgifterna finns. (15 kap. 2 § OSL)

Det innebär att incidenter i nätverk och informationssystem där det hanteras uppgifter som rör verksamhet eller uppgifter om säkerhetsåtgärder som omfattas av försvarssekretess inte ska rapporteras enligt denna lag. Detta gäller oavsett i vilken sektor incidenten inträffar. I de fall en incident upptäcks genom 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt och detta innebär att en verksamhet får del av uppgifter som omfattas av försvarssekretess, får verksamheten betydelse för Sveriges säkerhet. Bestämmelser om rapportering av incidenter som rör Sveriges säkerhet finns i 10 a § säkerhetsskyddsförordningen.

Beträffande den aggregerade information som Myndigheten för samhällsskydd och beredskap kan komma att få i sin egenskap av mottagare av incidentrapporter bör myndigheten i sin säkerhetsanalys undersöka om aggregerade uppgifter om incidenter inom en sektor eller för samtliga sektorer utgör en ny uppgift och i så fall om den rör Sveriges säkerhet.

Bakgrunden till paragrafen behandlas i kapitel 5, 12 och avsnitt 7.3.2.

Definitioner i lagen

7 §

Paragrafen genomför artikel 4 i NIS-direktivet.

Definitionen av säkerhet i nätverk och informationssystem i *punkten 2* har anpassats till etablerad svensk terminologi där begreppet integritet ersatts med begreppet riktighet. Det framgår också av den engelska versionen av NIS-direktivet att det utöver grundgreppen som definierar informationssäkerhet – tillgänglighet, riktighet och konfidentialitet – inte är integritet som avses utan autenticitet.

I *punkten 3* definieras begreppet leverantör av samhällsviktiga tjänster. De enheter som det hänvisas till kan vara både offentliga och enskilda aktörer.

Definitionerna i *punkterna 13–15* används inte direkt i lagen eller förordningen utan endast indirekt genom hänvisning till bilaga 2 till NIS-direktivet.

Beträffande definitionerna av internetbaserad marknadsplats, internetbaserad sökmotor och molntjänster i *punkterna 16–18* anges i skälen till NIS-direktivet att definitionerna är specifika för direktivet och inte påverkar andra instrument.

Vidare anges i *punkten 19* att 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 benämns NIS-direktivet i lagen.

I *punkten 20* definieras begreppet säkerhetsprinciper (security policies) som används i 26 och 27 §§. Uppräkningen av styrande dokument är inte uttömmande men visar på att det ska vara en viss nivå på dokumenten.

I *punkten 21* definieras vad som i lagen avses med CSIRT-enhet.

Identifiering av leverantörer av samhällsviktiga tjänster

8 §

Paragrafen genomför artiklarna 5.1–2, 5.4 och 6.1–2 i NIS-direktivet.

Verksamheter inom sektorer som finns upptagna som enheter i bilaga 2 till NIS-direktivet och som tillhandhåller en samhällsviktig tjänst ska enligt *första stycket* undersöka om verksamheten är bero-

ende av nätverk och informationssystem och om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

Med samhällsviktig tjänst avses en tjänst som är viktig för samhällets funktionalitet i sin helhet och där ett avbrott i tjänsten hindrar genomförandet av ekonomisk verksamhet, genererar omfattande ekonomiska förluster, undergräver användarnas förtroende och medför allvarliga konsekvenser för landets och unionens ekonomi. I 10 § 2 förordningen bemyndigas Myndigheten för samhällsskydd och beredskap att i föreskrifter fastställa vilka tjänster som är viktiga för att upprätthålla kritisk samhällelig och ekonomisk verksamhet (samhällsviktig tjänst). Myndigheten för samhällsskydd och beredskaps föreskrifter motsvarar det som i artikel 5.3 i NIS-direktivet benämns förteckning. Föreskrifterna får inga direkta rättsverkningar i form av krav på rapportering eller säkerhetsåtgärder för den som tillhandahåller en tjänst som finns på förteckningen. Däremot måste verksamheter som tillhandahåller en tjänst som anges i föreskrifterna undersöka om verksamheten är en leverantör av en samhällsviktig tjänst enligt lagen.

För att fastställa vad som kan anses vara en betydande störning ska enligt *andra stycket* beaktas ett antal sektorövergripande faktorer.

Sektorspecifika faktorer ska enligt *tredje stycket* beaktas när det är lämpligt. Sådana faktorer kan när det gäller energileverantörer vara mängden eller andelen producerad nationell el, för oljeleverantörer mängden olja per dag, för lufttransport, inbegripet flygplatser och lufttrafikföretag, järnvägstransport och kusthamnar andelen nationell trafikmängd och antalet passagerare eller lastningar per år, för bankverksamhet eller finansmarknadsinfrastrukturer deras betydelse för systemet på grundval av samlade tillgångar eller förhållandet mellan dessa tillgångar och BNP, för hälso- och sjukvårdssektorn antalet patienter som leverantören vårdar per år, för produktion, bearbetning och leverans av vatten, volym, antal och typer av användare, inbegripet t.ex. sjukhus, offentlig sektor, organisationer och personer samt förekomsten av alternativa vattenkällor för samma geografiska område.

Inom vissa sektorer finns internationella koder och riktlinjer som bör beaktas när leverantörer ska identifieras. Den samarbetsgrupp som inrättats genom NIS-direktivet ska enligt direktivet verka för en enhetlig tillämpning av faktorerna inom unionen.

Tillhandahålls tjänsten även i ett eller flera andra länder i Europeiska unionen ska den nationella kontaktpunkten enligt *fjärde stycket* samråda med motsvarande funktion i andra berörda länder innan ett beslut om identifiering fattas. Med motsvarande funktion avses nationella kontaktpunkter enligt NIS-direktivet. MSB företräder som nationell kontaktpunkt Sverige i bilaterala och multilaterala samråd i detta avseende.

Undersökningen ska enligt *femte stycket* dokumenteras och innehålla bakgrund och resonemang som legat till grund för bedömningen. Undersökningen är sådan information som leverantören ska tillhandahålla tillsynsmyndigheten enligt 26 § 1.

Bakgrunden till paragrafen behandlas i kapitel 6.

Utseende av företrädare för leverantörer av digitala tjänster

9 §

Paragrafen genomför artikel 18.2 i NIS-direktivet.

En leverantör av digitala tjänster omfattas av jurisdiktionen i det land i den Europeiska unionen där leverantören har sitt huvudsakliga etableringsställe. Det huvudsakliga etableringsstället ska anses vara där leverantören har sitt huvudkontor (se 2 § b). En leverantör som inte har huvudkontor inom Europeiska unionen, men erbjuder tjänster som omfattas av lagen där, ska utse en företrädare i något av de länder i unionen där tjänsten erbjuds. En företrädare är enligt definitionen i 7 § 9 en i unionen etablerad fysisk eller juridisk person som uttryckligen har utsetts att agera för en leverantör av digitala tjänster som inte är etablerad i unionen, till vilken en behörig nationell myndighet eller en CSIRT-enhet kan vända sig, i stället för till leverantören av digitala tjänster, i frågor som gäller de skyldigheter som leverantören av digitala tjänster har enligt lagen. När en företrädare har utsetts omfattas leverantören av jurisdiktionen i det land där företrädaren finns. Företrädaren bör utses uttryckligen genom en skriftlig fullmakt från leverantören att agera på dess vägnar med avseende på leverantörens skyldigheter enligt NIS-direktivet.

Bakgrunden till paragrafen behandlas i avsnitt 10.2.5.

Säkerhetsåtgärder

Leverantörer av samhällsviktiga tjänster

10 §

Paragrafen genomför artikel 14.1–3 i NIS-direktivet.

En förutsättning för en väl anpassad säkerhet är att det bedrivs ett systematiskt och riskbaserat informationssäkerhetsarbete. Det innebär att arbetet ska bedrivas långsiktigt, kontinuerligt och systematiskt samt att arbetet bör ha en tydlig rollfördelning med särskilt utpekat ansvar. I arbetet bör europeiska och internationellt godkända standarder beaktas.

Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om ett systematiskt informationssäkerhetsarbete enligt 10 § 1 förordningen.

Styrdokument avseende det systematiska informationssäkerhetsarbetet är sådan information om säkerhetsprinciper som leverantören ska tillhandahålla tillsynsmyndigheten enligt 26 § 1.

Bakgrunden till paragrafen behandlas i avsnitt 7.3.1–2 och 7.3.4.

11 §

Paragrafen genomför artikel 14.1 i NIS-direktivet.

Med säkerhet i nätverk och informationssystem avses systemens 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 nätverk och informationssystem (7 § 2).

Med teknisk säkerhet brukar avses områdena it-säkerhet (datasäkerhet och kommunikationssäkerhet) och fysisk säkerhet. I begreppet tekniska åtgärder ingår bl.a. skydd mot oönskad förändring, skydd mot obehörig insyn, att behöriga har åtkomst vid rätt tillfälle, skydd av personer, lokaler och utrustning av betydelse för informationssäkerhet samt skydd vid överföring av data. Skyddsåtgärderna ingår i det som brukar benämnas teknisk säkerhet. I begreppet organisatoriska åtgärder ingår bl.a. att upprätta styrdokument, utforma

rutiner, övervaka efterlevnad samt genomföra uppföljningar, dvs. det som brukar benämnas administrativ säkerhet[1]. De tekniska och organisatoriska åtgärder som leverantörer av samhällsviktiga tjänster ska vidta bör inte innebära krav på att någon särskild kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt. För att säkerställa en enhetlig tillämpning av säkerhetsåtgärder bör leverantörerna beakta europeiska eller internationellt accepterade standarder och specifikationer vid utformningen av säkerhetsåtgärder.

Åtgärder för att hantera risker omfattar åtgärder för att identifiera alla incidentrisker och för att förebygga, upptäcka och hantera incidenter för att begränsa deras inverkan. Säkerheten i nätverk och informationssystem omfattar lagrade, överförda och behandlade uppgifters säkerhet. Begreppet risk definieras i 7 § 8.

Med den senaste tekniska utvecklingen avses att samtliga tekniska lösningar som vid var tid finns tillgängliga på marknaden beaktas. Teknisk utveckling kan dels medföra att behovet av säkerhetsåtgärder förändras, dels innebära nya möjligheter att vidta effektiva säkerhetsåtgärder. Lämplig nivå beslutas av den verksamhetsansvarige med hänsyn till den föreliggande risken och de skadekonsekvenser som kan uppkomma. Beslutet ligger till grund för vilka säkerhetsåtgärder som ska vidtas under en viss period, se även 13 § om riskanalys.

Bestämmelser om standarder finns i 4 § förordningen.

Bakgrunden till paragrafen behandlas i avsnitt 7.3.1 och 7.3.4.

12 §

Paragrafen genomför artikel 14.2 i NIS-direktivet.

Säkerhetsåtgärderna i 11 § ska även omfatta åtgärder för att förebygga och minimera verkningar av incidenter i syfte att säkerställa kontinuiteten i tjänsten. När det gäller lämpliga åtgärder hänvisas till kommentaren till 11 §.

Bakgrunden till paragrafen behandlas i avsnitt 7.3.1.

[1] Terminologi för informationssäkerhet, Teknisk rapport SIS-TR 50:2015.

13 §

Paragrafen genomför artikel 14.1–2 i NIS-direktivet.

Valet av säkerhetsåtgärder enligt 11 och 12 §§ ska grunda sig på en riskanalys. Analysen ska kunna användas som beslutsstöd för leverantörens prioriteringar och avvägningar mellan olika typer av säkerhetsåtgärder i förhållande till tjänstens funktionalitet, finansiella och administrativa konsekvenser samt skyddet för den personliga integriteten. Analysen kan ingå som en del i verksamhetens övriga risk- och säkerhetsanalysarbete. Analysen ska dokumenteras, uppdateras årligen och innehålla en åtgärdsplan.

Riskanalysen är sådan information som leverantören ska tillhandahålla tillsynsmyndigheten enligt 26 § 1.

Bakgrunden till paragrafen behandlas i avsnitt 7.3.1.

Leverantörer av digitala tjänster

14 §

Paragrafen genomför artikel 16.1 i NIS-direktivet.

Till skillnad från vad som gäller för leverantörer av samhällsviktiga tjänster ska leverantörer av digitala tjänster själva utarbeta de åtgärder som krävs enligt paragrafen. Tillsynsmyndigheten ska inte meddela några närmare föreskrifter i detta avseende. I stället ska kommissionen senast den 9 augusti 2017 anta genomförandeakter för att specificera de element som leverantörerna ska ta hänsyn till vid bedömningen av vilka säkerhetsåtgärder som ska utarbetas och vidtas.

Begreppen tekniska och organisatoriska åtgärder och senaste tekniska utvecklingen behandlas i kommentaren till 11 §.

Med incidenthantering avses enligt definitionen i 7 § 7 alla förfaranden som stöder upptäckt, analys och begränsning av en incident och åtgärder mot en incident.

Bakgrunden till paragrafen behandlas i avsnitt 10.3.

15 §

Paragrafen genomför artikel 16.2 i NIS-direktivet.

Säkerhetsåtgärderna i 14 § ska även omfatta åtgärder för att förebygga och minimera verkningar av incidenter i syfte att säkerställa

kontinuiteten i tjänsten. När det gäller lämpliga åtgärder hänvisas till kommentaren till 11 §.

Bakgrunden till paragrafen behandlas i avsnitt 10.3.

Incidentrapportering

Leverantörer av samhällsviktiga tjänster

16 §

Paragrafen genomför artikel 14.3 i NIS-direktivet.

Paragrafens *första stycke* anger vem som ska rapportera incidenter och när rapporteringen ska ske. Endast händelser med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem och som orsakat en betydande inverkan på kontinuiteten på tjänsten ska rapporteras.

Ansvaret för rapportering åligger den verksamhet som identifierats som leverantör av en samhällsviktig tjänst.

Med utan onödigt dröjsmål avses att rapporteringen ska ske så snart de uppgifter som ska lämnas finns tillgängliga. Kravet på rapportering ska inte inverka negativt på arbetet att avhjälpa incidenten. Rapportering bör därför ske efter att de första kritiska åtgärderna för att avhjälpa incidenten vidtagits. I de fall incidenten påverkar flera leverantörer eller är gränsöverskridanden bör rapportering ske snarast. Det innebär att en första rapportering kan komma att behöva kompletteras när incidenten avhjälpts.

Myndigheten för samhällsskydd och beredskap får meddela närmare föreskrifter om incidentrapportering.

Det kan finnas skäl för att även andra leverantörer än de som är rapporteringsskyldiga enligt denna lag ska kunna rapportera incidenter enligt ett system för frivillig rapportering. Myndigheten för samhällsskydd och beredskap får föreskriva om de närmare förutsättningarna för sådan frivillig rapportering enligt 10 § 4 förordningen.

Incidenter som är av betydelse för Sveriges säkerhet ska inte rapporteras enligt denna lag. Sådana incidenter rapporteras i stället enligt 10 a § säkerhetskyddsförordningen (1996:633), se avsnitt 5.4.

I *andra stycket* anges att ett krav på innehåll i rapporten är att det ska vara möjligt att fastställa om incidenten har gränsöverskridande verkningar. Närmare utformning av rapporterns innehåll meddelas

i myndighetsföreskrifter, se 10 § 3 förordningen. Vid utformningen av rapporten bör även hänsyn tas till att den nationella kontaktpunkten ska lämna en sammanfattande rapport till kommissionen en gång om året. I rapporten ska bland annat ingå uppgifter om incidentens art och om vilka åtgärder som vidtagits (artikel 10.3). Vid rapporteringen bör inga personuppgifter behandlas utöver vad som krävs för administration av rapporten.

CSIRT-enheten får enligt *tredje stycket* inte ställa några ytterligare krav på leverantören med anledning av rapporteringen av incidenten som t.ex. ytterligare utredning.

Bakgrunden till paragrafen behandlas i avsnitt 7.3.2 och 7.3.4.

17§

Paragrafen genomför artikel 14.4 i NIS-direktivet.

Fastställandet av vilka incidenter som har en betydande inverkan på kontinuiteten i en samhällsviktig tjänst bör utgå från de faktorer som anges i bestämmelsen samt de förhållanden som finns inom respektive sektor. Beroende på vilken sektor som avses kan faktorerna också ges olika vikt. Befintliga bestämmelser om kontinuitet och driftsäkerhet i sektorn bör kunna användas som en utgångspunkt i den utsträckning det är lämpligt.

Den samarbetsgrupp som inrättats genom NIS-direktivet får utarbeta och anta riktlinjer om incidentrapportering och vilka faktorer som ska användas för fastställandet av hur betydande en incidents inverkan är (artikel 14.7). Myndigheten för samhällsskydd och beredskap är Sveriges representant i samarbetsgruppen och i den utsträckning samarbetsgruppen utarbetar och antar riktlinjer för skyldigheten att rapportera incidenter och vilka faktorer som ska användas bör Myndigheten för samhällsskydd och beredskap lämna råd och stöd till tillsynsmyndigheterna vid utarbetandet av myndighetsföreskrifter.

Fastställandet bör samordnas med förfarandet för fastställande av om en störning är betydande när leverantörer av samhällsviktiga tjänster identifieras.

Bakgrunden till paragrafen behandlas i avsnitt 6.2.2 och 7.3.2.

18 §

Paragrafen genomför artikel 16.5 i NIS-direktivet.

Till följd av bestämmelsen får CSIRT-enheten och tillsynsmyndigheten kännedom om incidenter och eventuella brister i säkerheten hos leverantörer av digitala tjänster som påverkat samhällviktiga tjänster. Incidenten kan utgöra bevis för att en leverantör av digitala tjänster inte uppfyller kraven på säkerhet och därmed ligga till grund för tillsynsåtgärder.

Vid rapportering ska inga personuppgifter behandlas utöver vad som krävs för administration av rapporten.

Bakgrunden till paragrafen behandlas i avsnitt 7.3.2.

Leverantörer av digitala tjänster

19 §

Paragrafen genomför artikel 16.3 i NIS-direktivet.

Med en incident avses enligt definitionen i 7 § 6 en händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem. Angående begreppet utan onödigt dröjsmål, se kommentaren till 16 §.

Kommissionen får anta genomförandeakter som fastställer format och förfaranden tillämpliga på rapporteringen. Till dess att sådana genomförandeakter antagits meddelas närmare föreskrifter i detta avseende i myndighetsföreskrifter, se 10 § 3 förordningen.

Vid rapporteringen bör inga personuppgifter behandlas utöver vad som krävs för administration av rapporten.

Att rapporteringen inte ska medföra ökat ansvar för den som rapporterat innebär att det inte får ställas några ytterligare krav på leverantören med anledning av rapporteringen. Det är t.ex. inte tillåtet att begära att leverantören genomför ytterligare utredning om incidenten.

Bakgrunden till paragrafen behandlas i avsnitt 10.3.

20 §

Paragrafen genomför artikel 16.4 i NIS-direktivet.

Bedömningen av om en incident har en avsevärd inverkan på tillhandahållandet av tjänsten ska framför allt göras utifrån de faktorer som anges i paragrafens *första stycke*. Till skillnad från vad som gäller för leverantörer av samhällsviktiga tjänster får tillsynsmyndigheten inte meddela föreskrifter i detta avseende. Kommissionen ska emellertid senast den 9 augusti 2017 anta genomförandeakter för att specificera faktorerna.

Av paragrafens *andra stycke* framgår att rapporteringsskyldigheten gäller bara om leverantören har tillgång till den information som behövs för att bedöma en incidents inverkan mot bakgrund av de angivna faktorerna. Detta innebär inte att rapporteringsskyldigheten bortfaller för det fall att någon av faktorerna är okända för leverantören. I vissa fall kan leverantören sakna möjlighet att ta reda på t.ex. antalet användare. Ett sådant exempel är när en molntjänstleverantör agerar personuppgiftsbiträde. Det kan då finnas uppgifter lagrade hos leverantöreren som leverantören kan vara förhindrad att behandla för egen räkning.

Bakgrunden till paragrafen behandlas i avsnitt 10.3.

Förpliktande att informera allmänheten om en incident

21 §

Paragrafen genomför artikel 16.7 i NIS-direktivet såvitt gäller skyldigheten för en leverantör att informera allmänheten om en incident.

Enligt NIS-direktivet får även behöriga myndigheter eller CSIRT-enheter i andra berörda länder i Europeiska unionen kräva att en leverantör av digitala tjänster under svensk jurisdiktion informerar allmänheten om en incident. I dessa fall får kravet mot leverantören framställas av den svenska CSIRT-enheten efter samråd inom CSIRT-nätverket eller med den behöriga myndigheten i det andra landet.

Bakgrunden till paragrafen behandlas i avsnitt 11.2.3.

Tillsyn

22 §

Paragrafen genomför artikel 8.1–2 i NIS-direktivet.

Syftet med åtgärden tillsyn är att kunna bedöma hur leverantörerna uppfyller säkerhetskraven och kraven på incidentrapportering samt bedöma vilka effekter direktivets krav får på säkerheten i nätverk och informationssystem. Det innebär att tillsyn i form av självskattning eller kontroll av att relevant dokumentation finns på plats inte uppfyller direktivets krav.

Resultatet från en tillsyn kan ligga till grund för sanktioner och förelägganden om att avhjälpa brister.

I 5 § förordningen anges vilka myndigheter som är nationella behöriga myndigheter, *tillsynsmyndigheter*, och att det finns en tillsynsmyndighet för varje sektor.

Bakgrunden till paragrafen behandlas i avsnitt 8.3.1 och 8.5.1–2.

23 §

Genom paragrafen genomförs artiklarna 15.1 och 17.2 a i NIS-direktivet.

Bestämmelsen ger tillsynsmyndigheten tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, i den utsträckning det krävs för att kunna utöva tillsyn.

Bakgrunden till paragrafen behandlas i avsnitt 8.5.3.

24 §

Paragrafen genomför artiklarna 15.2 och 17.2 a i NIS-direktivet.

Tillsynsmyndigheten får enligt *första stycket* förelägga en leverantör att tillhandahålla information enligt 26 och 27 §§.

Bestämmelsen kan också användas i de fall den som tillhandahåller en samhällsviktig tjänst inte anser sig omfattas av lagen. Genom att tillsynsmyndigheten utfärdar ett föreläggande som kan överklagas kan frågan om lagens tillämpningsområde prövas av domstol.

Ett beslut om föreläggande får enligt *andra stycket* förenas med vite. Beslutet kan överklagas, se 49 §.

Bakgrunden till paragrafen behandlas i avsnitt 6.2.2 och 8.5.3.

25 §

Paragrafen genomför artiklarna 15.1 och 17.2 a i NIS-direktivet.

Tillsynsmyndigheterna ska ha de befogenheter som de behöver för att utöva tillsyn och bör därför vid behov kunna begära biträde av Kronofogdemyndigheten.

Bakgrunden till paragrafen behandlas i avsnitt 8.5.3.

Leverantörer av samhällsviktiga tjänster

26 §

Paragrafen genomför artikel 15.2 i NIS-direktivet.

I paragrafens *första stycke* anges i punkterna 1–3 vilken information som leverantören av samhällsviktiga tjänster ska tillhandahålla tillsynsmyndigheten för att tillsynsmyndigheten ska kunna utöva en effektiv tillsyn. Det kan vara fråga om risk- och säkerhetsanalyser, åtgärdsplaner, dokumenterade säkerhetsprinciper, genomförda säkerhetsrevisioner m.m.

I *andra stycket* anges att tillsynsmyndigheten måste kunna uppge syftet med begäran och precisera vilken information som krävs. Bakgrunden till detta är att leverantören ska åsamkas så lite olägenheter som möjligt.

Dock måste leverantören alltid kunna beskriva hur det systematiska informationssäkerhetsarbetet ser ut för att tillsynsmyndigheten ska kunna få en uppfattning om hur informationssäkerhetsarbetet styrs och vilken information som är nödvändig för att kunna genomföra tillsynen.

Bakgrunden till paragrafen behandlas i avsnitt 8.5.3.

Leverantörer av digitala tjänster

27 §

Paragrafen genomför artikel 17.2 a i NIS-direktivet.

Bakgrunden till paragrafen behandlas i avsnitt 10.4.

28 §

Paragrafen genomför artikel 17.1 i NIS-direktivet.

Till skillnad mot vad som gäller beträffande leverantörer av samhällsviktiga tjänster ska tillsynsåtgärder beträffande leverantörer av digitala tjänster vidtas bara när tillsynsmyndigheten på något sätt fått kännedom om att leverantören inte uppfyller lagens krav. Tillsynsmyndigheten kan få sådan kännedom genom t.ex. en tjänsteanvändare, andra tillsynsmyndigheter eller genom incidentrapporteringen.

Bakgrunden till paragrafen behandlas i avsnitt 10.4.

Sanktioner och ingripanden

Underrättelse m.m.

29 §

Paragrafen är tillämplig endast på leverantörer av samhällsviktiga tjänster. Beträffande leverantörer av digitala tjänster får tillsynsmyndigheten inte vidta några tillsynsåtgärder om den inte fått kännedom om att leverantören inte följer regelverket.

Vad som är skälig tid enligt paragrafen får avgöras utifrån omständigheterna i det enskilda fallet. Att en leverantör av samhällsviktiga tjänster inte yttrar sig hindrar inte tillsynsmyndigheten från att gå vidare i tillsynen.

Bakgrunden till paragrafen behandlas i avsnitt 9.7.

30 §

Paragrafen genomför artiklarna 15.3 och 17.2 b i NIS-direktivet och är tillämplig på både leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster.

Det är inte givet att kännbara sanktioner i alla lägen är det mest effektiva sättet att uppnå lagens syfte. I de fall tillsynsmyndigheten konstaterar att en leverantör av samhällsviktiga tjänster eller en leverantör av digitala tjänster gjort sig skyldig till en överträdelse bör tillsynsmyndigheten, på lämpligt sätt, försöka förmå leverantören att vidta rättelse.

Bakgrunden till paragrafen behandlas i avsnitt 9.7.

Förelägganden m.m.

31§

Paragrafen genomför artiklarna 15.3, 17.2 b och 21 i NIS-direktivet.

Bakgrunden till paragrafen behandlas i avsnitt 8.5.3 och 9.5.

Sanktionsavgift

32 §

Paragrafen genomför artikel 21 i NIS-direktivet.

Avgiftsskyldigheten bygger på strikt ansvar.

Även statliga myndigheter och kommuner kan meddelas beslut om sanktionsavgift enligt lagen, se avsnitt 9.8.

Bakgrunden till paragrafen behandlas i avsnitt 9.6.

33 §

Paragrafen genomför artikel 21 i NIS-direktivet.

Angivna lägsta och högsta belopp är desamma som de som i dag gäller för företagsbot.

Bakgrunden till paragrafen behandlas i avsnitt 9.6.4.

34 §

Paragrafen genomför artikel 21 i NIS-direktivet.

Vid bestämningen av sanktionsavgiften i det enskilda fallet bör hänsyn tas till alla relevanta omständigheter. De omständigheter som anges i paragrafen bör särskilt beaktas. Uppräkningen är emellertid inte uttömmande. Utöver de i lagen angivna omständigheterna kan hänsyn behöva tas till hur länge överträdelsen pågått, om aktören tidigare har gjort sig skyldig till överträdelser av lagen, om överträdelserna i så fall är likartade och hur lång tid som gått mellan överträdelserna. Den överträdda bestämmelsens betydelse för tillsynsområdet kan också vara relevant. I mildrande riktning kan det vara aktuellt att beakta om leverantören har samarbetat med tillsynsmyndigheten för att komma till rätta med överträdelsen.

Bakgrunden till paragrafen behandlas i avsnitt 9.6.5.

35 §

Paragrafen genomför artikel 21 i NIS-direktivet.

Mot bakgrund av att avgiftsskyldigheten bygger på strikt ansvar måste det finnas en möjlighet för tillsynsmyndigheten att underlåta att besluta om sanktionsavgift. Tillsynsmyndigheten bör i det enskilda fallet göra en nyanserad bedömning av om omständigheterna ger anledning till jämkning eller eftergift. Omständigheter som kan vara av betydelse kan vara överträdelsens allvarlighet och om leverantören gjort rättelse. En annan situation som kan innebära att det framstår som oskäligt att besluta om sanktionsavgift är om leverantören drabbas av sanktionsavgift enligt något annat regelverk för i princip samma brist. Det skulle också kunna uppstå situationer där en leverantör på grund av avtal med t.ex. en underleverantör blir skyldig att betala skadestånd till följd av en brist som sanktioneras genom lagens bestämmelser.

Bakgrunden till paragrafen behandlas i avsnitt 9.6.6.

36 §

Paragrafen genomför artikel 21 i NIS-direktivet.

Om vite har dömts ut är det inte möjligt att besluta om sanktion för samma sak. Den avgörande tidpunkten för när sådant hinder uppkommer är när det inleds en domstolsprocess angående frågan om utdömande av vitet. Ett föreläggande om vite hindrar inte ett senare beslut om sanktionsavgift så länge tillsynsmyndigheten inte har ansökt om utdömande av vitet.

Bakgrunden till paragrafen behandlas i avsnitt 9.6.7.

37 §

Paragrafen genomför artikel 21 i NIS-direktivet.

Paragrafen reglerar förfarandet vid beslut om sanktionsavgift.

Bakgrunden till paragrafen behandlas i avsnitt 9.6.8.

38 §

Paragrafen genomför artikel 21 i NIS-direktivet.

Paragrafen innebär att sanktionsavgift inte får beslutas om den som anspråket riktas mot inte har getts tillfälle att yttra sig inom två år från överträdelsen.

Bakgrunden till paragrafen behandlas i avsnitt 9.6.8.

39–42 §§

Paragraferna genomför artikel 21 i NIS-direktivet.

I paragraferna anges hur betalning av sanktionsavgift ska ske och att beslut om sanktionsavgift vid utebliven betalning får ske utan föregående dom eller utslag. Vidare anges att obetald avgift ska lämnas för indrivning. Bestämmelser om indrivning av statliga fordringar finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Slutligen stadgas att en beslutad avgift faller bort om beslutet inte har verkställts inom fem år från laga kraft.

Bakgrunden till paragraferna behandlas i avsnitt 9.6.9.

Gemensam nationell kontaktpunkt

43 §

Paragrafen genomför artikel 8.3 i NIS-direktivet.

Myndigheten för samhällsskydd och beredskap är enligt 7 § förordningen gemensam nationell kontaktpunkt.

Den gemensamma kontaktpunktens uppgifter anges i 7 § förordningen.

Bakgrunden till paragrafen behandlas i avsnitt 11.1.

Enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet)

44 §

Paragrafen genomför artiklarna 9.1, 14.3 och 16.3 i NIS-direktivet.

Myndigheten för samhällsskydd och beredskap är enligt 8 § förordningen CSIRT-enhet i Sverige.

Kraven på CSIRT-enheten och CSIRT-enhetens uppgift anges i 8 § förordningen samt i punkt 2 i bilaga 1 till NIS-direktivet.

Bakgrunden till paragrafen behandlas i avsnitt 7.3.2 och 11.2.

Bemyndigande

45 §

Paragrafen genomför artiklarna 6 och 14.1–2 och 4 i NIS-direktivet.

Bemyndigandet i *punkt 1* gör det möjligt att meddela föreskrifter om de sektorspecifika och sektorövergripande faktorer som ska beaktas när det fastställs om en incident medför en betydande störning vid identifiering av leverantörer av samhällsviktiga tjänster. I 11 § förordningen bemyndigas tillsynsmyndigheten att, utifrån sina kunskaper om verksamheten och om konsekvenserna av en incident, meddela föreskrifter i detta avseende.

I arbetet med att ta fram sektorspecifika faktorer har samarbetsgruppen en viktig uppgift att verka för att bedömningen blir enhetlig inom hela unionen (artikel 5.6). Myndigheten för samhällsskydd och beredskap företräder Sverige i samarbetsgruppen som inrättats genom NIS-direktivet och tillsynsmyndigheterna ska stödja Myndigheten för samhällsskydd och beredskap med information om antalet leverantörer och eventuella tröskelvärden.

Bemyndigandet i *punkt 2* gör det möjligt att meddela föreskrifter om ett systematiskt och riskbaserat informationssäkerhetsarbete. Detta är ett sätt för verksamhetens ledning att systematiskt styra arbetet med informationssäkerhet. Arbetet bör utgå från en godkänd nationell eller internationell standard. Föreskrifter om detta finns redan i dag för statliga myndigheter (MSBFS 2016:1).

Föreskrifter enligt paragrafen ska enligt 10 § förordningen meddelas av Myndigheten för samhällsskydd och beredskap. I beredningen av föreskrifterna bör även beaktas bestämmelserna i förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Bemyndigandet i *punkt 3* gör det möjligt att meddela föreskrifter om vilka faktorer som ska användas för att avgöra om en incident ska rapporteras. Enligt 11 § 3 förordningen får tillsynsmyndigheten meddela sådana föreskrifter. Bedömningen bör utgå från de faktorer som anges i 17 § samt de förhållanden som finns inom respektive sektor. Beroende på vilken sektor som avses kan faktorerna också

tillmätas olika vikt. En incident är enligt 7 § 6 en händelse som har en faktisk inverkan på säkerheten i nätverk eller informationssystem. I den utsträckning samarbetsgruppen som inrättats enligt NIS-direktivet utarbetar och antar riktlinjer för vilka faktorer som ska användas för att fastställa om en incident har en betydande inverkan bör Myndigheten för samhällsskydd och beredskap, som ingår i samarbetsgruppen, lämna råd och stöd i föreskriftsarbetet (artikel 14.7).

Kostnadsmässiga och andra konsekvenser av myndighetsföreskrifter som meddelas i anslutning till lagen ska utredas enligt förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Bakgrunden till paragrafen behandlas i avsnitt 6.2.2, 7.3.1 och 7.3.2.

Föreskrifter

Leverantörer av samhällsviktiga tjänster

46 §

Paragrafen genomför artiklarna 5.3, 14.1–3 och 20 i NIS-direktivet

Bestämmelsen upplyser om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om samhällsviktiga tjänster, säkerhetsåtgärder, rapportering av incidenter samt förutsättningarna för frivillig rapportering av incidenter. Sådana föreskrifter finns i 10 § 2–4 och 11 § 1 i förordningen.

Kostnadsmässiga och andra konsekvenser av myndighetsföreskrifter som meddelas i anslutning till lagen ska utredas enligt förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Bakgrunden till paragrafen behandlas i avsnitt 6.2.1, 7.3.1, 7.3.2. och 7.3.4.

Leverantörer av digitala tjänster

47 §

Paragrafen genomför artiklarna 16.3 och 20 i NIS-direktivet

Bestämmelsen upplyser om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om rapportering av incidenter samt förutsättningarna för frivillig rapportering av incidenter. Sådana föreskrifter finns i 10 § 3–4 i förordningen.

Bakgrunden till paragrafen behandlas i avsnitt 10.3.

Överklagande m.m.

48 §

Paragrafen innebär en möjlighet för tillsynsmyndigheten att i enskilda fall bestämma att dess beslut om föreläggande ska gälla omedelbart för att undvika att beslutet förhalas genom ett överklagande. Den som beslutet gäller har vid ett överklagande av ett sådant beslut emellertid möjlighet att begära att beslutet tills vidare inte ska gälla, s.k. inhibition. Bestämmelser om inhibition finns i 28 § förvaltningsprocesslagen (1971:291).

Bakgrunden till paragrafen behandlas i avsnitt 9.9.

49 §

Paragrafen reglerar möjligheterna till överklagande av beslut enligt lagen.

Bakgrunden till paragrafen behandlas i avsnitt 9.10.

Kommittédirektiv 2016:29

Genomförande av EU-direktiv om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem

Beslut vid regeringssammanträde den 31 mars 2016

Sammanfattning

En särskild utredare ska föreslå hur EU-direktivet om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem ska genomföras i svensk rätt.

Utredaren ska bl.a.

- föreslå hur direktivets krav på utpekande av myndigheter med ansvar för vissa funktioner ska genomföras, med inriktningen att Myndigheten för samhällsskydd och beredsskap (MSB) ges en samordnande roll på området men att andra myndigheters ansvar för tillsyn inom särskilda sektorer ska fortsätta att gälla,
- föreslå hur identifiering av och krav på aktörer som omfattas av direktivet kan genomföras i ett samlat regelverk med beaktande av gällande bestämmelser, sektorsansvar och vad som är mest effektivt utifrån olika perspektiv,
- föreslå nödvändiga ändringar i offentlighets- och sekretesslagen (2009:400) för att känslig information i incidentrapporter ska kunna skyddas, och
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 1 maj 2017.

EU-direktivet och motsvarande svenska regler

Direktivet innehåller bl.a. skyldigheter för varje medlemsstat att anta en nationell strategi för säkerhet i nätverk och informationssystem och att utse myndigheter med särskilda uppgifter på detta område. Medlemsstaterna blir vidare skyldiga att identifiera operatörer som bedriver samhällsviktig verksamhet inom sju sektorer och som är beroende av nätverk och informationssystem. Sektorerna omfattar energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten och digital infrastruktur. Den aktuella sektorsindelningen innebär att kommunala verksamheter kan omfattas. För sådana aktörer innebär direktivet bl.a. att verksamheten kan komma att behöva anpassas för att uppnå en hög nivå av säkerhet i nätverk och informationssystem och att it-incidenter av viss dignitet ska rapporteras till behörig myndighet. Direktivet bedöms träda i kraft under våren 2016. Medlemsstaterna är skyldiga att ha genomfört direktivet senast 21 månader därefter.

Frågor som berör informations- och cybersäkerhet och särskilt hur it-incidenter ska förebyggas och hanteras har tidigare varit aktuella i ett flertal utredningar. Riksrevisionen har i en rapport från november 2014 (RiR 2014:23) funnit brister i regeringens arbete med informationssäkerhetsfrågor inom den civila statsförvaltningen. Granskningen föranledde Riksrevisionen att lämna ett flertal rekommendationer till regeringen och dess myndigheter. Riksrevisionen påpekade särskilt att det finns ett behov av att utreda hur tillsynen över informationssäkerheten kan samlas och koordineras på ett bättre sätt än i dag. Även i betänkandena Informations- och cybersäkerhet i Sverige (SOU 2015:23) och En ny säkerhetsskyddslag (SOU 2015:25) lämnas förslag på åtgärder inom informationssäkerhetsområdet.

Regeringen har konstaterat att delar av arbetet med informationssäkerhet i den civila statsförvaltningen inte har genomförts ändamålsenligt (skr. 2014/15:84). Som ett första steg för att förbättra samhällets förmåga att identifiera, begränsa och förhindra it-angrepp mot informationssystem i samhället, har regeringen tagit initiativ till ett system för obligatorisk it-incidentrapportering för statliga myndigheter. De bestämmelser som införts i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder

vid höjd beredskap och i säkerhetsskyddsförordningen (1996:633) innebär att alla statliga myndigheter från den 1 april 2016 ska rapportera allvarliga it-incidenter till MSB eller, i vissa fall, till Säkerhetspolisen eller Försvarsmakten. Detta system utelämnar dock enskilda aktörer samt kommuner och landsting. Bestämmelser som rör it-incidentrapportering för enskilda aktörer finns i dag i begränsad utsträckning, t.ex. för de aktörer som omfattas av lagen (2003:389) om elektronisk kommunikation. Genomförandet av direktivet, som även omfattar andra aktörer än statliga myndigheter, i svensk rätt är därför av stor betydelse för att uppnå en förbättrad informations- och cybersäkerhet i samhället.

Uppdraget att föreslå hur EU-direktivet ska genomföras

Det är viktigt att säkerställa en hög nivå av säkerhet för nätverk och informationssystem inom ett antal sektorer i Sverige i enlighet med EU-direktivet. Hänsyn ska också tas till behovet av att skydda Sveriges säkerhet, behovet av en fungerande brottsbekämpning och myndigheters och företags behov av att kunna skydda känsliga uppgifter. Regelverket ska dock inte skapa en större administrativ börda för de enskilda aktörerna än nödvändigt för direktivets efterlevnad. Enkelhet, överskådlighet, konsekvens och kostnadseffektivitet ska eftersträvas.

Direktivet innebär ett antal långtgående skyldigheter för medlemsstaterna i och med de krav som direktivet ställer på att varje medlemsstat ska ta fram en nationell strategi, peka ut myndigheter med särskilt ansvar enligt direktivet och identifiera och ställa krav på de aktörer som berörs av bestämmelserna.

I betänkandet Informations- och cybersäkerhet i Sverige (SOU 2015:23) föreslås att regeringen ska anta en nationell strategi för statens informations- och cybersäkerhet. Betänkandet har remitterats och bereds för närvarande inom Regeringskansliet. Regeringen avser att prioritera detta arbete och bedömer att strategin bör kunna anpassas för att motsvara direktivets krav på vad en nationell strategi för säkerhet i nätverk och informationssystemska innehålla. Frågan om hur en sådan strategi bör utformas omfattas således inte av utredarens uppdrag.

Hur ska ansvarsfördelningen mellan myndigheter i Sverige se ut?

Direktivet ålägger medlemsstaterna att utse en eller flera behöriga myndigheter som utövar tillsyn över direktivets genomförande och tillämpning. En viktig åtgärd för att direktivet ska kunna tillämpas är att medlemsstaternas tillsynsmyndigheter ges tillräckliga befogenheter för att kontrollera att aktörerna, dvs. operatörer som bedriver samhällsviktig verksamhet och leverantörer av digitala tjänster, följer direktivet. Myndigheterna ska därför enligt direktivet ha möjlighet att begära dels att aktörerna lämnar nödvändig information om säkerheten i sina nätverk och informationssystem, dels att de genomgår säkerhetsrevision. Medlemsstaterna ska också se till att tillsynsmyndigheten har tillgång till effektiva och proportionerliga sanktioner. I medlemsstaterna ska det även finnas ett eller flera incidenthanteringsorgan (s.k. CSIRT, Computer Security Incident Response Team) och en nationell kontaktpunkt för samarbetet med andra medlemsstater. Den nationella kontaktpunkten ska vara ansvarig för att samordna frågor om säkerhet i nätverk och informationssystem enligt direktivet och fungera som kontaktpunkt i gränsöverskridande frågor på unionsnivå.

Direktivet ställer också krav på ett formaliserat samarbete mellan medlemsstaterna, bl.a. när en medlemsstat identifierar operatörer som bedriver samhällsviktig verksamhet även i annan medlemsstat. Genom direktivet inrättas också en samarbetsgrupp där representanter för medlemsstaterna ska delta och ett formellt samarbete mellan de nationella organisationerna för CSIRT. Samarbetsgruppen är tänkt att ha en strategisk funktion medan medlemsstaterna inom ramen för ett särskilt CSIRT-nätverk bl.a. ska kunna utbyta operativ information och diskutera specifika problem med koppling till inträffade it-incidenter.

MSB har i dag ett särskilt uppdrag inom samhällets informationssäkerhet. Enligt MSB:s instruktion ansvarar myndigheten bl.a. för att stödja och samordna arbetet med samhällets informationssäkerhet, i vilket ingår förebyggande arbete liksom även samordning och hantering vid inträffade it-incidenter. MSB svarar vidare 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 (Computer Emergency Response Team) och innebär därutöver att myndigheten är Sveriges kontakt-

punkt gentemot motsvarande funktioner i andra länder, däribland CERT-EU. MSB har sedan funktionen fördes över till myndigheten från Post- och telestyrelsen fortsatt att bygga upp såväl kompetens som ett brett kontaktnät inom informationssäkerhetsområdet. Det finns flera myndigheter som utövar tillsyn över informationssäkerheten inom sina sektorer och som inom dessa områden är bemyndigade att utfärda föreskrifter. Detta gäller exempelvis Post- och telestyrelsen, Svenska kraftnät och Finansinspektionen. Även Säkerhetspolisen och Försvarsmakten utfärdar föreskrifter om bl.a. informationssäkerhet för verksamheter som omfattas av kraven i säkerhetsskyddslagen (1996:627). Den tillsyn som Säkerhetspolisen och Försvarsmakten genomför mot bakgrund av dessa föreskrifter faller utanför EU-direktivet eftersom det gäller nationell säkerhet. Detsamma gäller för elektroniska kommunikationstjänster, e-legitimationer och betrodda tjänster i enlighet med EU-direktivets artikel 1 (3).

Mot bakgrund av det uppdrag som MSB i dag har på informationssäkerhetsområdet och den kompetens som finns inom myndigheten bör Sveriges CSIRT-organisation finnas hos MSB och MSB anförtros rollen som nationell kontaktpunkt. Det innebär att det är till MSB som aktörerna ska rapportera it-incidenter i enlighet med EU-direktivets krav. Detta hindrar dock inte att aktörerna kan ha skyldighet att rapportera it-incidenter till den myndighet som har tillsynsansvar inom den aktuella sektorn. I MSB:s roll bör det också ingå att delta i CSIRT-nätverket och i den samarbetsgrupp som skapas.

Tillsynsmyndigheterna inom de sektorer som omfattas av direktivet bör även fortsättningsvis ha kvar ansvaret för att kontrollera att aktörerna följer respektive sektors regler om informationssäkerhet. Det behöver analyseras om dessa myndigheters mandat behöver förändras för att uppfylla direktivets krav. För sådana aktörer som träffas av direktivet och där tillsyn över säkerheten i nätverk och informationssystem i dag saknas, behöver det övervägas vilken myndighet som kan anförtros uppgiften att utöva tillsyn. I avsaknad av andra myndigheter med tillsynsuppgifter inom den aktuella sektorn och inom informationssäkerhet, bör det utredas om MSB ska vara tillsynsmyndighet eller om uppgiften ska anförtros en myndighet med närliggande tillsynsuppgifter. Detta kan t.ex. övervägas inom olje- och gassektorn. Inriktningen bör vara att Post- och telestyrel-

sen ges fortsatt och vid behov kompletterande ansvar för tillsyn av de digitala infrastrukturer som nämns i EU-direktivets bilaga 2.

Då MSB redan i dag har ansvar för att samordna arbetet med samhällets informationssäkerhet bör MSB få en samordnande roll mellan tillsynsmyndigheterna. Utöver att vara CSIRT, nationell kontaktpunkt och att delta i samarbetsgrupperna innebär denna roll att MSB behöver få del av tillsynsrapporter från andra sektorsmyndigheter i syfte att få en samlad bild över EU-direktivets genomförande och tillämpning i Sverige. Detta medför dock inte något övertagande av sektorsmyndigheternas ansvar för tillsyn över aktörer eller något mandat att styra hur dessa myndigheter ska använda sina resurser.

Eftersom direktivet möjliggör för medlemsstaterna att skydda information som gäller nationell säkerhet är det av vikt att MSB och andra tillsynsmyndigheter, om de får del av information som omfattas av säkerhetsskyddslagstiftningen, samverkar med Säkerhetspolisen eller Försvarsmakten.

Utredaren ska

- föreslå hur MSB:s roll som CSIRT-organisation, nationell kontaktpunkt och deltagare i de samarbetsnätverk som direktivet lägger grund för ska utformas och regleras, och
- lämna förslag på ett system för tillsyn i enlighet med direktivets krav, där befintliga myndigheter behåller eller kompletterar sina nuvarande roller, men där MSB ges en samordnande funktion.

Hur ska operatörer identifieras och vilka krav ska ställas på dem och leverantörer av digitala tjänster?

Direktivet ålägger medlemstaterna att identifiera de offentliga och enskilda operatörer som tillhandahåller samhällsviktiga tjänster inom ett antal särskilt utpekade sektorer och som är beroende av nätverk och informationssystem. Medlemsstaterna ska enligt direktivet införa regler som innebär att dessa aktörer ska vidta tekniska och organisatoriska åtgärder för att hantera säkerhetsrisker i sina nätverk och informationssystem och att rapportera allvarliga it-incidenter.

Vid sidan av operatörer som bedriver samhällsviktig verksamhet reglerar direktivet även på liknande sätt säkerheten i nätverk och informationssystem hos leverantörer av digitala tjänster, s.k. Digital Service Providers (DSP). I den kategorin ingår e-handelsplatser, sök-

motorer och molntjänster. Gemensamt för dessa aktörer är att de tillhandahåller digitala tjänster över nationsgränserna och att en incident hos en sådan aktör skulle kunna medföra allvarlig påverkan på flera medlemsstaters samhällsviktiga verksamheter. Enligt direktivet ska alla leverantörer av digitala tjänster hanteras på samma sätt inom hela EU utifrån vad som är proportionerligt i förhållande till den risk som verksamheten kan utgöra. Medlemsstaterna är inte skyldiga att identifiera leverantörer av digitala tjänster men däremot att se till att även dessa aktörer vidtar tekniska och organisatoriska åtgärder för att hantera säkerhetsrisker mot nätverk och informationssystem och att de rapporterar allvarliga it-incidenter till tillsynsmyndigheten. Skyldigheten gäller enbart för den medlemsstat där en sådan aktör har sitt fasta etableringsställe eller en representant.

Det behöver mot denna bakgrund analyseras hur direktivets krav på identifiering av operatörer som bedriver samhällsviktig verksamhet och krav på aktörerna ska genomföras i svensk rätt. Analysen bör göras med utgångspunkten att det är verksamhetsutövaren som är ansvarig för att avgöra om denne omfattas av regelverket, vilket motsvarar vad som gäller enligt t.ex. säkerhetsskyddslagen (1996:627). I dag finns ett flertal regelverk som ställer krav på informationssäkerhet utifrån olika förutsättningar. I linje med regeringens ambition att verka för ett mer ändamålsenligt arbete med informationssäkerhet inom statsförvaltningen bör det utredas ifall direktivet, särskilt direktivets krav på operatörer som bedriver samhällsviktig verksamhet och leverantörer av digitala tjänster, bör genomföras i ett samlat regelverk om säkerhet för nätverk och informationssystem.

Direktivet tillåter medlemsstaterna att skydda information som gäller nationell säkerhet och information som kan påverka möjligheten att upprätthålla lag och ordning särskilt i fråga om brottsbekämpning. Det svenska systemet för obligatorisk it-incidentrapportering för statliga myndigheter har utformats på sådant sätt att it-incidenter i vissa särskilt säkerhetskänsliga system, inklusive incidenter som upptäckts genom stöd enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt, i stället för till MSB ska rapporteras enligt säkerhetsskyddsförordningen till Säkerhetspolisen eller Försvarsmakten. Myndigheterna på försvarsområdet och försvarsindustrin omfattas inte av direktivets krav och dessa aktörers rapportering av it-incidenter ska med hänsyn till rikets säkerhet inte omfattas av den nya ordning som föreslås. Även it-

incidenter hos andra aktörer som har upptäckts genom stöd enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt (FRA) bör kunna undantas från direktivets tillämpning om rapporteringen innebär risk för att sekretesskyddade uppgifter om FRA:s förmåga röjs. Det kan även finnas andra aktörer som visserligen omfattas av direktivets krav men som ändå bör undantas från reglerna för att skydda information som gäller nationell säkerhet. It-incidenter som skulle röja information som gäller nationell säkerhet kan dock även fortsättningsvis rapporteras enligt den ordning som från den 1 april 2016 gäller enligt säkerhetsskyddsförordningen.

Bestämmelser om informationssäkerhet i sektorsspecifika EU-rättsakter, som innehåller motsvarande eller mer långtgående krav, ska ha företräde framför de aktuella bestämmelserna i direktivet. Även detta bör beaktas i de överväganden som görs.

Enligt direktivet ska tillsynsmyndigheterna ha tillräckliga verktyg för att se till att regelverket efterlevs. I detta ligger ett sanktionssystem med effektiva och proportionerliga åtgärder. För svenskt vidkommande bör ett sådant system vara uppbyggt enligt den struktur som redan gäller i dag, dvs. att en tillsynsmyndighets beslut om sanktioner kan överklagas till allmän förvaltningsdomstol. Direktivet gör ingen åtskillnad mellan offentliga och enskilda aktörer. Frågan bör därför analyseras med utgångspunkt i att även offentliga aktörer, på lämpligt sätt, ska kunna åläggas sanktioner.

Utredaren ska, med beaktande av att direktivet inte hindrar medlemsstaterna från att skydda sina nationella säkerhetsintressen och de begränsningar som nämnts ovan,

- föreslå hur operatörer som bedriver samhällsviktig verksamhet i Sverige ska identifieras,
- föreslå hur direktivets krav på både operatörer som bedriver samhällsviktig verksamhet och leverantörer av digitala tjänster bör genomföras i svensk rätt, och
- analysera och föreslå vilka bestämmelser om sanktioner som Sverige behöver införa.

Direktivet hindrar inte medlemsstaterna från att anta mer långtgående bestämmelser om säkerhet i nätverk och informationssystem än vad direktivet kräver. Det innehåller även bestämmelser om frivillig rapportering av incidenter. Utredaren får lämna andra förslag

denne anser nödvändiga och som ligger inom ramen för EU-direktivet eller dessa direktiv.

Medför direktivet behov av förändringar i sekretesskyddet?

Operatörer som bedriver samhällsviktig verksamhet och leverantörer av digitala tjänster är enligt direktivet skyldiga att bl.a. anmäla it-incidenter. Som tidigare nämnts bör sådana it-incidenter rapporteras till MSB som får ansvar för Sveriges CSIRT-verksamhet och, i förekommande fall, till aktuell sektorsmyndighet. Därigenom kan aktörerna behöva lämna känslig information om bl.a. säkerhets- och bevakningsåtgärder till tillsynsmyndigheten. En skyldighet att anmäla it-incidenter införs den 1 april 2016 för statliga myndigheter genom en ny bestämmelse i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Den information som statliga myndigheter kommer att rapportera till MSB omfattas av sekretess enligt 18 kap. 8 § 3 offentlighets- och sekretesslagen (OSL) om uppgifterna lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser telekommunikation eller system för automatiserad behandling av information. Det bör analyseras om det finns behov av bestämmelser om sekretessbrytande uppgiftsskyldighet för att berörda myndigheter ska kunna uppfylla sin rapporteringsskyldighet till MSB.

Bestämmelsen i 18 kap. 8 § 3 OSL är utrustad med ett s.k. rakt skaderekvisit. Vid införandet förordade dock flera remissinstanser i stället ett omvänt skaderekvisit (prop. 2003/04:92 s. 78 f.). I samband med att betänkandet Informations- och cybersäkerhet i Sverige (SOU 2015:23) remitterades pekade flera remissinstanser på att sekretesskyddet för aktuella uppgifter behöver ses över. MSB framförde i det sammanhanget att det kan finnas anledning att överväga möjligheten att föreskriva om absolut sekretess för it-incidentrapporter. Det bör analyseras om det nuvarande sekretesskyddet är tillräckligt för att skydda de uppgifter som ska rapporteras till MSB och övriga tillsynsmyndigheter eller om det finns behov av ett starkare sekretesskydd. Uppgifter kan även vara känsliga med hänsyn till den rapporterande aktörens ekonomiska verksamhet. Det bör även ana-

lyseras om det befintliga sekretesskyddet för uppgifter om enskilds affärs- och driftsförhållanden är tillräckligt.

Direktivets bestämmelser om samarbete mellan medlemsstaterna kan innebära att information som helt eller delvis omfattas av sekretess behöver utlämnas till annan medlemsstat eller kommissionen. En förutsättning för ett sådant utlämnande är enligt 8 kap. 3 § OSL att utlämnande görs i enlighet med särskilda föreskrifter i lag eller förordning, eller att uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

Som nämnts ovan ges medlemsstaterna enligt direktivet möjlighet att skydda information som gäller nationell säkerhet eller som kan påverka möjligheten att upprätthålla lag och ordning särskilt i fråga om brottsbekämpning. Det innebär att Sverige behåller rätten att själv besluta om information som skyddas av sekretess enligt t.ex. 15 kap. 1 och 2 §§ OSL ska delas med andra medlemsstater eller om så inte ska ske. Motsvarande nationell beslutanderätt finns dock inte beträffande sådana uppgifter som endast omfattas av sekretess enligt 18 kap. 8 § 3 OSL. I dag finns ingen särskild föreskrift i lag eller förordning som medger utlämnande av information om it-incidenter till annan medlemsstat eller kommissionen. Det bör övervägas om det finns behov av sådana föreskrifter eller om sådana uppgiftsutbyten som följer av direktivet kan göras med stöd av 8 kap. 3 § första stycket 1 OSL, utan att information som rör rikets säkerhet lämnas ut.

En annan fråga som aktualiseras genom det aktuella direktivet är hur bestämmelserna i en svensk författning om säkerhet i nätverk och informationssystem kommer att förhålla sig till personuppgiftslagstiftningen. Enligt direktivet ska detta inte påverka tillämpningen av dataskyddsdirektivet 95/46/EG, vilket har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204). Inom kort förväntas EU besluta om en förordning som utgör en ny generell reglering för personuppgiftsbehandling inom EU. Förordningen kommer att ersätta det nuvarande dataskyddsdirektivet och innebär att bl.a. personuppgiftslagen måste upphävas. Det behöver därför också analyseras vilken personuppgiftsbehandling som direktivet

kan komma ge upphov till och om det medför behov av författningsändringar.

Utredaren ska därför

- ta ställning till om bestämmelserna i offentlighets- och sekretesslagen innebär ett tillräckligt skydd för sådana uppgifter som kan komma att rapporteras med anledning av en it-incident eller om nuvarande lagstiftning behöver ändras och vid sådant behov föreslå författningsändringar,
- undersöka om det behövs en uppgiftsskyldighet för att uppgifter som följer av direktivet ska kunna delas mellan de svenska aktörer som träffas av direktivet och MSB och vid behov föreslå författningsändringar,
- ta ställning till behovet av författningsändringar för att möjliggöra utbyte av andra uppgifter än sådana som rör rikets säkerhet med andra medlemsstater och kommissionen och vid behov föreslå sådana ändringar, och
- analysera vilken personuppgiftsbehandling som kan bli aktuell vid tillämpningen av direktivets bestämmelser och vid behov föreslå författningsändringar.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för enskilda och det allmänna samt konsekvenserna i övrigt av förslagen. 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 det kommunala självstyret ska därför, utöver dess konsekvenser, också de särskilda avvägningar som lett fram till förslagen särskilt redovisas.

Arbetets bedrivande och redovisning av uppdraget

Utredaren ska löpande hålla Regeringskansliet (Justitiedepartementet) informerat om arbetet.

Vid genomförandet av uppdraget ska utredaren hålla sig informerad om arbetet med betänkandena Informations- och cybersäkerhet i Sverige (SOU 2015:23) och En ny säkerhetsskyddslag (SOU 2015:25). Utredaren ska också hålla sig informerad om det arbete som bedrivs i Dricksvattenutredningen (L 2013:02) och av den utredare som biträder Justitiedepartementet med att utreda frågan om åtgärder för att öka Polismyndighetens tillgång till information om it-brottslighet.

Under genomförandet av uppdraget ska utredaren, i den utsträckning som bedöms lämplig, också ha en dialog med och inhämta upplysningar från de myndigheter och andra organisationer som berörs av aktuella frågor.

Uppdraget ska redovisas senast den 1 maj 2017.

(Justitiedepartementet)

I

(Lagstiftningsakter)

DIREKTIV

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

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 ekonomiska och sociala kommitténs yttrande ([1]),

i enlighet med det ordinarie lagstiftningsförfarandet ([2]), och

av följande skäl:

(1) Nätverks- och informationssystem och nätverks- och informationstjänster spelar en viktig roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och i synnerhet för den inre marknadens funktion.

(2) Säkerhetsincidenter, som blir allt mer omfattande och vanliga och får allt större inverkan, utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Dessa system kan också bli mål för avsiktligt sabotage i syfte att skada dem eller förorsaka driftsavbrott. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande ekonomiska förluster, undergräva användarnas förtroende och medföra allvarliga konsekvenser för unionens ekonomi.

(3) Nätverks- och informationssystem, i synnerhet internet, spelar en viktig roll genom att underlätta den gränsöverskridande rörligheten för varor, tjänster och personer. På grund av denna transnationella natur kan allvarliga störningar av dessa system, vare sig de är avsiktliga eller oavsiktliga och oberoende av var de förekommer, påverka enskilda medlemsstater och unionen som helhet. Säkerheten i nätverks- och informationssystem är därför avgörande för att den inre marknaden ska fungera väl.

(4) På grundval av de betydande framstegen inom det europeiska forumet för medlemsstaterna vad gäller att främja diskussioner och utbyten av bästa praxis, inbegripet utarbetandet av principer för ett europeiskt samarbete vid it-relaterade kriser, bör en samarbetsgrupp inrättas, bestående av företrädare för medlemsstaterna, kommissionen och Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), som ska stödja och underlätta strategiskt

([1]) EUT C 271, 19.9.2013, s. 133.
([2]) Europaparlamentets ståndpunkt av den 13 mars 2014 (ännu ej offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 17 maj 2016 (ännu ej offentliggjord i EUT). Europaparlamentets ståndpunkt av den 6 juli 2016 (ännu ej offentliggjord i EUT).

samarbete mellan medlemsstaterna vad gäller säkerhet i nätverks- och informationssystem. För att denna grupp ska vara effektiv och inkluderande är det viktigt att alla medlemsstater har en minimikapacitet och en strategi som säkerställer en hög nivå på säkerheten i nätverks- och informationssystem på det egna territoriet. Dessutom bör säkerhets- och rapporteringskrav gälla för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, för att främja en riskhanteringskultur och säkerställa att de allvarligaste incidenterna rapporteras.

(5) Den befintliga kapaciteten räcker inte för att säkerställa en hög nivå på säkerheten i nätverks- och informationssystem i unionen. Medlemsstaterna har mycket olika beredskapsnivåer, vilket har lett till skilda tillvägagångssätt i unionen. Resultatet blir olika skyddsnivåer för konsumenter och företag, vilket undergräver den allmänna nivån på säkerheten i nätverks- och informationssystem i unionen. Avsaknaden av gemensamma krav för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster gör det i sin tur omöjligt att inrätta en övergripande och effektiv mekanism för samarbete på unionsnivå. Universitet och forskningscentrum har en avgörande roll att spela när det gäller att främja forskning, utveckling och innovation på dessa områden.

(6) Effektiva åtgärder för att lösa problemen vad gäller säkerhet i nätverks- och informationssystem förutsätter därför ett övergripande angreppssätt på unionsnivå, som omfattar en gemensam miniminivå för kapacitetsuppbyggnad och planering, utbyte av information, samarbete och gemensamma säkerhetskrav för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. Leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster är emellertid inte förhindrade att genomföra striktare säkerhetsåtgärder än de som föreskrivs i detta direktiv.

(7) Detta direktiv bör tillämpas på både leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, så att alla relevanta incidenter och risker täcks. De skyldigheter som införs för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster bör dock inte tillämpas på företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster i den mening som avses i Europaparlamentets och rådets direktiv 2002/21/EG ([1]), vilka omfattas av de specifika krav på säkerhet och integritet som föreskrivs i det direktivet, och inte heller på leverantörer av betrodda tjänster i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 910/2014 ([2]), vilka omfattas av de säkerhetskrav som föreskrivs i den förordningen.

(8) Detta direktiv bör inte påverka varje enskild medlemsstats möjlighet att vidta de åtgärder som är nödvändiga för att skydda dess väsentliga säkerhetsintressen, för att upprätthålla allmän ordning och säkerhet och för att möjliggöra utredning, upptäckt och lagföring av brott. Enligt artikel 346 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) ska ingen medlemsstat vara förpliktad att lämna information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen. Rådets beslut 2013/488/EU ([3]) och sekretessavtal, eller informella sekretessavtal såsom *Traffic Light Protocol*, är relevanta i detta sammanhang.

(9) Vissa ekonomiska sektorer regleras redan eller kan komma att regleras av sektorsspecifika unionsrättsakter som inbegriper regler med anknytning till säkerheten i nätverks- och informationssystem. När dessa unionsrättsakter innehåller bestämmelser med krav på säkerhet i nätverks- och informationssystem eller rapportering av incidenter, bör de bestämmelserna tillämpas, om de innehåller krav vilkas verkan minst motsvarar verkan av skyldigheterna i detta direktiv. Medlemsstaterna bör då tillämpa bestämmelserna i sådana sektorsspecifika unionsrättsakter, inklusive sådana som rör jurisdiktion, och bör inte genomföra identifieringsförfarandet för leverantörer av samhällsviktiga tjänster enligt definitionen i detta direktiv. Medlemsstaterna bör i detta sammanhang informera kommissionen om tillämpningen av sådana *lex specialis*-bestämmelser. Vid fastställandet av huruvida kraven på säkerhet i nätverks- och informationssystem och rapportering av incidenter som ingår i sektorsspecifika unionsrättsakter motsvarar kraven i detta direktiv, bör endast bestämmelserna i relevanta unionsrättsakter och deras tillämpning i medlemsstaterna beaktas.

(10) I sjöfartssektorn omfattar säkerhetskraven för rederier, fartyg, hamnanläggningar, hamnar och sjötrafikinformationstjänster enligt unionsrättsakter all verksamhet, inbegripet radio- och telekommunikationssystem, datorsystem och nätverk. De obligatoriska förfarandena inbegriper rapportering av alla incidenter och bör därför anses utgöra *lex specialis*, i den mån dessa krav är åtminstone likvärdiga med motsvarande bestämmelser i detta direktiv.

([1]) Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv) (EGT L 108, 24.4.2002, s. 33).

([2]) 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).

([3]) Rådets beslut 2013/488/EU av den 23 september 2013 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 274, 15.10.2013, s. 1).

(11) När medlemsstaterna identifierar operatörer i sjöfartssektorn, bör de ta hänsyn till befintliga och framtida internationella koder och riktlinjer som utvecklats särskilt av Internationella sjöfartsorganisationen, i syfte att skapa ett enhetligt tillvägagångssätt för enskilda sjöfartsoperatörer.

(12) Regleringen och tillsynen inom banksektorn och sektorn för finansmarknadsinfrastrukturer har i hög grad harmoniserats på unionsnivå, genom användning av unionens primärrätt och sekundärrätt och standarder som utvecklats tillsammans med de europeiska tillsynsmyndigheterna. Inom bankunionen säkerställs tillämpningen och tillsynen av dessa krav genom den gemensamma tillsynsmekanismen. För medlemsstater som inte ingår i bankunionen säkerställs detta av medlemsstaternas relevanta banktillsynsmyndigheter. Inom tillsynspraxis på andra områden inom regleringen av finanssektorn säkerställer Europeiska systemet för finansiell tillsyn också en hög grad av enhetlighet och konvergens. Även Europeiska värdepappers- och marknadsmyndigheten utövar direkt tillsyn över vissa enheter, nämligen kreditvärderingsinstitut och transaktionsregister.

(13) Operativ risk utgör en viktig del av reglering och tillsyn inom banksektorn och sektorn för finansmarknadsinfrastrukturer. Den omfattar all verksamhet, inbegripet nätverks- och informationssystems säkerhet, integritet och motståndskraft. Kraven på dessa system, som ofta är mer långtgående än de som föreskrivs i detta direktiv, fastställs i ett antal unionsrättsakter, som inbegriper bestämmelser om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag och bestämmelser om tillsynskrav för kreditinstitut och värdepappersföretag, vilka inbegriper krav avseende operativ risk, bestämmelser om marknader för finansiella instrument, vilka inbegriper krav avseende riskbedömning för värdepappersföretag och för reglerade marknader, bestämmelser om OTC-derivat, centrala motparter och transaktionsregister, vilka inbegriper krav avseende operativ risk för centrala motparter och transaktionsregister, och bestämmelser om förbättrad värdepappersavveckling i unionen och om värdepapperscentraler, vilka inbegriper krav avseende operativ risk. Dessutom utgör krav på rapportering av incidenter en del av normal tillsynspraxis inom finanssektorn och ingår ofta i tillsynshandböcker. Medlemsstaterna bör beakta dessa bestämmelser och krav vid tillämpningen av *lex specialis*.

(14) Såsom Europeiska centralbanken konstaterade i sitt yttrande av den 25 juli 2014 ([1]) påverkar detta direktiv inte den ordning för Eurosystemets tillsyn över betalnings- och avvecklingssystem som fastställs i unionsrätten. Det skulle vara lämpligt att de myndigheter som ansvarar för denna övervakning utbytte erfarenheter om frågor som rör säkerhet i nätverks- och informationssystem med de behöriga myndigheterna enligt detta direktiv. Detsamma gäller för medlemmar i Europeiska centralbankssystemet som står utanför euroområdet och som utövar sådan tillsyn över betalnings- och avvecklingssystem på grundval av nationella lagar och andra författningar.

(15) En internetbaserad marknadsplats ger konsumenter och näringsidkare möjlighet att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare och är slutdestinationen för ingåendet av sådana avtal. Den bör inte omfatta onlinetjänster som endast fungerar som mellanhand för tredjepartstjänster genom vilka ett avtal slutligen kan ingås. Den bör därför inte omfatta onlinetjänster som jämför priset på vissa varor eller tjänster från olika näringsidkare och sedan leder användaren vidare till den näringsidkare som valts för köp av varan. Datatjänster som tillhandahålls av den internetbaserade marknadsplatsen kan inbegripa behandling av transaktioner, sammanställning av data eller profilering av användare. Applikationsbutiker, som fungerar som onlinebutiker och möjliggör digital distribution av applikationer eller programvara från tredje part, ska betraktas som en typ av internetbaserad marknadsplats.

(16) En internetbaserad sökmotor gör det möjligt för användaren att göra sökningar på i princip alla webbplatser på grundval av en sökning inom vilket ämnesområde som helst. Den kan också vara inriktad på webbplatser på ett visst språk. Definitionen av internetbaserad sökmotor enligt detta direktiv bör inte omfatta sökfunktioner som begränsas till innehållet på en särskild webbplats, oberoende av om sökfunktionen tillhandahålls av en extern sökmotor. Den bör inte heller omfatta onlinetjänster som jämför priset på vissa varor eller tjänster från olika näringsidkare och sedan leder användaren vidare till den näringsidkare som valts för köp av varan.

(17) Molntjänster omfattar många olika verksamheter, som kan levereras enligt olika modeller. Vid tillämpningen av detta direktiv omfattar termen *molntjänster* tjänster som medger åtkomst till en skalbar och elastisk pool av delbara dataresurser. Sådana dataresurser omfattar resurser såsom nätverk, servrar eller annan infrastruktur, lagring, applikationer och tjänster. Termen *skalbar* avser dataresurser 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 dataresurser som avsätts och utnyttjas beroende på efterfrågan för att

([1]) EUT C 352, 7.10.2014, s. 4.

tillgängliga resurser snabbt ska kunna utökas och minskas i takt med arbetsbördan. Termen *delbar* används för att beskriva dataresurser 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.

(18) En internetknutpunkts (IXP) uppgift är att koppla samman nätverk. En IXP tillhandahåller inte tillträde till nätverk och fungerar inte som transitleverantör eller transitförmedlare. En IXP tillhandahåller inte heller andra tjänster utan samband med sammankoppling, även om detta inte hindrar en IXP-leverantör från att tillhandahålla andra tjänster. En IXP är till för att sammankoppla nätverk som är tekniskt och organisatoriskt separata. Termen *autonomt system* används för att beskriva ett tekniskt fristående nätverk.

(19) Medlemsstaterna bör ansvara för att fastställa vilka enheter som uppfyller kriterierna för definitionen av leverantör av samhällsviktiga tjänster. I syfte att säkerställa ett enhetligt tillvägagångssätt bör definitionen av leverantör av samhällsviktiga tjänster tillämpas konsekvent i alla medlemsstater. I detta syfte föreskriver detta direktiv en bedömning av de enheter som är verksamma i specifika sektorer och delsektorer, upprättandet av en förteckning över samhällsviktiga tjänster, beaktandet av en gemensam förteckning över sektorsöverskridande faktorer för fastställande av om en eventuell incident skulle medföra en betydande störning, en samrådsprocess med de berörda medlemsstaterna i de fall där enheter tillhandahåller tjänster i mer än en medlemsstat, och samarbetsgruppens stöd vid identifieringsförfarandet. I syfte att säkerställa att eventuella förändringar på marknaden återspeglas på ett korrekt sätt bör förteckningen över identifierade leverantörer regelbundet ses över av medlemsstaterna och vid behov uppdateras. Medlemsstaterna bör slutligen till kommissionen överlämna den information som är nödvändig för att bedöma i vilken utsträckning denna gemensamma metod har gjort det möjligt för medlemsstaterna att tillämpa definitionen konsekvent.

(20) Vid förfarandet för identifiering av leverantörer av samhällsviktiga tjänster bör medlemsstaterna, åtminstone för varje delsektor som avses i detta direktiv, bedöma vilka tjänster som måste betraktas som viktiga för att upprätthålla kritisk samhällelig och ekonomisk verksamhet samt huruvida de enheter som är förtecknade i de sektorer och delsektorer som avses i detta direktiv och tillhandahåller dessa tjänster uppfyller kriterierna för identifiering av leverantörer. Vid bedömning av huruvida en enhet tillhandahåller en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, är det tillräckligt att undersöka om enheten tillhandahåller en tjänst som finns upptagen i förteckningen över samhällsviktiga tjänster. Det bör dessutom påvisas att tillhandahållandet av den samhällsviktiga tjänsten är beroende av nätverks- och informationssystem. Slutligen bör medlemsstaterna, vid bedömning av huruvida en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten, beakta ett antal sektorsöverskridande faktorer samt, i lämpliga fall, sektorsspecifika faktorer.

(21) Vid identifiering av leverantörer av samhällsviktiga tjänster krävs det att leverantören utför en faktisk och reell verksamhet med hjälp av en stabil struktur för att den ska anses vara etablerad i en medlemsstat. Den rättsliga formen för en sådan struktur bör här, oavsett om det är en filial eller ett dotterbolag med juridisk personlighet, inte vara den avgörande faktorn.

(22) Det är möjligt att enheter verksamma inom de sektorer och delsektorer som avses i detta direktiv tillhandahåller både samhällsviktiga och icke samhällsviktiga tjänster. Inom luftfartssektorn tillhandahåller t.ex. flygplatser tjänster som en medlemsstat kan anse vara samhällsviktiga, såsom skötseln av start- och landningsbanorna, men också ett antal tjänster som kan betraktas som icke samhällsviktiga, såsom tillhandahållande av butiksområden. Leverantörer av samhällsviktiga tjänster bör omfattas av de specifika säkerhetskraven endast när det gäller tjänster som anses vara samhällsviktiga. I syfte att identifiera leverantörer bör medlemsstaterna därför upprätta en förteckning över de tjänster som betraktas som samhällsviktiga.

(23) Förteckningen över tjänster bör omfatta alla de tjänster som tillhandahålls på en viss medlemsstats territorium och som uppfyller kraven enligt detta direktiv. Medlemsstaterna bör kunna lägga till nya tjänster i den befintliga förteckningen. Förteckningen över tjänster bör fungera som referenspunkt för medlemsstaterna och möjliggöra identifiering av leverantörer av samhällsviktiga tjänster. Syftet med förteckningen är att identifiera de typer av samhällsviktiga tjänster inom en viss sektor som det hänvisas till i detta direktiv och därmed skilja dem från de icke samhällsviktiga tjänster som en enhet med verksamhet inom en viss sektor kan ansvara för. Den förteckning över tjänster som varje medlemsstat upprättar skulle utgöra ett ytterligare bidrag till bedömningen av lagstiftningspraxis inom varje medlemsstat med syftet att säkerställa en övergripande enhetlighet mellan medlemsstaternas identifieringsförfaranden.

(24) Om en enhet tillhandahåller en samhällsviktig tjänst i två eller flera medlemsstater, bör dessa medlemsstater vid identifieringsförfarandet föra bilaterala eller multilaterala diskussioner med varandra. Denna samrådsprocess är avsedd att hjälpa dem att bedöma om leverantören i fråga är av kritisk betydelse när det gäller gränsöverskridande inverkan, varigenom varje berörd medlemsstat ges möjlighet att lägga fram sina synpunkter avseende riskerna med de tjänster som tillhandahålls. I denna process bör de berörda medlemsstaterna beakta varandras synpunkter, och bör i detta avseende kunna begära bistånd från samarbetsgruppen.

(25) Till följd av identifieringsförfarandet bör medlemsstaterna vidta nationella åtgärder för att fastställa vilka enheter som omfattas av skyldigheter när det gäller säkerhet i nätverks- och informationssystem. Detta skulle kunna uppnås genom upprättande av en förteckning över alla leverantörer av samhällsviktiga tjänster eller genom antagande av nationella bestämmelser, inbegripet objektivt mätbara kriterier, såsom leverantörens produktion eller antalet användare, som gör det möjligt att fastställa vilka enheter som omfattas av skyldigheter när det gäller säkerhet i nätverks- och informationssystem. De nationella åtgärderna, oavsett om de redan har vidtagits eller om de vidtas mot bakgrund av detta direktiv, bör omfatta alla rättsliga åtgärder, administrativa åtgärder och strategier som möjliggör identifiering av leverantörer av samhällsviktiga tjänster enligt detta direktiv.

(26) För att ge en indikation om betydelsen i förhållande till den berörda sektorn av de identifierade leverantörerna av samhällsviktiga tjänster, bör medlemsstaterna beakta dessa leverantörers antal och storlek, till exempel i form av marknadsandelar eller den mängd som produceras eller levereras, utan att vara förpliktade att lämna ut uppgifter som skulle avslöja vilka leverantörer som har identifierats.

(27) För att fastställa om en incident skulle medföra en betydande störning vid tillhandahållandet av en samhällsviktig tjänst, bör medlemsstaterna beakta ett antal olika faktorer, såsom antalet användare som är beroende av tjänsten för privata eller yrkesmässiga ändamål. Användningen av tjänsten kan vara direkt, indirekt eller ske genom förmedling. Vid bedömningen av en incidents eventuella inverkan på ekonomisk och samhällelig verksamhet eller allmän säkerhet, uttryckt i grad och varaktighet, bör medlemsstaterna också bedöma hur länge det sannolikt skulle ta tills avbrottet skulle börja ha en negativ inverkan.

(28) Utöver de sektorsöverskridande faktorerna bör också sektorsspecifika faktorer beaktas vid fastställelsen av huruvida en incident skulle medföra en betydande störning vid tillhandahållandet av en samhällsviktig tjänst. När det gäller energileverantörer kan sådana faktorer omfatta mängden eller andelen producerad nationell el, för oljeleverantörer mängden olja per dag, för lufttransport, inbegripet flygplatser och lufttrafikföretag, järnvägstransport och kusthamnar andelen nationell trafikmängd och antalet passagerare eller lastningar per år, för bankverksamhet eller finansmarknadsinfrastrukturer deras betydelse för systemet på grundval av samlade tillgångar eller förhållandet mellan dessa tillgångar och BNP, för hälso- och sjukvårdssektorn antalet patienter som leverantören vårdar per år, för produktion, bearbetning och leverans av vatten, volym, antal och typer av användare, inbegripet t.ex. sjukhus, offentlig sektor, organisationer och personer) samt förekomsten av alternativa vattenkällor för samma geografiska område.

(29) För att uppnå och bibehålla en hög nivå på säkerheten i nätverks- och informationssystem bör alla medlemsstater ha en nationell strategi för säkerhet i nätverks- och informationssystem genom vilken fastställs de strategiska mål och konkreta politiska åtgärder som ska genomföras.

(30) Mot bakgrund av skillnaderna i nationella förvaltningsstrukturer och för att skydda befintliga sektorsspecifika arrangemang eller unionens tillsyns- och regleringsmyndigheter och undvika överlappning, bör medlemsstaterna kunna utse mer än en nationell behörig myndighet med ansvar för att utföra uppgifter som rör säkerheten i de nätverks- och informationssystem som används av leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster enligt detta direktiv.

(31) För att underlätta gränsöverskridande samarbete och kommunikation och för att göra det möjligt att genomföra detta direktiv på ett effektivt sätt måste varje medlemsstat, utan att det påverkar sektorsspecifika regleringsarrangemang, utse en nationell gemensam kontaktpunkt med ansvar för samordningen av frågor angående säkerhet i nätverks- och informationssystem och gränsöverskridande samarbete på unionsnivå. Behöriga myndigheter och gemensamma kontaktpunkter bör förses med de tekniska och finansiella resurser och personalresurser som de behöver för att på ett effektivt sätt kunna utföra de uppgifter som de tilldelas och därmed uppnå målen med detta direktiv. Eftersom syftet med detta direktiv är att förbättra den inre marknadens funktion genom att skapa tillit och förtroende, måste medlemsstaternas organ kunna samarbeta effektivt med ekonomiska aktörer och ha en struktur som är förenlig med detta.

(32) Behöriga myndigheter eller enheter för hantering av it-säkerhetsincidenter (*Computer Security Incident Response Teams*, nedan kallade *CSIRT-enheter*) bör ta emot rapporter om incidenter. De gemensamma kontaktpunkterna bör inte direkt ta emot några rapporter om incidenter, såvida de inte också fungerar som behörig myndighet eller som en CSIRT-enhet. En behörig myndighet eller en CSIRT-enhet bör dock kunna ge den gemensamma kontaktpunkten i uppgift att vidarebefordra incidentrapporter till de gemensamma kontaktpunkterna i andra berörda medlemsstater.

(33) För att säkerställa att medlemsstaterna och kommissionen får information på ett ändamålsenligt sätt bör den gemensamma kontaktpunkten lämna en sammanfattande rapport till samarbetsgruppen som bör vara anonymiserad för att bevara rapporternas konfidentialitet och identiteten på leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, eftersom information om de rapporterande enheternas identitet inte krävs för utbyte av bästa praxis inom samarbetsgruppen. Den sammanfattande rapporten bör innehålla uppgifter om antalet mottagna incidentrapporter samt information om de rapporterade incidenternas art, såsom vilka typer av säkerhetsöverträdelser det rör sig om eller hur allvarliga eller långvariga de varit.

(34) Medlemsstaterna bör ha både den tekniska och organisatoriska kapacitet som krävs för att förebygga, upptäcka, vidta åtgärder mot och begränsa effekterna av incidenter och risker vad gäller nätverks- och informationssystem. Medlemsstater bör därför säkerställa att de har väl fungerande CSIRT-enheter, även kallade *incidenthanteringsorganisationer* (*Computer Emergency Response Teams*, Cert), som uppfyller grundläggande krav för att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå. För att alla typer av leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster ska kunna dra nytta av sådan kapacitet och sådant samarbete bör medlemsstaterna säkerställa att alla typer omfattas av en utsedd CSIRT-enhet. 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.

(35) Eftersom de flesta nätverks- och informationssystem drivs privat, är det mycket viktigt med samarbete mellan offentlig och privat sektor. Leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster bör uppmuntras att upprätta egna informella samarbetsmekanismer för att säkerställa säkerheten i nätverks- och informationssystem. Samarbetsgruppen bör vid behov kunna bjuda in berörda parter till diskussionerna. För att effektivt uppmuntra utbyte av information och bästa praxis är det mycket viktigt att säkerställa att samarbetet inte leder till nackdelar för de leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster som deltar i sådana utbyten.

(36) Enisa bör bistå medlemsstaterna och kommissionen genom att tillhandahålla expertis och rådgivning och underlätta utbytet av bästa praxis. Kommissionen bör samråda med Enisa vid tillämpningen av detta direktiv, och medlemsstaterna bör ha möjlighet att göra detta. För att bygga upp kapacitet och kunskap bland medlemsstaterna bör samarbetsgruppen också fungera som ett instrument för utbyte av bästa praxis, diskussioner om medlemsstaternas kapacitet och beredskap och, på frivillig grund, bistå medlemmarna vid utvärdering av nationella strategier för säkerhet i nätverks- och informationssystem, vid kapacitetsuppbyggnad och utvärderingar av övningar som avser säkerheten i nätverks- och informationssystem.

(37) Medlemsstaterna bör vid behov kunna använda eller anpassa befintliga organisationsstrukturer eller strategier vid tillämpningen av detta direktiv.

(38) Samarbetsgruppens och Enisas respektive uppgifter är beroende av och kompletterar varandra. Enisa bör generellt bistå samarbetsgruppen i utförandet av dess uppgifter i enlighet med Enisas mål enligt Europaparlamentets och rådets förordning (EU) nr 526/2013 [1], nämligen att bistå unionens institutioner, organ och byråer samt medlemsstaterna med att genomföra de strategier som krävs för att uppfylla rättsliga och regleringsmässiga krav på säkerhet i nätverks- och informationssystem i befintliga och framtida unionsrättsakter. Enisa bör särskilt tillhandahålla bistånd på de områden som motsvarar dess egna uppgifter enligt förordning (EU) nr 526/2013, nämligen att analysera strategier för säkerhet i nätverks- och informationssystem, stödja anordnandet och genomförandet av övningar på unionsnivå som avser säkerhet i nätverks- och informationssystem samt utbyta information och bästa praxis vad gäller åtgärder för ökad medvetenhet och utbildning. Enisa bör också delta i utarbetandet av riktlinjer för sektorsspecifika kriterier för fastställande av hur betydande en incidents inverkan är.

[1] Europaparlamentets och rådets förordning (EU) nr 526/2013 av den 21 maj 2013 om Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och om upphävande av förordning (EG) nr 460/2004 (EUT L 165, 18.6.2013, s. 41).

(39) I syfte att främja avancerad säkerhet i nätverks- och informationssystem bör samarbetsgruppen vid behov samarbeta med berörda unionsinstitutioner, -organ, och -byråer för att utbyta sakkunskap och bästa praxis samt ge råd om säkerhetsaspekter på nätverks- och informationssystem som kan påverka deras arbete, samtidigt som befintliga arrangemang för utbyte av konfidentiell information respekteras. Vid samarbete med rättsvårdande myndigheter om säkerhetsaspekter på nätverks- och informationssystem som kan påverka deras arbete bör samarbetsgruppen respektera befintliga informationskanaler och etablerade nätverk.

(40) Information om incidenter blir allt mer värdefull för allmänheten och företag, särskilt små och medelstora företag. I vissa fall tillhandahålls sådan information redan via webbplatser på nationell nivå, på ett specifikt lands språk, och är främst inriktad på incidenter och händelser med en nationell dimension. Eftersom företag i allt större utsträckning bedriver gränsöverskridande verksamhet och medborgare använder onlinetjänster, bör information om incidenter tillhandahållas i samlad form på unionsnivå. CSIRT-nätverkets sekretariat uppmuntras att upprätta en webbplats eller upplåta utrymme åt en särskild sida på en befintlig webbplats, där allmän information om allvarliga incidenter i unionen görs tillgänglig för allmänheten. Informationen ska vara särskilt inriktad på företags intressen och behov. CSIRT-enheter som deltar i CSIRT-nätverket uppmanas att på frivillig grund tillhandahålla den information som ska offentliggöras på denna webbplats, utan att därvid inkludera konfidentiell eller känslig information.

(41) I fall då information anses vara konfidentiell enligt unionsbestämmelser och nationella bestämmelser om affärshemligheter, bör konfidentiell behandling säkerställas vid genomförande av verksamhet och uppfyllande av mål enligt detta direktiv.

(42) Övningar där incidentscenarier simuleras i realtid är viktiga för att testa medlemsstaternas beredskap och samarbete när det gäller säkerhet i nätverks- och informationssystem. Övningsserien CyberEurope, som samordnas av Enisa med deltagande av medlemsstaterna är ett användbart verktyg för att testa och utarbeta rekommendationer för hur incidenthanteringen på unionsnivå bör förbättras med tiden. Med tanke på att medlemsstaterna för närvarande inte har någon skyldighet att vare sig planera eller delta i övningar, bör inrättandet av CSIRT-nätverket enligt detta direktiv göra det möjligt för medlemsstaterna att delta i övningar på grundval av noggrann planering och strategiska val. Den samarbetsgrupp som inrättas enligt detta direktiv bör diskutera de strategiska besluten om övningar, särskilt men inte enbart när det gäller övningarnas regelbundenhet och utformningen av scenarierna. Enisa bör i enlighet med sitt mandat stödja anordnandet och genomförandet av unionsomfattande övningar genom att tillhandahålla expertis och rådgivning till samarbetsgruppen och CSIRT-nätverket.

(43) I och med att säkerhetsproblem som påverkar nätverks- och informationssystem är globala till sin natur behövs ett närmare internationellt samarbete för att förbättra säkerhetsstandarder och informationsutbyte och för att främja ett gemensamt sätt att hantera säkerhetsfrågor.

(44) Ansvaret för att säkerställa säkerheten i nätverks- och informationssystemen vilar i hög grad på leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. En riskhanteringskultur, som inbegriper riskbedömning och genomförande av säkerhetsåtgärder som är anpassade till riskerna, bör främjas och utvecklas genom ändamålsenliga krav i lagstiftning och frivillig branschpraxis. Att skapa trovärdiga och lika konkurrensvillkor är också avgörande för att samarbetsgruppen och CSIRT-nätverket ska fungera effektivt och för att säkerställa ett effektivt samarbete från alla medlemsstater.

(45) Detta direktiv är tillämpligt endast på offentliga förvaltningar vilka identifieras som leverantörer av samhällsviktiga tjänster. Det är därför medlemsstaternas ansvar att säkerställa säkerheten i nätverks- och informationssystem som används av offentliga förvaltningar som inte omfattas av detta direktiv.

(46) Åtgärder för riskhantering omfattar åtgärder för att identifiera alla incidentrisker, för att förebygga, upptäcka och hantera incidenter och för att begränsa deras inverkan. Säkerheten i nätverks- och informationssystem omfattar lagrade, överförda och behandlade uppgifters säkerhet.

(47) Behöriga myndigheter bör behålla rätten att anta nationella riktlinjer angående de omständigheter under vilka leverantörer av samhällsviktiga tjänster är skyldiga att rapportera incidenter.

(48) Många företag i unionen är beroende av leverantörer av digitala tjänster för att tillhandahålla sina tjänster. Eftersom vissa digitala tjänster skulle kunna utgöra en viktig resurs för sina användare, inklusive leverantörer av samhällsviktiga tjänster, och dessa användare inte alltid har alternativ tillgängliga, bör detta direktiv också gälla för leverantörer av sådana tjänster. För många företag är säkerheten, kontinuiteten och tillförlitligheten hos den typ av digitala tjänster som avses i detta direktiv av avgörande betydelse för att företaget ska fungera väl. En störning i en sådan digital tjänst kan hindra tillhandahållandet av andra tjänster som är beroende av den och därmed påverka viktig ekonomisk och samhällelig verksamhet i unionen. Sådana digitala tjänster skulle därför kunna vara av avgörande betydelse för att företag som är beroende av dem ska fungera väl och för dessa företags deltagande i den inre marknaden och den gränsöverskridande handeln inom unionen. Leverantörer av digitala tjänster som omfattas av detta direktiv är sådana som anses erbjuda digitala tjänster som många företag i unionen i allt högre grad är beroende av.

(49) Leverantörer av digitala tjänster bör säkerställa en säkerhetsnivå som är anpassad till graden av risk för de digitala tjänster som de tillhandahåller, med beaktande av den betydelse som deras tjänster har för verksamhet som bedrivs av andra företag inom unionen. Graden av risk för leverantörer av samhällsviktiga tjänster, som ofta är viktiga för att upprätthålla kritisk samhällelig och ekonomisk verksamhet, är i praktiken högre än för leverantörer av digitala tjänster. Säkerhetskraven för leverantörer av digitala tjänster bör därför vara lindrigare. Leverantörer av digitala tjänster bör fritt kunna vidta de åtgärder som de anser lämpliga för att hantera risker för säkerheten i deras nätverks- och informationssystem. Leverantörer av digitala tjänster bör, på grund av den gränsöverskridande arten, omfattas av ett mer harmoniserat tillvägagångssätt på unionsnivå. Genomförandeakter bör underlätta fastställandet och genomförandet av sådana åtgärder.

(50) Trots att hårdvarutillverkare och mjukvaruutvecklare varken är leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster, ökar deras produkter säkerheten i nätverks- och informationssystem. De spelar därför en viktig roll när det gäller att göra det möjligt för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster att skydda sina nätverks- och informationssystem. Sådana hårdvaru- och mjukvaruprodukter omfattas redan av befintliga bestämmelser om produktansvar.

(51) De tekniska och organisatoriska åtgärder som leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster åläggs bör inte innebära krav på att någon särskild kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt.

(52) Leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster bör säkerställa säkerheten i de nätverks- och informationssystem som de använder. Det rör sig framför allt om privata nätverks- och informationssystem som antingen förvaltas av deras interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Säkerhets- och rapporteringskraven bör gälla för relevanta leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, oavsett om de sköter underhållet av sina nätverks- och informationssystem internt eller lägger ut uppgifterna på entreprenad.

(53) För att undvika oproportionella finansiella och administrativa bördor för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster bör kraven stå i proportion till den risk som det berörda nätverks- och informationssystemet utgör, med beaktande av den senaste tekniska utvecklingen. När det gäller leverantörer av digitala tjänster, bör dessa krav inte gälla för mikroföretag och små företag.

(54) När offentliga förvaltningar i medlemsstaterna använder tjänster som erbjuds av leverantörer av digitala tjänster, särskilt molntjänster, är det möjligt att de från leverantörerna av dessa tjänster vill kräva ytterligare säkerhetsåtgärder utöver dem som leverantörer av digitala tjänster vanligtvis skulle erbjuda i överensstämmelse med kraven i detta direktiv. De bör kunna göra detta genom avtalsförpliktelser.

(55) Definitionerna av internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster i detta direktiv är specifika för det här direktivet och påverkar inte andra instrument.

(56) Detta direktiv bör inte hindra medlemsstaterna från att anta nationella åtgärder som innebär krav på offentliga organ att säkerställa särskilda säkerhetskrav när de sluter avtal om molntjänster. Alla sådana nationella åtgärder bör tillämpas på det berörda offentliga organet och inte på leverantören av molntjänster.

(57) Med tanke på de avgörande skillnaderna mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, särskilt de förstnämndas direkta koppling till fysisk infrastruktur och de senares gränsöverskridande art, bör harmoniseringsnivån för dessa två grupper av enheter i detta direktiv differentieras. Medlemsstaterna bör kunna identifiera de relevanta leverantörerna av samhällsviktiga tjänster och införa strängare krav än de som fastställs i detta direktiv. Medlemsstaterna bör inte identifiera leverantörer av digitala tjänster, eftersom detta direktiv bör gälla för alla leverantörer av digitala tjänster som omfattas av dess tillämpningsområde. Dessutom bör detta direktiv och de genomförandeakter som antas enligt detsamma säkerställa en hög harmoniseringsnivå för leverantörer av digitala tjänster med avseende på säkerhets- och rapporteringskrav. Detta bör möjliggöra en enhetlig behandling av leverantörer av digitala tjänster i hela unionen, på ett sätt som står i proportion till leverantörernas art och den grad av risk de kan utsättas för.

(58) Utan att det påverkar medlemsstaternas skyldigheter enligt unionsrätten bör detta direktiv inte hindra medlemsstaterna från att införa säkerhets- och rapporteringskrav för enheter som inte är leverantörer av digitala tjänster inom ramen för detta direktivs tillämpningsområde.

(59) Behöriga myndigheter bör säkerställa att de upprätthåller informella och tillförlitliga kanaler för informationsutbyte. Vid offentliggörande av incidenter som rapporteras till de behöriga myndigheterna bör allmänhetens intresse av att få information om hot vägas mot eventuell renomméskada och kommersiell skada för de leverantörer av samhällsviktiga tjänster och de leverantörer av digitala tjänster som rapporterar incidenter. Vid genomförandet av rapporteringsskyldigheterna bör behöriga myndigheter och CSIRT-enheterna särskilt ta hänsyn till behovet av att hålla uppgifter om produkters sårbara aspekter strikt konfidentiella till dess att lämpliga säkerhetslösningar släpps.

(60) Leverantörer av digitala tjänster bör omfattas av mindre ingripande, reaktiv efterhandstillsyn som är anpassad till deras tjänsters och verksamheters art. Den berörda behöriga myndigheten bör därför endast vidta åtgärder när den har mottagit bevis – till exempel från leverantören av digitala tjänster själv, från en annan behörig myndighet, inbegripet en behörig myndighet i en annan medlemsstat, eller från en tjänsteanvändare – för att en leverantör av digitala tjänster inte uppfyller kraven i detta direktiv, särskilt efter en incident. Den behöriga myndigheten bör därför inte ha någon allmän skyldighet att utöva tillsyn av leverantörer av digitala tjänster.

(61) Behöriga myndigheter bör ha de medel som de behöver för att kunna fullgöra sina förpliktelser, inbegripet befogenhet att inhämta tillräckligt med information för att bedöma nivån på säkerheten i nätverks- och informationssystem.

(62) Incidenter kan vara en följd av brottslig verksamhet, vars förebyggande, utredning och lagföring stöds av samordning och samarbete mellan leverantörer av samhällsviktiga tjänster, leverantörer av digitala tjänster, behöriga myndigheter och rättsvårdande myndigheter. Om en incident misstänks ha samband med allvarlig brottslig verksamhet enligt unionsrätt eller nationell rätt, bör medlemsstaterna uppmuntra leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster att rapportera incidenter som misstänks vara av allvarlig brottslig art till de relevanta rättsvårdande myndigheterna. När så är lämpligt är det önskvärt att samordningen mellan behöriga myndigheter och rättsvårdande myndigheter i olika medlemsstater underlättas av Europeiska it-brottscentrumet (EC3) och Enisa.

(63) Säkerheten för personuppgifter undergrävs ofta till följd av incidenter. I detta sammanhang bör behöriga myndigheter och dataskyddsmyndigheter samarbeta och utbyta information om alla relevanta frågor för att hantera personuppgiftsincidenter till följd av incidenter.

(64) Jurisdiktion över leverantörer av digitala tjänster bör tillkomma den medlemsstat där den berörda leverantören av digitala tjänster har sitt huvudsakliga etableringsställe i unionen, vilket i princip motsvarar den plats där leverantören har sitt huvudkontor i unionen. Det krävs att leverantören utför en faktisk och reell verksamhet med hjälp av en stabil struktur för att den ska anses vara etablerad. Den rättsliga formen för en sådan struktur bör här, oavsett om det är en filial eller ett dotterbolag med juridisk personlighet, inte vara den avgörande faktorn. Detta

kriterium bör inte vara avhängigt av om nätverks- och informationssystemen är fysiskt belägna på en viss plats; att sådana system finns och används innebär inte i sig att det rör sig om ett huvudsakligt etableringsställe och utgör därför inte ett kriterium för att fastställa det huvudsakliga etableringsstället.

(65) En leverantör av digitala tjänster som inte är etablerad i unionen men erbjuder tjänster inom unionen bör utse en företrädare. I syfte att fastställa om en sådan leverantör av digitala tjänster erbjuder tjänster inom unionen bör det kontrolleras om det är uppenbart att leverantören av digitala tjänster planerar att erbjuda tjänster till personer i en eller flera medlemsstater. Enbart den omständigheten att en webbplats tillhörande leverantören av digitala tjänster eller en mellanhand, eller en e-postadress och andra kontaktuppgifter, är tillgängliga i unionen, eller att ett språk används som allmänt används i det tredjeland där leverantören av digitala tjänster är etablerad, är inte 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 detta andra språk, eller att kunder eller användare i unionen omnämns, göra det uppenbart att leverantören av digitala tjänster planerar att erbjuda tjänster inom unionen. Företrädaren bör agera på leverantören av digitala tjänsters vägnar och det bör vara möjligt för behöriga myndigheter eller CSIRT-enheterna att kontakta företrädaren. Företrädaren bör utses uttryckligen genom en skriftlig fullmakt från leverantören av digitala tjänster att agera på dess vägnar med avseende på leverantörens skyldigheter enligt detta direktiv, inklusive incidentrapportering.

(66) Standardisering av säkerhetskrav är en marknadsdriven process. För att säkerställa en enhetlig tillämpning av säkerhetsstandarder bör medlemsstaterna främja efterlevnad eller överensstämmelse med specificerade standarder för att garantera en hög nivå på säkerheten i nätverks- och informationssystem på unionsnivå. Enisa bör bistå medlemsstaterna genom rådgivning och riktlinjer. Därför kan det vara lämpligt att utarbeta harmoniserade standarder, i enlighet med Europaparlamentets och rådets förordning (EU) nr 1025/2012 ([1]).

(67) Enheter som inte omfattas av detta direktivs tillämpningsområde kan drabbas av incidenter med en betydande inverkan på de tjänster som de tillhandahåller. Om dessa enheter anser att det ligger i allmänhetens intresse att rapportera förekomsten av sådana incidenter till de berörda myndigheterna i medlemsstaterna, bör de kunna göra det på frivillig grund. Sådana rapporter bör behandlas av den behöriga myndigheten eller CSIRT-enheten förutsatt att behandlingen inte utgör en oproportionell eller orimlig börda för de berörda medlemsstaterna.

(68) 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 säkerhets- och rapporteringskrav som är tillämpliga på leverantörer av digitala tjänster. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([2]). När kommissionen antar genomförandeakter om de förfaranden som krävs för samarbetsgruppens verksamhet bör den ta största hänsyn till yttrandet från Enisa.

(69) När kommissionen antar genomförandeakter om säkerhetskraven för leverantörer av digitala tjänster bör den ta största hänsyn till yttrandet från Enisa och samråda med berörda parter. Kommissionen uppmuntras dessutom att beakta följande exempel: när det gäller systems och anläggningars säkerhet: fysisk säkerhet och miljösäkerhet, funktionssäkerhet, kontroll av åtkomst till nätverks- och informationssystem samt nätverks- och informationssystemens integritet; när det gäller incidenthantering: incidenthanteringsförfaranden, kapacitet att upptäcka incidenter, incidentrapportering och kommunikation; när det gäller driftskontinuitetshantering: strategier för tjänstekontinuitet samt beredskapsplaner, kapacitet för katastrofberedskap; när det gäller övervakning, revision och testning: strategier för övervakning och loggning, beredskapsövningar, testning av nätverks- och informationssystem, säkerhetsbedömningar och övervakning av efterlevnaden.

(70) Vid genomförandet av detta direktiv bör kommissionen på lämpligt sätt samarbeta med relevanta sektorskommittéer och organ som inrättas på unionsnivå inom de områden som omfattas av detta direktiv.

([1]) 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).

([2]) 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).

(71) Detta direktiv bör med jämna mellanrum ses över av kommissionen i samråd med berörda parter, främst i syfte att avgöra behovet av ändringar med hänsyn till samhällsutvecklingen, den politiska utvecklingen, den tekniska utvecklingen eller ändrade marknadsvillkor.

(72) Utbytet av information om risker och incidenter inom samarbetsgruppen och CSIRT-nätverket och uppfyllandet av kravet att rapportera incidenter till de behöriga nationella myndigheterna eller CSIRT-enheterna kan kräva behandling av personuppgifter. Sådan behandling bör ske i enlighet med Europaparlamentets och rådets direktiv 95/46/EG ([1]) och Europaparlamentets och rådets förordning (EG) nr 45/2001 ([2]). Vid tillämpningen av detta direktiv bör Europaparlamentets och rådets förordning (EG) nr 1049/2001 ([3]) tillämpas där så är lämpligt.

(73) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den 14 juni 2013 ([4]).

(74) Eftersom målet för detta direktiv, nämligen att uppnå en hög gemensam nivå på säkerheten i nätverks- och informationssystem 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.

(75) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna, i synnerhet rätten till respekt för privatliv och kommunikationer, skydd av personuppgifter, näringsfriheten, rätten till egendom, rätten till ett effektivt rättsmedel och rätten att yttra sig. Detta direktiv bör genomföras i enlighet med dessa rättigheter och principer.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte och tillämpningsområde

1. I detta direktiv fastställs åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverks- och informationssystem inom unionen, i syfte att förbättra den inre marknadens funktion.

2. Direktivet omfattar i detta syfte följande:

a) Det fastställer skyldigheter för alla medlemsstater att anta en nationell strategi för säkerhet i nätverks- och informationssystem.

b) Det inrättar en samarbetsgrupp i syfte att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna och att utveckla förtroende och tillit mellan dem.

c) Det inrättar ett nätverk för enheter för hantering av it-säkerhetsincidenter (nedan kallat *CSIRT-nätverket*) i syfte att bidra till utvecklingen av förtroende och tillit mellan medlemsstaterna och främja ett snabbt och effektivt operativt samarbete.

([1]) Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).
([2]) Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).
([3]) Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).
([4]) EUT C 32, 4.2.2014, s. 19.

d) Det fastställer säkerhets- och rapporteringskrav för leverantörer av samhällsviktiga tjänster och för leverantörer av digitala tjänster.

e) Det fastställer skyldigheter för medlemsstaterna att utse nationella behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter med uppgifter som har anknytning till säkerheten i nätverks- och informationssystem.

3. Säkerhets- och rapporteringskraven enligt detta direktiv ska inte tillämpas på företag som omfattas av kraven i artiklarna 13a och 13b i direktiv 2002/21/EG eller på leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 i förordning (EU) nr 910/2014.

4. Detta direktiv påverkar inte tillämpningen av rådets direktiv 2008/114/EG ([1]) eller Europaparlamentets och rådets direktiv 2011/93/EU ([2]) och 2013/40/EU ([3]).

5. Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget får information som är konfidentiell enligt unionsbestämmelser och nationella bestämmelser, såsom bestämmelser om affärshemligheter, utbytas med kommissionen och andra relevanta myndigheter endast när 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 sådant utbyte ska informationens konfidentialitet bevaras och säkerhetsintressen och kommersiella intressen hos leverantörer av såväl samhällsviktiga tjänster som digitala tjänster skyddas.

6. Detta direktiv påverkar inte medlemsstaternas åtgärder för att skydda sina väsentliga statliga funktioner, särskilt för att skydda den nationella säkerheten, inklusive åtgärder för skydd av information vars avslöjande medlemsstaterna anser strida mot sina väsentliga säkerhetsintressen, och för att upprätthålla lag och ordning, särskilt för att möjliggöra utredning, upptäckt och lagföring av brott.

7. Om det i en sektorsspecifik unionsrättsakt föreskrivs krav på att leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster antingen ska säkerställa säkerheten i sina nätverks- och informationssystem eller rapportera incidenter, ska bestämmelserna i den sektorsspecifika unionsrättsakten tillämpas, förutsatt att verkan av kraven i fråga minst motsvarar verkan av skyldigheterna i detta direktiv.

Artikel 2

Behandling av personuppgifter

1. Behandling av personuppgifter enligt detta direktiv ska ske i enlighet med direktiv 95/46/EG.

2. Behandling av personuppgifter som utförs av unionens institutioner och organ enligt detta direktiv ska ske i enlighet med förordning (EG) nr 45/2001.

Artikel 3

Minimiharmonisering

Utan att det påverkar tillämpningen av artikel 16.10 eller medlemsstaternas skyldigheter enligt unionsrätten får medlemsstaterna anta eller behålla bestämmelser som syftar till att uppnå en högre nivå på säkerheten i nätverks- och informationssystem.

([1]) 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 (EUT L 345, 23.12.2008, s. 75).

([2]) 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).

([3]) 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).

Artikel 4

Definitioner

I detta direktiv avses med

1. *nätverks- och informationssystem*:

   a) ett elektroniskt kommunikationsnät enligt artikel 2 a i direktiv 2002/21/EG,

   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 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 vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem,

3. *nationell strategi för säkerheten i nätverks- och informationssystem*: en ram med strategiska mål och prioriteringar för säkerhet i nätverks- och informationssystem på nationell nivå,

4. *leverantör av samhällsviktiga tjänster*: en offentlig eller privat enhet av en typ som avses i bilaga II vilken uppfyller kriterierna i artikel 5.2,

5. *digital tjänst*: en tjänst i den mening som avses i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ([1]) av en typ som anges i bilaga III,

6. *leverantör av digitala tjänster*: en juridisk person som tillhandahåller en digital tjänst,

7. *incident*: en händelse med en faktisk negativ inverkan på säkerheten i nätverks- och informationssystem,

8. *incidenthantering*: alla förfaranden som stöder upptäckt, analys och begränsning av en incident och åtgärder mot en incident,

9. *risk*: en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i nätverks- och informationssystem,

10. *företrädare*: en i unionen etablerad fysisk eller juridisk person som uttryckligen har utsetts att agera för en leverantör av digitala tjänster som inte är etablerad i unionen, till vilken en behörig nationell myndighet eller en CSIRT-enhet kan vända sig, i stället för till leverantören av digitala tjänster, i frågor som gäller de skyldigheter som leverantören av digitala tjänster har enligt detta direktiv,

11. *standard*: en standard i den mening som avses i artikel 2.1 i förordning (EU) nr 1025/2012,

12. *specifikation*: en teknisk specifikation i den mening som avses i artikel 2.4 i förordning (EU) nr 1025/2012,

13. *internetknutpunkt (IXP)*: en nätfacilitet som möjliggör sammankoppling av mer än två oberoende autonoma system, främst i syfte att underlätta utbytet av internettrafik; en IXP tillhandahåller sammankoppling enbart för autonoma system och kräver inte att den internettrafik som passerar mellan två deltagande autonoma system passerar genom ett tredje autonomt system och ändrar inte heller trafiken eller påverkar den på något annat sätt,

14. *domännamnssystem (DNS)*: ett hierarkiskt, distribuerat namngivningssystem i ett nätverk som hanterar domännamnsförfrågningar,

([1]) 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).

15. *leverantör av DNS-tjänst*: en enhet som tillhandahåller DNS-tjänster på internet,

16. *registreringsenhet för toppdomäner*: en enhet som administrerar och förvaltar registreringen av internetdomännamn under en specifik toppdomän,

17. *internetbaserad marknadsplats*: en digital tjänst som gör det möjligt för konsumenter och/eller näringsidkare enligt definitionen i artikel 4.1 a respektive 4.1 b i Europaparlamentets och rådets direktiv 2013/11/EU ([1]) att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare antingen på webbplatsen för den internetbaserade marknadsplatsen eller på en webbplats tillhörande en näringsidkare där datatjänster som tillhandahålls av en internetbaserad marknadsplats används,

18. *internetbaserad sökmotor*: en digital tjänst som gör det möjligt för användare att göra sökningar på i princip alla webbplatser eller webbplatser på ett visst språk på grundval av en förfrågan om vilket ämne som helst i form av ett nyckelord, en fras eller annan inmatning och som returnerar länkar som innehåller information om det begärda innehållet,

19. *molntjänster*: en digital tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser.

Artikel 5

Identifiering av leverantörer av samhällsviktiga tjänster

1. Senast den 9 november 2018 ska medlemsstaterna, för varje sektor och delsektor som avses i bilaga II, identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium.

2. Kriterierna för identifiering av leverantörer av samhällsviktiga tjänster enligt artikel 4.4 ska vara följande:

a) En enhet tillhandahåller en tjänst som är viktig för att upprätthålla kritisk samhällelig och/eller ekonomisk verksamhet,

b) tillhandahållandet av denna tjänst är beroende av nätverks- och informationssystem, och

c) en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

3. Med avseende på tillämpningen av punkt 1 ska varje medlemsstat upprätta en förteckning över de tjänster som avses i punkt 2 a.

4. Med avseende på tillämpningen av punkt 1 gäller att om en enhet tillhandahåller en tjänst som avses i punkt 2 a i två eller flera medlemsstater, ska dessa medlemsstater samråda med varandra. Detta samråd ska äga rum innan ett beslut om identifiering fattas.

5. Medlemsstaterna ska regelbundet och minst vartannat år efter den 9 maj 2018 se över och vid behov uppdatera förteckningen över identifierade leverantörer av samhällsviktiga tjänster.

6. Samarbetsgruppens roll ska, i överensstämmelse med de uppgifter som anges i artikel 11, vara att hjälpa medlemsstaterna att tillämpa ett enhetligt tillvägagångssätt i förfarandet för identifiering av leverantörer av samhällsviktiga tjänster.

7. Med avseende på den översyn som avses i artikel 23 ska medlemsstaterna, senast den 9 november 2018 och därefter vartannat år, tillhandahålla kommissionen den information som är nödvändig för att kommissionen ska kunna bedöma genomförandet av detta direktiv, särskilt enhetligheten i medlemsstaternas tillvägagångssätt för identifiering av leverantörer av samhällsviktiga tjänster. Denna information ska omfatta åtminstone

a) nationella åtgärder som gör det möjligt att identifiera leverantörer av samhällsviktiga tjänster,

([1]) Europaparlamentets och rådets direktiv 2013/11/EU av den 21 maj 2013 om alternativ tvistlösning vid konsumenttvister och om ändring av förordning (EG) nr 2006/2004 och direktiv 2009/22/EG (direktivet om alternativ tvistlösning) (EUT L 165, 18.6.2013, s. 63).

b) den förteckning över tjänster som avses i punkt 3,

c) det antal leverantörer av samhällsviktiga tjänster som har identifierats för varje sektor som avses i bilaga II samt en uppgift om deras betydelse för den sektorn,

d) tröskelvärden, om sådana finns, för att fastställa den relevanta leveransnivån med hänvisning till det antal användare som är beroende av tjänsten i enlighet med artikel 6.1 a eller till betydelsen av den specifika leverantören av samhällsviktiga tjänster i enlighet med artikel 6.1 f.

I syfte att bidra till tillhandahållandet av jämförbar information får kommissionen, med största hänsyn till yttrandet från Enisa, anta lämpliga tekniska riktlinjer om parametrar för den information som avses i denna punkt.

Artikel 6

Betydande störning

1. När medlemsstaterna fastställer om en störning är betydande enligt artikel 5.2 c, ska de beakta åtminstone följande sektorsöverskridande faktorer:

a) Det antal användare som är beroende av den tjänst som den berörda enheten tillhandahåller.

b) Hur beroende andra sektorer enligt bilaga II är av den tjänst som enheten tillhandahåller.

c) Vilken inverkan incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet eller allmän säkerhet, uttryckt i grad och varaktighet.

d) Enhetens marknadsandel.

e) Hur stort geografiskt område som skulle kunna påverkas av en incident.

f) Enhetens betydelse för upprätthållandet av en tillräcklig tjänstenivå, med beaktande av tillgången till alternativa sätt för att tillhandahålla tjänsten.

2. För att fastställa huruvida en incident skulle medföra en betydande störning ska medlemsstaterna även, i lämpliga fall, beakta sektorsspecifika faktorer.

KAPITEL II

NATIONELLA RAMAR FÖR SÄKERHETEN I NÄTVERKS- OCH INFORMATIONSSYSTEM

Artikel 7

Nationell strategi för säkerhet i nätverks- och informationssystem

1. Varje medlemsstat ska anta en nationell strategi för säkerhet i nätverks- och informationssystem som fastställer strategiska mål och lämpliga politiska åtgärder och lagstiftningsåtgärder för att uppnå och bibehålla en hög nivå på säkerheten i nätverks- och informationssystem och som täcker åtminstone de sektorer som avses i bilaga II och de tjänster som avses i bilaga III. Den nationella strategin för säkerhet i nätverks- och informationssystem ska i synnerhet omfatta följande:

a) Målen och prioriteringarna i den nationella strategin för säkerhet i nätverks- och informationssystem.

b) En styrningsram för att uppnå målen och prioriteringarna i den nationella strategin för säkerhet i nätverks- och informationssystem, inklusive offentliga organs och andra berörda aktörers roller och ansvarsområden.

c) Identifiering av beredskaps-, svars- och återhämtningsåtgärder, inklusive samarbete mellan offentlig och privat sektor.

d) Uppgift om program för utbildning och åtgärder för ökad medvetenhet rörande den nationella strategin för säkerhet i nätverks- och informationssystem.

e) Uppgift om forsknings- och utvecklingsplaner rörande den nationella strategin för säkerhet i nätverks- och informationssystem.

f) En riskbedömningsplan för identifiering av risker.

g) En förteckning över de olika aktörer som deltar i genomförandet av den nationella strategin för säkerhet i nätverks- och informationssystem.

2. Medlemsstaterna får begära Enisas bistånd vid utarbetandet av nationella strategier för säkerhet i nätverks- och informationssystem.

3. Medlemsstaterna ska underrätta kommissionen om sina nationella strategier för säkerhet i nätverks- och informationssystem inom tre månader från deras antagande. Härvid får medlemstaterna utesluta delar av strategin som rör nationell säkerhet.

Artikel 8

Nationella behöriga myndigheter och gemensam kontaktpunkt

1. Varje medlemsstat ska utse en eller flera nationella behöriga myndigheter för säkerhet i nätverks- och informationssystem (nedan kallad *den behöriga myndigheten*), åtminstone för de sektorer som avses i bilaga II och de tjänster som avses i bilaga III. Medlemsstaterna får tilldela en eller flera befintliga myndigheter denna roll.

2. De behöriga myndigheterna ska övervaka tillämpningen av detta direktiv på nationell nivå.

3. Varje medlemsstat ska utse en gemensam nationell kontaktpunkt för säkerhet i nätverks- och informationssystem (nedan kallad *den gemensamma kontaktpunkten*). Medlemsstaterna får tilldela en befintlig myndighet denna roll. Om en medlemsstat bara utser en behörig myndighet, ska denna behöriga myndighet också vara den gemensamma kontaktpunkten.

4. Den gemensamma kontaktpunkten ska utöva en sambandsfunktion för att säkerställa gränsöverskridande samarbete mellan medlemsstaternas myndigheter och med de berörda myndigheterna i andra medlemsstater samt med den samarbetsgrupp som avses i artikel 11 och det CSIRT-nätverk som avses i artikel 12.

5. Medlemsstaterna ska säkerställa att de behöriga myndigheterna och de gemensamma kontaktpunkterna har tillräckliga resurser för att på ett effektivt sätt kunna utföra de uppgifter de tilldelas och därigenom uppnå målen med detta direktiv. Medlemsstaterna ska säkerställa att de utsedda företrädarna samarbetar på ett effektivt och säkert sätt i samarbetsgruppen.

6. De behöriga myndigheterna och den gemensamma kontaktpunkten ska, när så är lämpligt och i överensstämmelse med nationell rätt, samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna och de nationella dataskyddsmyndigheterna.

7. Varje medlemsstat ska utan dröjsmål underrätta kommissionen om utnämningen av den behöriga myndigheten och den gemensamma kontaktpunkten och deras uppgifter samt alla senare ändringar. Varje medlemsstat ska offentliggöra utnämningen av den behöriga myndigheten och den gemensamma kontaktpunkten. Kommissionen ska offentliggöra förteckningen över utsedda gemensamma kontaktpunkter.

Artikel 9

Enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter)

1. Varje medlemsstat ska utse en eller flera CSIRT-enheter som ska uppfylla kraven i punkt 1 i bilaga I, som täcker åtminstone de sektorer som avses i bilaga II och de tjänster som avses i bilaga III och som ansvarar för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande. En CSIRT-enhet får inrättas inom en behörig myndighet.

2. Medlemsstaterna ska säkerställa att CSIRT-enheterna har de resurser som de behöver för att effektivt utföra sina uppgifter enligt punkt 2 i bilaga I.

Medlemsstaterna ska säkerställa att deras CSIRT-enheter samarbetar på ett ändamålsenligt, effektivt och säkert sätt i det CSIRT-nätverk som avses i artikel 12.

3. Medlemsstaterna ska säkerställa att deras CSIRT-enheter har tillgång till lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur på nationell nivå.

4. Medlemsstaterna ska underrätta kommissionen om sina CSIRT-enheters uppgifter samt om huvudinslagen i deras incidenthanteringsförfarande.

5. Medlemsstaterna får begära Enisas bistånd vid inrättandet av nationella CSIRT-enheter.

Artikel 10

Samarbete på nationell nivå

1. Om den behöriga myndigheten, den gemensamma kontaktpunkten och CSIRT-enheten i en och samma medlemsstat är separata, ska de samarbeta när det gäller fullgörandet av skyldigheterna enligt detta direktiv.

2. Medlemsstaterna ska säkerställa att antingen de behöriga myndigheterna eller CSIRT-enheterna mottar incidentrapporter som lämnas in i enlighet med detta direktiv. Om en medlemsstat beslutar att CSIRT-enheterna inte ska motta rapporter ska CSIRT-enheterna, i den mån det är nödvändigt för att de ska kunna utföra sina uppgifter, beviljas tillgång till uppgifter om incidenter som rapporterats av leverantörer av samhällsviktiga tjänster enligt artikel 14.3 och 14.5, eller av leverantörer av digitala tjänster enligt artikel 16.3 och 16.6.

3. Medlemsstaterna ska säkerställa att de behöriga myndigheterna eller CSIRT-enheterna informerar de gemensamma kontaktpunkterna om incidentrapporter som lämnats in i enlighet med detta direktiv.

Den gemensamma kontaktpunkten ska senast den 9 augusti 2018, och därefter en gång om året, lämna en sammanfattande rapport till samarbetsgruppen om de rapporter som mottagits, inklusive antalet rapporter och de rapporterade incidenternas art, samt om vilka åtgärder som vidtagits i enlighet med artiklarna 14.3, 14.5, 16.3 och 16.6.

KAPITEL III

SAMARBETE

Artikel 11

Samarbetsgrupp

1. För att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna och skapa förtroende och tillit, och i syfte att uppnå en hög gemensam nivå på säkerheten i nätverks- och informationssystem i unionen, inrättas härmed en samarbetsgrupp.

Samarbetsgruppen ska utföra sina uppgifter på grundval av tvååriga arbetsprogram enligt punkt 3 andra stycket.

2. Samarbetsgruppen ska bestå av företrädare för medlemsstaterna, kommissionen och Enisa.

När så är lämpligt får samarbetsgruppen bjuda in företrädare för de berörda parterna att delta i arbetet.

Kommissionen ska tillhandahålla sekretariatet.

3. Samordningsgruppen ska ha följande uppgifter:

a) Tillhandahålla strategisk vägledning för verksamheten i det CSIRT-nätverk som inrättas enligt artikel 12.

b) Utbyta bästa praxis om informationsutbyte angående incidentrapportering enligt artiklarna 14.3, 14.5, 16.3 och 16.6.

c) Utbyta bästa praxis mellan medlemsstaterna och, i samarbete med Enisa, bistå medlemsstaterna med kapacitetsuppbyggnad för att säkerställa säkerheten i nätverks- och informationssystem.

d) Diskutera medlemsstaternas förmåga och beredskap samt utvärdera, på frivillig grund, nationella strategier för säkerhet i nätverks- och informationssystem och CSIRT-enheternas effektivitet och identifiera bästa praxis.

e) Utbyta information och bästa praxis vad gäller åtgärder för ökad medvetenhet och utbildning.

f) Utbyta information och bästa praxis om forskning och utveckling vad gäller säkerhet i nätverks- och informationssystem.

g) Vid behov utbyta erfarenheter om frågor som rör säkerhet i nätverks- och informationssystem med unionens berörda institutioner, organ och byråer.

h) Diskutera de standarder och specifikationer som avses i artikel 19 med företrädare för de relevanta europeiska standardiseringsorganen.

i) Samla in information om bästa praxis vad gäller risker och incidenter.

j) Årligen studera de sammanfattande rapporter som avses i artikel 10.3 andra stycket.

k) Diskutera arbetet med övningar som avser säkerhet i nätverks- och informationssystem och utbildning, inklusive det arbete som utförs av Enisa.

l) Med Enisas bistånd utbyta bästa praxis för medlemsstaternas identifiering av leverantörer av samhällsviktiga tjänster, inklusive i samband med beroende, vad gäller risker och incidenter, som sträcker sig över gränser.

m) Diskutera metoder för rapportering av incidentrapporter enligt artiklarna 14 och 16.

Samarbetsgruppen ska, senast den 9 februari 2018 och därefter vartannat år, utarbeta ett arbetsprogram med åtgärder som ska vidtas för att genomföra dess mål och uppgifter, som ska överensstämma med målen för detta direktiv.

4. Med avseende på den översyn som avses i artikel 23 ska samarbetsgruppen, senast den 9 augusti 2018 och därefter med 1,5 års mellanrum, utarbeta en rapport med en bedömning av erfarenheterna av det strategiska samarbetet enligt den här artikeln.

5. Kommissionen ska anta genomförandeakter i vilka fastställs de förfaranden som krävs för samarbetsgruppens verksamhet. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 22.2.

Vid tillämpningen av första stycket ska kommissionen senast den 9 februari 2017 förelägga den kommitté som avses i artikel 22.1 det första utkastet till genomförandeakt.

Artikel 12

CSIRT-nätverk

1. För att bidra till utvecklingen av förtroende och tillit mellan medlemsstaterna och för att främja snabbt och effektivt operativt samarbete inrättas härmed ett nätverk för nationella CSIRT-enheter.

2. CSIRT-nätverket ska bestå av företrädare för medlemsstaternas CSIRT-enheter och Cert-EU. Kommissionen ska delta i CSIRT-nätverket som observatör. Enisa ska tillhandahålla sekretariatet och aktivt stödja samarbetet mellan CSIRT-enheterna.

3. CSIRT-nätverket ska ha följande uppgifter:

a) Utbyta information om CSIRT-enheternas tjänster, verksamhet och samarbetskapacitet.

b) På begäran av en företrädare för en CSIRT-enhet från en medlemsstat som kan komma att påverkas av en incident, utbyta och diskutera ej kommersiellt känsliga uppgifter rörande incidenten och dithörande risker; en CSIRT-enhet från en medlemsstat kan dock neka att bidra till diskussionen om det finns en risk för att det skulle skada utredningen av incidenten.

c) På frivillig grund utbyta och tillgängliggöra icke-konfidentiella uppgifter om enskilda incidenter.

d) På begäran av en företrädare för en medlemsstats CSIRT-enhet, diskutera och om möjligt utarbeta en samordnad åtgärd till följd av en incident som har upptäckts inom den medlemsstatens jurisdiktion.

e) Stödja medlemsstaterna i hanteringen av gränsöverskridande incidenter på grundval av deras frivilliga ömsesidiga bistånd.

f) Diskutera, utforska och identifiera ytterligare former av operativt samarbete, inklusive med avseende på

   i) kategorier av risker och incidenter,

   ii) tidiga varningar,

   iii) ömsesidigt bistånd,

   iv) principer och metoder för samordning, när medlemsstaterna vidtar åtgärder mot gränsöverskridande risker och incidenter.

g) Informera samarbetsgruppen om sin verksamhet och om ytterligare former av operativt samarbete som diskuterats enligt led f samt begära vägledning i sistnämnda avseende.

h) Diskutera lärdomar från övningar som avser säkerhet i nätverks- och informationssystem, inklusive från sådana som organiserats av Enisa.

i) På begäran av en enskild CSIRT-enhet, diskutera den enhetens kapacitet och beredskap.

j) Utfärda riktlinjer för att underlätta konvergens mellan operativ praxis med avseende på tillämpningen av bestämmelserna i denna artikel om operativt samarbete.

4. Med avseende på den översyn som avses i artikel 23 ska CSIRT-nätverket, senast den 9 augusti 2018 och därefter med 1,5 års mellanrum, utarbeta en rapport med en bedömning av erfarenheterna av det operativa samarbetet enligt denna artikel, inklusive slutsatser och rekommendationer. Rapporten ska även föreläggas samarbetsgruppen.

5. CSIRT-nätverket ska fastställa sin arbetsordning.

Artikel 13

Internationellt samarbete

Unionen får i enlighet med artikel 218 i EUF-fördraget ingå internationella avtal med tredjeländer eller internationella organisationer, och därvid tillåta och organisera deras deltagande i vissa av samarbetsgruppens verksamheter. Sådana avtal ska beakta behovet av att säkerställa ändamålsenligt skydd av uppgifter.

KAPITEL IV

SÄKERHET I NÄTVERKS- OCH INFORMATIONSSYSTEM SOM ANVÄNDS AV LEVERANTÖRER AV SAMHÄLLSVIKTIGA TJÄNSTER

Artikel 14

Säkerhetskrav och incidentrapportering

1. Medlemsstaterna ska säkerställa att leverantörer av samhällsviktiga tjänster vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder i sin verksamhet. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken.

2. Medlemsstaterna ska säkerställa att leverantörer av samhällsviktiga tjänster vidtar lämpliga åtgärder för att förebygga och minimera verkningarna av incidenter som påverkar säkerheten i nätverks- och informationssystem som används för att tillhandahålla sådana samhällsviktiga tjänster, i syfte att säkerställa kontinuiteten i dessa tjänster.

3. Medlemsstaterna ska säkerställa att leverantörer av samhällsviktiga tjänster utan onödigt dröjsmål till den behöriga myndigheten eller CSIRT-enheten rapporterar incidenter som har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänster som de tillhandahåller. Rapporterna ska innehålla information som gör det möjligt för den behöriga myndigheten eller CSIRT-enheten att fastställa incidentens eventuella gränsöverskridande verkningar. Rapportering ska inte medföra ökat ansvar för den rapporterande parten.

4. För att avgöra om en incident har en betydande inverkan ska hänsyn framför allt tas till följande faktorer:

a) Det antal användare som påverkas av störningen av den samhällsviktiga tjänsten.

b) Hur länge incidenten varar.

c) Hur stort geografiskt område som påverkas av incidenten.

5. Mot bakgrund av informationen i rapporten från leverantören av den samhällsviktiga tjänsten ska den behöriga myndigheten eller CSIRT-enheten informera den eller de andra berörda medlemsstaterna, om incidenten har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i den medlemsstaten. Därvid ska den behöriga myndigheten eller CSIRT-enheten, i enlighet med unionsrätten eller med nationell lagstiftning som är förenlig med unionsrätten, bevara nämnda leverantörs säkerhetsintressen och kommersiella intressen samt konfidentialiteten hos informationen i leverantörens rapport.

När omständigheterna tillåter ska den behöriga myndigheten eller CSIRT-enheten förse den rapporterande leverantören av samhällsviktiga tjänster med relevant information om uppföljningen av rapporten, såsom information som skulle kunna bidra till effektiv hantering av incidenten.

På begäran av den behöriga myndigheten eller CSIRT-enheten ska den gemensamma kontaktpunkten vidarebefordra rapporter enligt första stycket till gemensamma kontaktpunkter i andra medlemsstater som påverkats av incidenten.

6. Efter samråd med den rapporterande leverantören av samhällsviktiga tjänster får den behöriga myndigheten eller CSIRT-enheten informera allmänheten om enskilda incidenter, om allmänheten behöver känna till dem för att det ska vara möjligt att förhindra en incident eller åtgärda en pågående incident.

7. Behöriga myndigheter som agerar tillsammans inom samarbetsgruppen får utarbeta och anta riktlinjer för under vilka omständigheter leverantörer av samhällsviktiga tjänster är skyldiga att rapportera incidenter, inklusive riktlinjer om vilka faktorer som ska användas för att fastställa om en incident har betydande inverkan enligt punkt 4.

Artikel 15

Genomförande och efterlevnad

1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har de befogenheter och medel de behöver för att bedöma huruvida leverantörer av samhällsviktiga tjänster uppfyller sina skyldigheter enligt artikel 14 och effekterna därav på säkerheten i nätverks- och informationssystem.

2. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har de befogenheter och medel som krävs för att ålägga leverantörer av samhällsviktiga tjänster att tillhandahålla

a) den information som är nödvändig för att bedöma säkerheten i deras nätverks- och informationssystem, inbegripet dokumenterade säkerhetsprinciper,

b) bevis för ett effektivt genomförande av säkerhetsprinciper, såsom resultaten av en säkerhetsrevision utförd av den behöriga myndigheten eller en auktoriserad revisor och, i det senare fallet, att ge den behöriga myndigheten tillgång till resultaten, inklusive de underliggande bevisen.

När den behöriga myndigheten begär sådan information eller sådana bevis ska den uppge syftet med begäran och precisera vilken information som krävs.

3. Efter att ha bedömt information eller resultat av säkerhetsrevisioner enligt punkt 2, får den behöriga myndigheten utfärda bindande anvisningar till leverantörerna av samhällsviktiga tjänster om hur de ska avhjälpa de identifierade bristerna.

4. Den behöriga myndigheten ska ha ett nära samarbete med dataskyddsmyndigheter när den åtgärdar incidenter som medför personuppgiftsincidenter.

KAPITEL V

SÄKERHET I NÄTVERKS- OCH INFORMATIONSSYSTEM SOM ANVÄNDS AV LEVERANTÖRER AV DIGITALA TJÄNSTER

Artikel 16

Säkerhetskrav och incidentrapportering

1. Medlemsstaterna ska säkerställa att leverantörer av digitala tjänster utarbetar och vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder när de tillhandahåller sådana tjänster som avses i bilaga III inom unionen. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken, varvid hänsyn ska tas till

a) säkerheten i system och anläggningar,

b) incidenthantering,

c) hantering av driftskontinuitet,

d) övervakning, revision och testning,

e) efterlevnad av internationella standarder.

2. Medlemsstaterna ska säkerställa att leverantörer av digitala tjänster vidtar åtgärder för att förebygga och minimera den inverkan som incidenter som påverkar säkerheten i deras nätverks- och informationssystem har på de tjänster som avses i bilaga III och som erbjuds inom unionen, i syfte att säkerställa kontinuiteten i dessa tjänster.

3. Medlemsstaterna ska säkerställa att leverantörer av digitala tjänster utan onödigt dröjsmål till den behöriga myndigheten eller CSIRT-enheten rapporterar alla incidenter som har en avsevärd inverkan på tillhandahållandet av en tjänst som avses i bilaga III och som de erbjuder inom unionen. Rapporterna ska innehålla information som gör det möjligt för den behöriga myndigheten eller CSIRT-enheten att fastställa vilken betydelse eventuell gränsöverskridande inverkan har. Rapportering ska inte medföra ökat ansvar för den rapporterande parten.

4. För att fastställa om en incident har en avsevärd inverkan ska hänsyn framför allt tas till följande faktorer:

a) Det antal användare som påverkas av incidenten, framför allt användare som är beroende av tjänsten för att kunna tillhandahålla sina egna tjänster.

b) Hur länge incidenten varar.

c) Hur stort geografiskt område som påverkas av incidenten.

d) I vilken utsträckning incidenten stör tjänstens funktion.

e) I vilken utsträckning incidenten inverkar på den ekonomiska och samhälleliga verksamheten.

Skyldigheten att rapportera en incident ska endast gälla om leverantören av digitala tjänster har tillgång till den information som behövs för att bedöma en incidents inverkan mot bakgrund av de faktorer som avses i första stycket.

5. Om en leverantör av samhällsviktiga tjänster är beroende av en tredjepartsleverantör av digitala tjänster för tillhandahållandet av en tjänst som är viktig för att upprätthålla kritisk samhällelig och ekonomisk verksamhet, ska leverantören av samhällsviktiga tjänster rapportera varje betydande inverkan på kontinuiteten i de samhällsviktiga tjänsterna till följd av en incident som påverkar leverantören av digitala tjänster.

6. Om så är lämpligt, och särskilt om den incident som avses i punkt 3 berör två eller flera medlemsstater, ska den behöriga myndigheten eller CSIRT-enheten informera andra medlemsstater som påverkats. Därvid ska de behöriga myndigheterna, CSIRT-enheter och gemensamma kontaktpunkter, i enlighet med unionsrätten eller nationell lagstiftning som är förenlig med unionsrätten, bevara leverantören av digitala tjänsters säkerhetsintressen och kommersiella intressen samt den tillhandahållna informationens konfidentialitet.

7. Efter samråd med den berörda leverantören av digitala tjänster får den behöriga myndigheten eller CSIRT-enheten och, om så är lämpligt, myndigheterna eller CSIRT-enheterna i andra berörda medlemsstater, informera allmänheten om enskilda incidenter eller kräva att leverantören av digitala tjänster gör det, om allmänheten behöver känna till dem för att det ska vara möjligt att förhindra en incident eller åtgärda en pågående incident eller om incidentens avslöjande på annat sätt omfattas av allmänintresset.

8. Kommissionen ska anta genomförandeakter för att ytterligare specificera de element som avses i punkt 1 och de faktorer som anges i punkt 4 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 22.2 senast den 9 augusti 2017.

9. Kommissionen får anta genomförandeakter som fastställer format och förfaranden tillämpliga på rapporteringskrav. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 22.2.

10. Utan att det påverkar tillämpningen av artikel 1.6 får medlemsstaterna inte införa ytterligare säkerhets- eller rapporteringskrav för leverantörer av digitala tjänster.

11. Kapitel V ska inte tillämpas på mikroföretag och små företag enligt definitionen i kommissionens rekommendation 2003/361/EG ([1]).

([1]) 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).

Artikel 17

Genomförande och efterlevnad

1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna vid behov vidtar åtgärder genom tillsynsåtgärder i efterhand, när de har mottagit bevis på att en leverantör av digitala tjänster inte uppfyller kraven i artikel 16. Sådana bevis får läggas fram av en behörig myndighet i en annan medlemsstat där tjänsten tillhandahålls.

2. Vid tillämpning av punkt 1 ska de behöriga myndigheterna ha de befogenheter och medel som krävs för att ålägga leverantörer av digitala tjänster att

a) tillhandahålla den information som behövs för en bedömning av säkerheten i deras nätverks- och informationssystem, inbegripet dokumenterade säkerhetsprinciper, och

b) åtgärda varje underlåtenhet att uppfylla kraven i artikel 16.

3. Om en leverantör av digitala tjänster har sitt huvudsakliga etableringsställe eller en företrädare i en medlemsstat, men dess nätverks- och informationssystem är belägna i en eller flera andra medlemsstater, ska den behöriga myndigheten i den medlemsstat där det huvudsakliga etableringsstället eller företrädaren finns och de behöriga myndigheterna i dessa andra medlemsstater samarbeta och vid behov bistå varandra. Detta bistånd och samarbete får omfatta informationsutbyte mellan de berörda behöriga myndigheterna och begäranden om att de tillsynsåtgärder som avses i punkt 2 ska vidtas.

Artikel 18

Jurisdiktion och territorialitet

1. Vid tillämpningen av detta direktiv ska en leverantör av digitala tjänster anses omfattas av jurisdiktionen i den medlemsstat där leverantören har sitt huvudsakliga etableringsställe. En leverantör av digitala tjänster ska anses ha sitt huvudsakliga etableringsställe i en medlemsstat om den har sitt huvudkontor i denna medlemsstat.

2. En leverantör av digitala tjänster som inte är etablerad i unionen men som erbjuder sådana tjänster som avses i bilaga III inom unionen ska utse en företrädare i unionen. Företrädaren ska vara etablerad i en av de medlemsstater där tjänsterna erbjuds. Leverantören av digitala tjänster ska anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad.

3. Att leverantören av digitala tjänster utser en företrädare ska inte påverka eventuella rättsliga åtgärder mot leverantören av digitala tjänster själv.

KAPITEL VI

STANDARDISERING OCH FRIVILLIG RAPPORTERING

Artikel 19

Standardisering

1. För att främja en enhetlig tillämpning av artiklarna 14.1, 14.2, 16.1 och 16.2 ska medlemsstaterna, utan att föreskriva eller gynna användning av en viss typ av teknik, uppmuntra användningen av europeiska eller internationellt accepterade standarder och specifikationer av relevans för säkerheten i nätverks- och informationssystem.

2. Enisa ska i samarbete med medlemsstaterna utarbeta råd och riktlinjer för de tekniska områden som ska beaktas när det gäller punkt 1 samt för redan befintliga standarder, inklusive medlemsstaternas nationella standarder, som skulle kunna täcka dessa områden.

Artikel 20

Frivillig rapportering

1. Utan att det påverkar tillämpningen av artikel 3 får enheter som inte har identifierats som leverantörer av samhällsviktiga tjänster och som inte är leverantörer av digitala tjänster, på frivillig grund, rapportera incidenter som har en betydande inverkan på kontinuiteten i de tjänster som de tillhandahåller.

2. Vid behandlingen av rapporter ska medlemsstaterna agera i enlighet med det förfarande som fastställs i artikel 14. Medlemsstaterna får ge behandling av obligatoriska rapporter företräde framför behandling av frivilliga rapporter. Frivilliga rapporter ska endast behandlas om behandlingen inte utgör en oproportionell eller orimlig börda för de berörda medlemsstaterna.

En frivillig rapport får inte leda till att den rapporterande enheten åläggs skyldigheter som den inte skulle ha varit föremål för om den inte hade gett in rapporten.

KAPITEL VII

SLUTBESTÄMMELSER

Artikel 21

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella bestämmelser som har antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast den 9 maj 2018 samt utan dröjsmål eventuella ändringar som berör dem.

Artikel 22

Kommittéförfarande

1. Kommissionen ska biträdas av kommittén för säkerhet i nätverks- och informationssystem. 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.

Artikel 23

Översyn

1. Kommissionen ska senast den 9 maj 2019 lämna en rapport till Europaparlamentet och rådet, där den bedömer enhetligheten i medlemsstaternas tillvägagångssätt vid identifieringen av leverantörer av samhällsviktiga tjänster.

2. Kommissionen ska regelbundet se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet. I detta syfte 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. I sin översyn ska kommissionen också bedöma förteckningarna i bilagorna II och III samt enhetligheten i identifieringen av leverantörer av samhällsviktiga tjänster och tjänster i de sektorer som avses i bilaga II. Den första rapporten ska lämnas senast den 9 maj 2021.

Artikel 24

Övergångsbestämmelser

1. Utan att det påverkar tillämpningen av artikel 25 och i syfte att erbjuda medlemsstaterna ytterligare möjligheter till lämpligt samarbete under införlivandeperioden, ska samarbetsgruppen och CSIRT-nätverket börja utföra sina uppgifter enligt artikel 11.3 respektive 12.3 senast den 9 februari 2017.

2. Under perioden från och med den 9 februari 2017 till och med den 9 november 2018 ska samarbetsgruppen, i syfte att hjälpa medlemsstaterna att tillämpa ett enhetligt tillvägagångssätt i förfarandet för identifiering av leverantörer av samhällsviktiga tjänster, diskutera förfarandet för, innehållet i och typen av nationella åtgärder som möjliggör identifiering av leverantörer av samhällsviktiga tjänster inom en särskild sektor i enlighet med de kriterier som anges i artiklarna 5 och 6. Samarbetsgruppen ska på begäran av en medlemsstat också diskutera medlemsstatens utkast till specifika nationella åtgärder som möjliggör identifiering av leverantörer av samhällsviktiga tjänster inom en särskild sektor i enlighet med de kriterier som anges i artiklarna 5 och 6.

3. Senast den 9 februari 2017 ska medlemsstaterna vid tillämpning av denna artikel säkerställa att de är korrekt företrädda i samarbetsgruppen och CSIRT-nätverket.

Artikel 25

Införlivande

1. Medlemsstaterna ska senast den 9 maj 2018 anta och offentliggöra de bestämmelser i lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta.

De ska tillämpa dessa bestämmelser från och med den 10 maj 2018.

När en medlemsstat antar dessa bestämmelser 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.

2. Medlemsstaterna ska till kommissionen överlämna texten till de centrala bestämmelser i nationell rätt som de antar inom det område som omfattas av detta direktiv.

Artikel 26

Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 27

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Strasbourg den 6 juli 2016.

På Europaparlaments vägnar	*På rådets vägnar*
M. SCHULZ	I. KORČOK
Ordförande	*Ordförande*

BILAGA I

KRAV PÅ ENHETER FÖR HANTERING AV IT-SÄKERHETSINCIDENTER (*COMPUTER SECURITY INCIDENT RESPONSE TEAMS*, NEDAN KALLADE *CSIRT-ENHETER*) SAMT DERAS UPPGIFTER

Kraven på CSIRT-enheter samt deras uppgifter ska på ett lämpligt och entydigt sätt fastställas och stödjas genom nationell politik och/eller lagstiftning. Följande ska ingå:

1. Krav på CSIRT-enheter

   a) CSIRT-enheterna ska säkerställa en hög nivå på tillgången till sina kommunikationstjänster genom att undvika felkritiska systemdelar (*single points of failure*) och ska kunna kontaktas och kontakta andra när som helst och på flera olika sätt. Kommunikationskanalerna ska dessutom vara tydligt specificerade och välkända för användargruppen och samarbetspartner.

   b) CSIRT-enheternas lokaler och de informationssystem som de använder sig av ska vara belägna på säker plats.

   c) Driftskontinuitet:

      i) CSIRT-enheter ska ha ett ändamålsenligt system för handläggning och dirigering av ansökningar, så att överlämnanden underlättas.

      ii) CSIRT-enheter ska ha tillräckligt med personal för att ständigt vara tillgängliga.

      iii) CSIRT-enheter ska förlita sig på en infrastruktur med säkerställd kontinuitet. Därför måste systemen ha inbyggd redundans och reservlokaler finnas tillgängliga.

   d) CSIRT-enheter ska om de så önskar ha möjlighet att delta i internationella samarbetsnätverk.

2. CSIRT-enheters uppgifter

   a) CSIRT-enheters uppgifter ska omfatta minst följande:

      i) Övervakning av incidenter på nationell nivå.

      ii) Tillhandahållande av tidiga varningar, larm, meddelanden och informationsspridning till relevanta aktörer om risker och incidenter.

      iii) Åtgärder till följd av incidenter.

      iv) Tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet.

      v) Deltagande i CSIRT-nätverket.

   b) CSIRT-enheter ska bygga upp samarbetsrelationer med den privata sektorn.

   c) För att underlätta samarbete ska CSIRT-enheter främja antagandet och användningen av gemensam eller standardiserad praxis för

      i) förfaranden för hantering av incidenter och risker,

      ii) klassificeringssystem för incidenter, risker och information.

BILAGA II

TYPER AV ENHETER ENLIGT ARTIKEL 4.4

Sektor	Delsektor	Typ av enhet
1. Energi	a) Elektricitet	— Elföretag enligt definitionen i artikel 2.35 i Europaparlamentets och rådets direktiv 2009/72/EG ([1]) som bedriver ”leverans eller handel” enligt definitionen i artikel 2.19 i det direktivet
		— Systemansvariga för distributionssystemet enligt definitionen i artikel 2.6 i direktiv 2009/72/EG
		— Systemansvariga för överföringssystemet enligt definitionen i artikel 2.4 i direktiv 2009/72/EG
	b) Olja	— Operatörer av oljeledningar
		— Operatörer av oljeproduktion, raffinaderier, bearbetningsanläggningar, lagring och överföring
	c) Gas	— Gashandelsföretag eller gashandlare enligt definitionen i artikel 2.8 i Europaparlamentets och rådets direktiv 2009/73/EG ([2])
		— 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
2. Transporter	a) Lufttransport	— Lufttrafikföretag enligt definitionen i artikel 3.4 i Europaparlamentets och rådets förordning (EG) nr 300/2008 ([3])
		— Flygplatsens ledningsenheter enligt definitionen i artikel 2.2 i Europaparlamentets och rådets direktiv 2009/12/EG ([4]), 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 ([5]), och enheter som driver kringliggande installationer vid flygplatser

Sektor	Delsektor	Typ av enhet
		— Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänst enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 549/2004 ([6])
	b) Järnvägstransport	— Infrastrukturförvaltare enligt definitionen i artikel 3.2 i Europaparlamentets och rådets direktiv 2012/34/EU ([7])
		— Järnvägsföretag enligt definitionen i artikel 3.1 i direktiv 2012/34/EU, inbegripet tjänsteleverantörer enligt definitionen i artikel 3.12 i direktiv 2012/34/EU
	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 ([8]), 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 ([9]), 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 sjötrafikinformationstjänster enligt definitionen i artikel 3 o i Europaparlamentets och rådets direktiv 2002/59/EG ([10])
	d) Vägtransport	— Vägmyndigheter enligt definitionen i artikel 2.12 i kommissionens delegerade förordning (EU) 2015/962 ([11]) med ansvar för trafikstyrning och trafikledning
		— Operatörer av intelligenta transportsystem enligt definitionen i artikel 4.1 i Europaparlamentets och rådets direktiv 2010/40/EU ([12])
3. Bankverksamhet		Kreditinstitut enligt definitionen i artikel 4.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013 ([13])
4. Finans-marknads-infrastruktur		— Operatörer av handelsplatser enligt definitionen i artikel 4.24 i Europaparlamentets och rådets direktiv 2014/65/EU ([14])
		— Centrala motparter enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 648/2012 ([15])
5. Hälso- och sjukvårdssektorn	Hälso- och sjukvårdsmiljöer (inklusive sjukhus och privata kliniker)	Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU ([16])

Sektor	Delsektor	Typ av enhet
6. Leverans och distribution av dricksvatten		Leverantörer och distributörer av dricksvatten enligt definitionen i artikel 2.1 a i rådets direktiv 98/83/EG ([17]), dock exklusive distributörer för vilka distribution av dricksvatten endast utgör en del av deras allmänna verksamhet, som består i distribution av andra förnödenheter och varor som inte anses utgöra samhällsviktiga tjänster
7. Digital infrastruktur		— Internetknutpunkter
		— Leverantörer av DNS-tjänster
		— Registreringsenheter för toppdomäner

([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 (EUT L 211, 14.8.2009, s. 55).
([2]) 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).
([3]) 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).
([4]) Europaparlamentets och rådets direktiv 2009/12/EG av den 11 mars 2009 om flygplatsavgifter (EUT L 70, 14.3.2009, s. 11).
([5]) 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).
([6]) 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).
([7]) 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).
([8]) 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).
([9]) Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd (EUT L 310, 25.11.2005, s. 28).
([10]) 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 (EGT L 208, 5.8.2002, s. 10).
([11]) 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).
([12]) 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).
([13]) 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 (EUT L 176, 27.6.2013, s. 1).
([14]) 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).
([15]) 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).
([16]) 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).
([17]) Rådets direktiv 98/83/EG av den 3 november 1998 om kvaliteten på dricksvatten (EGT L 330, 5.12.1998, s. 32).

BILAGA III

TYPER AV DIGITALA TJÄNSTER ENLIGT ARTIKEL 4.5

1. Internetbaserad marknadsplats.
2. Internetbaserad sökmotor.
3. Molntjänster.

Jämförelsetabell

Jämförelsetabell – en sammanställning av bestämmelserna i NIS-direktivet och motsvarande bestämmelser i den föreslagna lagen och i den föreslagna förordningen.

Artikel i NIS-direktivet	*Bestämmelse i lagen eller förordningen*
1.1	1 § lagen
1.2	–
1.3	3–4 §§ lagen
1.4–5	–
1.6	6 § lagen
1.7	5 § första stycket lagen
2	–
3	–
4	7 § lagen
5.1	2 § a och 8 § lagen
5.2	8 § första stycket lagen
5.3	46 § 1 lagen 10 § 2 förordningen
5.4	8 § fjärde stycket lagen 3 § första stycket förordningen
5.5	10 § 2 förordningen
5.6	–
5.7	–
6.1	8 § andra stycket och 45 § 1 lagen
6.2	8 § tredje stycket och 45 § 1 lagen 11 § 2 förordningen

7	–
8.1–2	22 § lagen 5 § förordningen
8.3–4	43 § lagen 7 § förordningen
8.5	–
8.6	6 § 1 och 8 § 6 förordningen Framgår även av 6 § förvaltningslagen (1986:223) och 6 § andra stycket myndighetsförordningen (2007:515)
8.7	–
9.1	44 § lagen 8 § förordningen
9.2–3	8 § andra stycket förordningen
9.4–5	–
10.1	Framgår redan av 6 § förvaltningslagen (1986:223) och 6 § andra stycket myndighetsförordningen (2007:515)
10.2	8 § tredje stycket 1 förordningen
10.3	7 § tredje stycket förordningen
11	–
12	–
13	–
14.1	10, 11, 13 §§, 45 § 2 och 46 § 2 lagen 10 § 1 och 11 § 1 förordningen
14.2	10, 12, 13 §§, 45 § 2 och 46 § 2 lagen 10 § 1 och 11 § 1 förordningen
14.3	10, 16, 44 §§ och 46 § 3 lagen 10 § 3 förordningen
14.4	17 § och 45 § 3 lagen 11 § 3 förordningen
14.5	7 § andra stycket, 8 § tredje stycket 2 och 5 förordningen, 15 kap. 1 a § offentlighets- och sekretesslagen (2009:400)

14.6	8 § tredje stycket 4 förordningen
14.7	6 § 2, 9 § och 11 § 3 förordningen
15.1–2	23–26 §§ lagen
15.3	30–31 §§ lagen
15.4	6 § 1 förordningen
16.1	14 § lagen
16.2	15 § lagen
16.3	19 och 44 §§ och 47 § 1 lagen 10 § 3 förordningen
16.4	20 § lagen
16.5	18 § lagen
16.6	8 § tredje stycket 3 förordningen, 15 kap. 1 a § offentlighets- och sekretesslagen (2009:400)
16.7	21 § lagen 8 § tredje stycket 4 förordningen
16.8–10	–
16.11	2 § b lagen
17.1	28 § lagen
17.2 a	23 §, 24 § första och tredje stycket, 25 och 27 §§ lagen
17.2 b	30–31 §§ lagen
17.3	6 § 5 förordningen
18.1	2 § b lagen
18.2	2 § b och 9 § lagen
18.3	–
19.1	4 § förordningen
19.2	–
20.1–2	46 § 4, 47 § 2 lagen 10 § 4 förordningen
21	31–42 §§ lagen
22	–
23	–

24	–
25	–
26	–
27	–

Statens offentliga utredningar 2017

Kronologisk förteckning

1. För Sveriges landsbygder – en sammanhållen politik för arbete, hållbar tillväxt och välfärd. N.
2. Kraftsamling för framtidens energi. M.
3. Karens för statsråd och statssekreterare. Fi.
4. För en god och jämlik hälsa. En utveckling av det folkhälsopolitiska ramverket. S.
5. Svensk social trygghet i en globaliserad värld. Del 1 och 2. S.
6. Se barnet! Ju.
7. Straffprocessens ramar och domstolens beslutsunderlag i brottmål – en bättre hantering av stora mål. Ju.
8. Kunskapsläget på kärnavfallsområdet 2017. Kärnavfallet – en fråga i ständig förändring. M.
9. Det handlar om oss. – unga som varken arbetar eller studerar. U.
10. Ny ordning för att främja god sed och hantera oredlighet i forskning. U.
11. Vägskatt. Volym 1 och 2. Fi.
12. Att ta emot människor på flykt. Sverige hösten 2015. Ju.
13. Finansiering av infrastruktur med privat kapital? Fi.
14. Migrationsärenden vid utlandsmyndigheterna. Ju.
15. Kvalitet och säkerhet på apoteksmarknaden. S.
16. Sverige i Afghanistan 2002–2014. UD.
17. Om oskuldspresumtionen och rätten att närvara vid rättegången. Genomförande av EU:s oskuldspresumtionsdirektiv. Ju.
18. En nationell strategi för validering. U.
19. Uppdrag: Samverkan. Steg på vägen mot fördjupad lokal samverkan för unga arbetslösa. A.
20. Tillträde för nybörjare – ett öppnare och enklare system för tillträde till högskoleutbildning. U.
21. Läs mig! Nationell kvalitetsplan för vård och omsorg om äldre personer. Del 1 och 2. S.
22. Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. M.
23. digitalforvaltning.nu. Fi.
24. Ett arbetsliv i förändring – hur påverkas ansvaret för arbetsmiljön? A.
25. Samlad kunskap – stärkt handläggning. S.
26. Delningsekonomi. På användarnas villkor. Fi.
27. Vissa frågor inom fastighets- och stämpelskatteområdet. Fi.
28. Ett nationellt centrum för kunskap om och utvärdering av arbetsmiljö. A.
29. Brottsdatalag. Ju
30. En omreglerad spelmarknad. Del 1 och 2. Fi.
31. Stärkt konsumentskydd på bostadsrättsmarknaden. Ju.
32. Substitution i Centrum – stärkt konkurrenskraft med kemikaliesmarta lösningar. M.
33. Stärkt ställning för hyresgäster. Ju.
34. Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. M.
35. Samling för skolan. Nationell strategi för kunskap och likvärdighet. U.
36. Informationssäkerhet för samhällsviktiga och digitala tjänster. Ju.

Statens offentliga utredningar 2017

Systematisk förteckning

Tillträde för nybörjare – ett öppnare och enklare system för tillträde till högskoleutbildning. [20]

Samling för skolan. Nationell strategi för kunskap och likvärdighet. [35]

Utrikesdepartementet

Sverige i Afghanistan 2002–2014. [16]