Lagrådsremiss

Informationssäkerhet för samhällsviktiga och digitala tjänster

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 15 februari 2018

Morgan Johansson

Ida Wettervik
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Nätverk och informationssystem spelar en allt viktigare roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och den inre marknadens funktion. Europaparlamentet och rådet antog därför 2016 ett direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverk och informationssystem inom hela EU, det s.k. NIS-direktivet.

I syfte att genomföra NIS-direktivet i svensk rätt föreslår regeringen en ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster. Den nya lagen innebär bl.a. att

- vissa leverantörer av samhällsviktiga tjänster och digitala tjänster ska vidta säkerhetsåtgärder till skydd för säkerheten i nätverk och informationssystem
- leverantörerna ska rapportera incidenter som påverkar kontinuiteten i tjänsterna
- den myndighet som regeringen bestämmer ska utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till den följs, och ska kunna besluta om vitesföreläggande och sanktionsavgift mot den som underlåter att följa lagens bestämmelser.

Den nya lagen föreslås träda i kraft den 1 augusti 2018.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag om informationssäkerhet för samhällsviktiga och digitala tjänster,
2. lag om ändring i lagen (2018:000) om informationssäkerhet för samhällsviktiga och digitala tjänster.

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag om informationssäkerhet för samhällsviktiga och digitala tjänster

Härigenom föreskrivs[1] följande.

Syftet med lagen

1 § Syftet med denna lag är att uppnå en hög nivå på säkerheten i nätverk och informationssystem för digitala tjänster samt för samhällsviktiga tjänster inom sektorerna

– energi,
– transport,
– bankverksamhet,
– finansmarknadsinfrastruktur,
– hälso- och sjukvård,
– leverans och distribution av dricksvatten, och
– digital infrastruktur.

Genom lagen 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).

Uttryck i lagen

2 § I lagen avses med

1. *nätverk och informationssystem*:

a) ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen (2003:389) om elektronisk kommunikation,

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

c) digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av a och b för att de ska kunna driftas, användas, skyddas och underhållas,

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, överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via dessa nätverk och informationssystem,

[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.

3. *samhällsviktig tjänst*: en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,

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, och som utgör en internetbaserad marknadsplats, internetbaserad sökmotor eller molntjänst,

5. *internetbaserad marknadsplats*: en 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) att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare, antingen på webbplatsen för den internetbaserade marknadsplatsen eller på en webbplats som tillhör en näringsidkare och där datatjänster som tillhandahålls av en internetbaserad marknadsplats används,

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

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

8. *företrädare*: en fysisk eller juridisk person som uttryckligen har utsetts att agera för en leverantör av digitala tjänster och till vilken myndigheter 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,

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

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

Lagens tillämpningsområde

3 § Lagen gäller för

1. leverantörer av det slag som anges i bilaga 2 till NIS-direktivet och som tillhandahåller en samhällsviktig tjänst, under förutsättning att leverantören är etablerad i Sverige, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten (leverantörer av samhällsviktiga tjänster).

2. juridiska personer som tillhandahåller en digital tjänst och som har sitt huvudsakliga etableringsställe i Sverige eller har utsett en företrädare som är etablerad här (leverantörer av digitala tjänster).

I 10 § finns en bestämmelse som gäller för andra leverantörer.

4 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka tjänster som är samhällsviktiga tjänster och vad som avses med en betydande störning enligt 3 § första stycket 1.

Undantag från lagens tillämpningsområde

Leverantörer av elektroniska kommunikationstjänster

5 § Lagen gäller inte för företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och därför omfattas av kraven i 5 kap. 6 b och c §§ lagen (2003:389) om elektronisk kommunikation.

Leverantörer av betrodda tjänster

6 § 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.

Leverantörer av digitala tjänster som är mikroföretag eller små företag

7 § Lagen gäller inte för leverantörer av digitala tjänster som är 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.

Säkerhetskänslig verksamhet

8 § Lagen gäller inte för verksamhet som omfattas av krav på säkerhetsskydd enligt säkerhetsskyddslagen (1996:627).

Leverantörer som omfattas av krav på informationssäkerhet i andra författningar

9 § Om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder och incidentrapportering, ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt denna lag.

Utseende av företrädare

10 § En juridisk person som erbjuder digitala tjänster i Sverige men som inte har sitt huvudsakliga etableringsställe inom Europeiska unionen ska, om inte något undantag från lagens tillämpningsområde enligt 5–9 §§ är tillämpligt, utse en företrädare som är etablerad i en medlemsstat där tjänsterna erbjuds.

Säkerhetsåtgärder

Skyldigheter för leverantörer av samhällsviktiga tjänster

11 § Leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.

12 § Leverantörer av samhällsviktiga tjänster ska göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder enligt 13 och 14 §§. I analysen ska det ingå en åtgärdsplan. Analysen ska dokumenteras och uppdateras årligen.

13 § 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 för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken.

14 § Leverantörer av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

Skyldigheter för leverantörer av digitala tjänster

15 § Leverantörer av digitala tjänster ska vidta de tekniska och organisatoriska åtgärder som de anser ändamålsenliga och proportionella och som hanterar risker som hotar säkerheten i nätverk och informationssystem som de använder när de tillhandahåller digitala tjänster inom Europeiska unionen. Åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken.

16 § Leverantörer av digitala tjänster ska vidta åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder. Skyldigheten gäller endast i förhållande till verkningar som sådana incidenter har på digitala tjänster som leverantören erbjuder inom Europeiska unionen. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

Bemyndigande

17 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om säkerhetsåtgärder enligt 11–16 §§.

Incidentrapportering

Rapporteringsskyldighet för leverantörer av samhällsviktiga tjänster

18 § 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 den myndighet som regeringen bestämmer.

Rapporteringsskyldighet för leverantörer av digitala tjänster

19 § Leverantörer av digitala tjänster ska utan onödigt dröjsmål rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av en digital tjänst som de erbjuder inom Europeiska unionen. Rapporteringen ska göras till den myndighet som regeringen bestämmer.

Bemyndigande

20 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om incidentrapportering enligt 18 och 19 §§.

Tillsyn

Tillsynsmyndighetens uppdrag

21 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet. Tillsynsmyndigheten ska utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

22 § Tillsynsåtgärder när det gäller leverantörer av digitala tjänster får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att en leverantör inte uppfyller kraven i 15, 16 eller 19 §.

Anmälningsskyldighet för leverantörer av samhällsviktiga tjänster

23 § Leverantörer av samhällsviktiga tjänster ska utan dröjsmål anmäla sig till tillsynsmyndigheten. Av en anmälan ska det framgå om leverantören tillhandahåller en samhällsviktig tjänst i två eller flera medlemsstater inom Europeiska unionen.

Tillsynsmyndighetens undersökningsbefogenheter

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

25 § Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av lagen.

26 § Tillsynsmyndigheten får förelägga den som står under tillsyn att ge tillträde och tillhandahålla information enligt 24 och 25 §§.

Ett sådant föreläggande får förenas med vite.

27 § Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att genomföra de åtgärder som avses i 24 och 25 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Ingripanden och sanktioner

Åtgärdsförelägganden

28 § Tillsynsmyndigheten får meddela de förelägganden som behövs för att leverantörer ska uppfylla kraven på utseende av företrädare, säkerhetsåtgärder och incidentrapportering enligt 10, 12–16, 18 och 19 §§ och enligt föreskrifter som har meddelats i anslutning till de paragraferna.

Ett sådant föreläggande får förenas med vite.

Sanktionsavgift

29 § Tillsynsmyndigheten ska ta ut en sanktionsavgift av den som underlåter att

1. göra en anmälan till tillsynsmyndigheten enligt 23 § eller enligt föreskrifter som har meddelats i anslutning till den paragrafen,
2. vidta säkerhetsåtgärder enligt någon av 12–16 § eller enligt föreskrifter som har meddelats i anslutning till de paragraferna, eller
3. rapportera incidenter enligt 18 eller 19 § eller enligt föreskrifter som har meddelats i anslutning till de paragraferna.

30 § En sanktionsavgift ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

31 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till den skada eller risk för skada som uppstått till följd av överträdelsen, om leverantören tidigare har begått en överträdelse och de kostnader som leverantören har undvikit till följd av överträdelsen.

32 § En sanktionsavgift 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.

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

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

Ett beslut om sanktionsavgift ska delges.

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

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

En sanktionsavgift tillfaller staten.

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

Föreskrifter om verkställighet

37 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om verkställighet av denna lag.

Förordnande om att beslut ska gälla omedelbart

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

Överklagande

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

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 augusti 2018.

2.2 Förslag till lag om ändring i lagen (2018:000) om informationssäkerhet för samhällsviktiga och digitala tjänster

Härigenom föreskrivs att 8 § lagen (2018:000) om informationssäkerhet för samhällsviktiga och digitala tjänster ska ha följande lydelse.

Lydelse enligt SFS 2018:000	*Föreslagen lydelse*
8 §	
Lagen gäller inte för verksamhet som omfattas av *krav på säkerhetsskydd enligt* säkerhetsskyddslagen *(1996:627).*	Lagen gäller inte för verksamhet som omfattas av säkerhetsskyddslagen *(2018:000).*

Denna lag träder i kraft den 1 april 2019.

3 Ärendet och dess beredning

I juli 2016 antog Europaparlamentet och rådet direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem inom hela unionen, kallat NIS-direktivet. 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. NIS-direktivet finns i *bilaga 1*.

Regeringen beslutade den 31 mars 2016 att ge en särskild utredare i uppdrag att föreslå hur NIS-direktivet ska genomföras i svensk rätt. I april 2017 överlämnade utredaren betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36). En sammanfattning av betänkandet finns i *bilaga 2*. Betänkandets lagförslag finns i *bilaga 3*.

Betänkandet har remitterats. En förteckning över remissinstanserna finns i *bilaga 4*.

I denna lagrådsremiss föreslås de lagändringar som bedöms nödvändiga för att genomföra NIS-direktivet i svensk rätt.

4 Övergripande om NIS-direktivet

Syftet med NIS-direktivet är att förbättra den inre marknadens funktion genom att skapa tillit och förtroende och att fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen (artikel 1.1 och skäl 31). Flera av åtgärderna syftar mer specifikt till att säkerställa kontinuiteten i de samhällsviktiga och digitala tjänster som omfattas av direktivet.

Direktivet innebär bl.a. att vissa leverantörer av samhällsviktiga tjänster och vissa leverantörer av digitala tjänster ska vidta säkerhetsåtgärder för att hantera risker och incidenter i nätverk och informationssystem som de är beroende av för att kunna tillhandahålla tjänsterna. Leverantörerna ska också rapportera incidenter som har en betydande eller avsevärd påverkan på kontinuiteten i tjänsterna.

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 enheter som särskilt pekas ut i direktivet. Enheterna utgör olika slags leverantörer inom sju olika sektorer. Sektorerna är energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Dessutom krävs att den tjänst som tillhandahålls är samhällsviktig, 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 samhällsviktiga, 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.

Medlemsstaterna ska enligt direktivet utse myndigheter med särskilda uppgifter, t.ex. tillsynsmyndigheter, nationella kontaktpunkter och enheter för hantering av incidenter, s.k. CSIRT-enheter (Computer Security Incident Response Team). 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 bestämmelser som antagits enligt direktivet.

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

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 som anges i direktivet. För leverantörer av digitala tjänster får medlemsstaterna emellertid inte införa ytterligare säkerhets- eller rapporteringskrav.

Närmare redogörelse för NIS-direktivets innehåll ges löpande genom lagrådsremissen.

5 En ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster

5.1 En ny lag ska införas

Regeringens förslag: NIS-direktivet ska i huvudsak genomföras genom en ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster.

Utredningens förslag stämmer i sak överens med regeringens.

Remissinstanserna: En majoritet av remissinstanserna anser att det är viktigt för samhällets informationssäkerhet att NIS-direktivet genomförs. Många remissinstanser anser emellertid att ett samlat regelverk för genomförandet av NIS-direktivet kommer medföra att de krav som ställs på dem i olika regelverk på informationssäkerhetsområdet blir svåröverskådliga och svårtillämpade, bland andra *Affärsverket Svenska kraftnät*, *Energimyndigheten*, *Finansinspektionen*, *Frobbit AB*, *Landstinget i Södermanland*, *Malmö kommun*, *Netnod*, *Stockholms läns landsting*, *Västra Götalands läns landsting*, *Stiftelsen för internetinfrastruktur*, *Sveriges Kommuner och Landsting*, *Stockholms universitet*, *Sveriges Advokatsamfund*, *Svenskt Näringsliv*, *Säkerhets- och försvarsföretagen* och *Säkerhetspolisen*. Med hänsyn till bl.a. detta avstyrker Sveriges Advokatsamfund förslaget.

Skälen för regeringens förslag

Befintliga rättsliga krav på informationssäkerhet

I svensk rätt finns flera regelverk som ställer krav på informationssäkerhet utifrån olika syften och förutsättningar.

Övergripande bestämmelser om informationssäkerhet och krav på incidentrapportering för statliga myndigheter finns i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Syftet med förordningen är 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. Varje myndighet ansvarar enligt förordningen för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.

För de mest skyddsvärda verksamheterna finns i säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633) bestämmelser om hantering av hemliga uppgifter och incidentrapportering. Syftet med säkerhetsskyddsregleringen är framför allt att säkerställa ett skydd för verksamheter där påverkan genom ett antagonistiskt angrepp skulle medföra allvarliga konsekvenser på nationell nivå. Säkerhetsskyddet ska förebygga att hemliga uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs, att obehöriga får tillträde till platser där de kan få tillgång till sådana uppgifter eller där verksamhet som har betydelse för rikets säkerhet bedrivs och att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som är av betydelse för rikets säkerhet. I propositionen Ett modernt och stärkt skydd för Sveriges säkerhet (prop. 2017/18:89) föreslår regeringen en ny säkerhetsskyddslag. Den nya säkerhetsskyddslagen föreslås innefatta skydd av uppgifter som är av betydelse för Sveriges säkerhet eller som ska skyddas enligt ett internationellt åtagande om säkerhetsskydd. Vidare föreslår regeringen att det ska förtydligas att kraven i säkerhetsskyddsregleringen gäller i såväl allmän som enskild verksamhet. Säkerhetsskyddet ska enligt förslaget både skydda uppgifter som är hemliga och de som inte är hemliga men som skulle omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) om den lagen hade varit tillämplig i den aktuella verksamheten. Regeringen föreslår också att skyddet av annan säkerhetskänslig verksamhet, t.ex. samhällsviktiga informationssystem, ska förbättras.

Enligt lagen (2003:389) om elektronisk kommunikation, förkortad LEK, är den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst skyldig att vidta tekniska och organisatoriska åtgärder för att skydda uppgifter som behandlas i samband med tillhandahållande av tjänsten. I LEK regleras också att 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 Post- och telestyrelsen (PTS).

Utöver nämnda regelverk finns det i nationell rätt i vissa fall krav på säkerhet som även kan omfatta informationssäkerhet, t.ex. mer allmänt

formulerade bestämmelser om riskhantering och bestämmelser med krav på driftsäkerhet eller kontinuitet i den tillhandahållna tjänsten.

Det finns även sektorer som regleras av sektorsspecifika EU-rättsakter som innehåller krav på säkerhet i nätverk och informationssystem. Sjöfartssektorn, banksektorn och sektorn för finansmarknadsinfrastruktur är exempel på sådana sektorer. Vidare finns det en skyldighet att rapportera personuppgiftsincidenter enligt Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), kallad dataskyddsförordningen, som ska börja tillämpas från och med den 25 maj 2018.

Ett samlat regelverk för genomförandet av NIS-direktivet

Det finns olika sätt att genomföra NIS-direktivet i svensk rätt. Ett alternativ är genom ett samlat regelverk som specifikt avser direktivets genomförande, dvs. genom en ny lag med en anslutande förordning. Utredningen har föreslagit en sådan lösning. Fördelarna med ett samlat regelverk för genomförandet är att det blir tydligt för myndigheter, enskilda och tillsynsmyndigheten vilken reglering som finns när det gäller samhällsviktiga och digitala tjänster. 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. Vidare kan det underlätta tillämpningen, inte minst mot bakgrund av att myndigheter och enskilda kan komma att omfattas av NIS-direktivet i flera medlemsstater.

Ett stort antal av remissinstanserna, såsom *Affärsverket Svenska kraftnät*, *Energimyndigheten*, *Finansinspektionen*, *Frobbit AB*, *Malmö kommun*, *Netnod*, *Stiftelsen för internetinfrastruktur*, *Stockholms läns landsting*, *Västra Götalands läns landsting*, *Sveriges Kommuner och Landsting*, *Säkerhets- och försvarsföretagen* och *Säkerhetspolisen*, anser att ett samlat regelverk för genomförandet kommer att medföra svårigheter i tillämpningen gentemot andra regelverk. De flesta av dessa remissinstanser påpekar särskilt att kraven på incidentrapportering i NIS-direktivet tillsammans med andra närliggande krav på rapportering, såsom i säkerhetsskyddsregleringen och dataskyddsförordningen, kan medföra att aktörer med anledning av samma händelse ska skicka incidentrapporter till flera myndigheter med varierande innehåll och svarstid. Enligt Finansinspektionen kan det medföra en risk för att vissa aktörer väljer att inte rapportera alla relevanta incidenter och att lagstiftarens syfte med reglerna därmed undermineras. Mot denna bakgrund förespråkar bl.a. Affärsverket Svenska kraftnät, Stiftelsen för internetinfrastruktur, Stockholms universitet och Säkerhets- och försvarsföretagen på olika sätt ett regelverk som omfattar hela eller större delar av informationssäkerhetsområdet. Ett flertal remissinstanser, bl.a. Energimyndigheten, Finansinspektionen, Frobbit AB, *Göteborgs kommun*, Malmö kommun, Netnod, *Svenska bankföreningen*, *Svenskt Näringsliv*, Sveriges Kommuner och Landsting och Säkerhets- och försvarsföretagen, föreslår eller poängterar vikten av en harmonisering av reglerna om säkerhetsåtgärder och incidentrapportering

i olika regelverk för att om möjligt undvika att samma incident behöver rapporteras till flera myndigheter.

Som remissinstanserna påpekar är en av nackdelarna med ett samlat regelverk för genomförandet 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 även omfattas av andra EU-rättsakter finns också en risk för att det kan bli otydligt vilken reglering som gäller. Ett regelverk som omfattar hela eller stora delar av informationssäkerhetsregleringen skulle också ligga i linje med de rekommendationer Riksrevisionen lämnat i sin rapport Informationssäkerheten i den civila statsförvaltningen (RiR 2014:23). Informationssäkerhetsområdet är emellertid, som vissa remissinstanser också påpekar, fragmenterat och svåröverskådligt. De EU-rättsliga och nationella reglerna är mer utvecklade inom vissa sektorer än inom andra. Det finns också skillnader mellan olika typer av leverantörer inom samma sektor. Vissa bestämmelser i nationell rätt 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. Beträffande de digitala tjänster som regleras av NIS-direktivet saknas i dag reglering helt. För att tillmötesgå remissinstansernas efterfrågan om ett regelverk för hela eller stora delar av informationssäkerhetsområdet och en harmonisering av kraven i de olika regelverken, skulle det därför krävas ett omfattande arbete som bl.a. inkluderar kartläggning av ett stort antal nationella och unionsrättsliga bestämmelser. Remissinstansernas förslag i dessa avseenden kan enligt regeringen inte genomföras inom ramen för detta lagstiftningsärende.

Enligt regeringens mening bör genomförandet av NIS-direktivet i stället ske genom ett samlat regelverk. NIS-direktivet innebär skyldigheter för både enskilda och offentliga aktörer. Ett genomförande av direktivet behöver följaktligen ske huvudsakligen i lagform. Det bör därför införas en ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster. I vilken utsträckning genomförandet bör ske genom bestämmelser i förordning eller myndighetsföreskrifter kommer behandlas löpande genom lagrådsremissen.

En nationell it-strategi

Enligt artikel 7 i NIS-direktivet ska medlemsstaterna anta en nationell strategi för säkerhet i nätverk och informationssystem. Regeringen antog den 22 juni 2017 en nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213). Det pågår ett arbete i Regeringskansliet med att säkerställa att strategin motsvarar direktivets krav. Genomförandet av NIS-direktivet bör därför i denna del ske inom ramen för det arbetet. Den nya lagen bör alltså inte reglera Sveriges skyldighet enligt NIS-direktivet att anta en nationell it-strategi.

5.2 Syftet med lagen

Regeringens förslag: Syftet med den nya lagen ska vara att uppnå en hög nivå på säkerheten i nätverk och informationssystem för digitala tjänster samt för samhällsviktiga tjänster inom sektorerna
- energi
- transport
- bankverksamhet
- finansmarknadsinfrastruktur
- hälso- och sjukvård
- leverans och distribution av dricksvatten
- digital infrastruktur.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningen har föreslagit att det i den nya lagen ska anges att lagens syfte är att uppnå en hög gemensam nivå på säkerheten i nätverk och informationssystem inom EU, för att förbättra den inre marknadens funktion.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens förslag: NIS-direktivets syfte är enligt artikel 1 att uppnå en hög gemensam nivå på säkerheten i nätverk och informationssystem inom EU, för att förbättra den inre marknadens funktion. För att den nya lagens bestämmelser ska bli mer lättillgängliga anser regeringen – liksom utredningen – att den nya lagen bör innehålla en bestämmelse som anger det övergripande syftet med lagen. Till skillnad från utredningen anser regeringen emellertid att syftet bör formuleras på så sätt att lagen, utöver att den genomför NIS-direktivet, har till syfte att höja nivån på säkerheten i nätverk och informationssystem. Vidare bör det tydliggöras att syftet endast avser informationssäkerhet för vissa tjänster och sektorer.

5.3 Lagen ska gälla för vissa leverantörer av samhällsviktiga och digitala tjänster

Regeringens förslag: Den nya lagen ska gälla för
- leverantörer av det slag som anges i bilaga 2 till NIS-direktivet och som tillhandahåller en samhällsviktig tjänst, under förutsättning att leverantören är etablerad i Sverige, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten (leverantörer av samhällsviktiga tjänster).
- juridiska personer som tillhandahåller en tjänst som utgör en internetbaserad marknadsplats, internetbaserad sökmotor eller molntjänst och som har sitt huvudsakliga etableringsställe i Sverige eller som har utsett en företrädare som är etablerad här (leverantörer av digitala tjänster).

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vad som avses med en betydande störning vid tillhandahållandet av en samhällsviktig tjänst.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningen har föreslagit att de faktorer som enligt NIS-direktivet ska beaktas vid bedömningen av om en incident skulle medföra en betydande störning vid tillhandahållandet av en samhällsviktig tjänst ska föras in i den nya lagen.

Remissinstanserna: *E-hälsomyndigheten* och *Affärsverket Svenska kraftnät* anser att regelverket även bör omfatta leverantörer av samhällsviktiga tjänster som inte omfattas av NIS-direktivet. Flera remissinstanser anser att det är viktigt att det meddelas föreskrifter som tydliggör vad som krävs för att en leverantör som tillhandahåller samhällsviktiga tjänster ska omfattas av den nya lagen. *Datainspektionen* anser att det bör införas en upplysningsbestämmelse om att personuppgiftsbehandling ska ske i enlighet med dataskyddsdirektivet.

Skälen för regeringens förslag

Leverantörer av samhällsviktiga tjänster som omfattas av NIS-direktivet

För att en leverantör ska anses vara en sådan leverantör av samhällsviktiga tjänster som omfattas av NIS-direktivet krävs att leverantören är en sådan typ av enhet som anges i bilaga 2 till direktivet. Enheterna utgör olika slags leverantörer, såsom operatörer av oljeproduktion och vissa kreditinstitut och vårdgivare, och finns inom sju angivna sektorer. Sektorerna är energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Vidare krävs att leverantören tillhandahåller en samhällsviktig tjänst, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. En samhällsviktig tjänst definieras i direktivet som en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet (artiklarna 4.4 och 5.2).

För att en leverantör av samhällsviktiga tjänster ska omfattas av NIS-direktivet krävs även att leverantören är etablerad på en medlemsstats territorium (artikel 5.1). En leverantör av samhällsviktiga tjänster ska anses etablerad i en medlemsstat om leverantören bedriver en faktisk och reell verksamhet med hjälp av en stabil struktur. Den rättsliga formen för en sådan struktur, dvs. om det är fråga om exempelvis en filial eller ett dotterbolag, är inte en avgörande faktor (skäl 21).

Både offentliga aktörer, såsom statliga myndigheter, landsting och kommuner, och privata aktörer kan utgöra en leverantör av samhällsviktiga tjänster som omfattas av direktivet (artikel 4.4).

Leverantörer av digitala tjänster som omfattas av NIS-direktivet

De leverantörer av digitala tjänster som omfattas av NIS-direktivet är juridiska personer som tillhandahåller digitala tjänster. Med digital tjänst avses enligt direktivet en tjänst i form av en internetbaserad marknadsplats, internetbaserad sökmotor eller molntjänst (artiklarna 4.5 och 4.6 samt bilaga 3).

Med ordet tjänst avses en tjänst i den mening som stadgas 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 artikel 1.1 b i det direktivet definieras en tjänst som alla informationssamhällets tjänster, dvs. tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare.

En internetbaserad marknadsplats är enligt NIS-direktivet en digital tjänst som gör det möjligt för konsumenter 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 marknadsplats är alltså en webbplats där kunden kan ta del av flera näringsidkares utbud på samma ställe. Marknadsplatsen kan på detta sätt jämföras med ett köpcentrum. Som exempel på internetbaserade marknadsplatser kan nämnas amazon.com, etsy.com och blocket.se. Applikationsbutiker, som fungerar som onlinebutiker och möjliggör digital distribution av applikationer eller programvara från tredje part, ska enligt NIS-direktivet betraktas som en internetbaserad marknadsplats (skäl 15). 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 inte av begreppet internetbaserad marknadsplats. Sådana onlinetjänster, t.ex. pricerunner.se och prisjakt.nu, fungerar endast som mellanhand för tredjepartstjänster genom vilka ett avtal slutligen kan ingås (skäl 15). När en aktör tillhandahåller egna varor eller tjänster genom en e-butik är det inte heller fråga om tillhandahållande av en digital tjänst i form av en internetbaserad marknadsplats. Näringsidkaren tillhandahåller i sådana fall inte en digital tjänst i direktivets mening, utan använder webbplatsen i syfte att tillhandahålla andra varor och tjänster än digitala tjänster.

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). Exempel på internetbaserade sökmotorer är google.com, yahoo.com och bing.com. Jämförelsesajter och sökfunktioner som begränsas till innehållet på en särskild webbplats anses inte utgöra internetbaserade sökmotorer (skäl 16).

Molntjänster definieras i NIS-direktivet som en digital tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser (artikel 4.19). I skäl 17 till direktivet anges följande. Sådana dataresurser som molntjänster kan möjliggöra tillgång till är exempelvis 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.

GoogleApps, iCloud och Dropbox är exempel på molntjänster. En användare av privata moln tillhandahåller inte en molntjänst och är således inte en leverantör av en digital tjänst enligt direktivet.

För att en juridisk person som tillhandahåller internetbaserade marknadsplatser, internetbaserade sökmotorer eller molntjänster ska omfattas av NIS-direktivet krävs även att leverantören har sitt huvudsakliga etableringsställe i EU eller har utsett en företrädare som är etablerad i unionen. En leverantör av digitala tjänster ska omfattas av jurisdiktionen i den medlemsstat där leverantören har sitt huvudsakliga etableringsställe eller där den utsedde företrädaren är etablerad (artikel 18.1 och 18.2).

En leverantör av digitala tjänster som har sitt huvudsakliga etableringsställe i Sverige eller som har utsett en företrädare som är etablerad här ska alltså omfattas av den svenska reglering som genomför NIS-direktivet. Det huvudsakliga etableringsstället är i princip där leverantören har sitt huvudkontor. Att nätverk och informationssystem är fysiskt belägna på en viss plats innebär inte att det är fråga om ett huvudsakligt etableringsställe (skäl 64). I avsnitt 5.5 behandlas närmare när leverantörer av digitala tjänster ska utse en företrädare.

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

Det tillhandahålls samhällsviktiga tjänster av leverantörer som inte omfattas av NIS-direktivet. Ett exempel är de som tillhandahåller fjärrvärme. Direktivet omfattar som nämnts endast sådana slags leverantörer som tas upp i bilaga 2 till direktivet och leverantörer som tillhandahåller fjärrvärme tas inte upp där.

Ett antal remissinstanser, däribland *E-hälsomyndigheten* och *Affärsverket Svenska kraftnät*, anser att den nya lagen även bör omfatta leverantörer av samhällsviktiga tjänster som inte omfattas av direktivet. Enligt regeringens mening kan det finnas behov av tydligare kravställning rörande informationssäkerhet även för samhällsviktiga verksamheter som inte omfattas av NIS-direktivet. En mer övergripande lag skulle, som bl.a. Affärsverket Svenska kraftnät påpekar, kunna vara till fördel för enhetligheten på området, ge mindre utrymme för olika tolkningar och skapa bättre förutsättningar för leverantörerna att överblicka regelverket. Det finns emellertid inte möjlighet att inom ramen för detta lagstiftningsärende ta ställning till hur all samhällsviktig verksamhets informationssäkerhet bör regleras. Den nya lagen bör därför omfatta endast sådana leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster som omfattas av NIS-direktivet.

Föreskrifter om vad som utgör en betydande störning

Som framgår ovan är ett krav för att en leverantör ska anses vara en sådan leverantör av samhällsviktiga tjänster som omfattas av NIS-direktivet – och följaktligen den nya lagen – att leverantören tillhandahåller en samhällsviktig tjänst. Enligt regeringens förslag i avsnitt 6.2 ska regeringen

eller den myndighet som regeringen bestämmer få meddela föreskrifter om vilka tjänster som ska anses som samhällsviktiga enligt den nya lagen. Ett annat krav är att en incident skulle medföra en betydande störning vid tillhandahållandet av den samhällsviktiga tjänsten.

Vid bedömningen av vad som är en betydande störning ska enligt artikel 6 i NIS-direktivet ett antal olika faktorer beaktas. Dessa faktorer är det antal användare som är beroende av den tjänst som den berörda leverantören tillhandahåller, hur beroende andra sektorer enligt bilaga 2 till direktivet är av den tjänst som leverantören tillhandahåller, vilken inverkan incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet eller allmän säkerhet, uttryckt i grad och varaktighet, leverantörens marknadsandel, hur stort geografiskt område som skulle kunna påverkas av en incident och leverantörens betydelse för upprätthållandet av en tillräcklig tjänstenivå, med beaktande av tillgången till alternativa sätt för att tillhandahålla tjänsten.

När det gäller faktorn antalet användare som är beroende av tjänsten, kan användningen av tjänsten vara direkt, indirekt eller ske genom förmedling. Vid bedömningen av en incidents eventuella inverkan på ekonomisk och samhällelig verksamhet eller allmän säkerhet, bör medlemsstaterna också bedöma hur länge det sannolikt skulle dröja tills avbrottet skulle få en oacceptabel inverkan (skäl 27).

I lämpliga fall ska även sektorsspecifika faktorer beaktas. När det gäller energileverantörer kan sådana faktorer omfatta mängden eller andelen producerad nationell el, för oljeleverantörer mängden olja per dag, för lufttransport, 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, och för hälso- och sjukvårdssektorn antalet patienter som leverantören vårdar per år (skäl 28).

Artikel 6 ger tillämparen en begränsad vägledning vid bedömningen av vad som utgör en betydande störning och vänder sig snarare till de nationella lagstiftarna. Såsom flera remissinstanser påpekar, t.ex. *Energiföretagen* och *Sveriges Hamnar*, behövs därför föreskrifter som ger närmare vägledning. Till skillnad från utredningen anser regeringen att samtliga bestämmelser om vad som utgör en betydande störning vid tillhandahållandet av en samhällsviktig tjänst bör meddelas i förordning eller myndighetsföreskrifter. Enligt regeringens mening kan föreskrifterna behöva gå utöver vad regeringen eller den myndighet som regeringen bestämmer kan meddela med stöd av 8 kap. 7 § regeringsformen. Det bör därför införas ett bemyndigande i den nya lagen som anger att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande störning.

Personuppgiftsbehandling

Enligt artikel 2 i NIS-direktivet ska personuppgiftsbehandling enligt direktivet 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, kallat dataskyddsdirektivet. Dataskyddsdirektivet ersätts från och med den 25 maj 2018 av dataskyddsförordningen.

Datainspektionen anser att den nya lagen bör innehålla en upplysningsbestämmelse med samma innebörd som artikel 2 i NIS-direktivet. En upplysningsbestämmelse skulle enligt Datainspektionen understryka vikten av att dataskyddsbestämmelserna tillämpas när åtgärder enligt NIS-direktivet ger upphov till personuppgiftsbehandling.

Regeringen instämmer i att det är viktigt att personuppgiftsbehandling vid tillämpning av den nya lagen sker i enlighet med gällande dataskyddsreglering. Däremot ser regeringen inte behov av att i den nya lagen införa en bestämmelse som upplyser om gällande personuppgiftsreglering.

5.4 Undantag från lagens tillämpningsområde

5.4.1 Elektroniska kommunikationstjänster, betrodda tjänster och mikroföretag eller små företag

Regeringens förslag: Den nya lagen ska inte gälla för
- vissa leverantörer av elektroniska kommunikationsnät och kommunikationstjänster
- vissa leverantörer av betrodda tjänster
- leverantörer av digitala tjänster som är mikroföretag eller små företag.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningen har föreslagit att undantaget för leverantörer av elektroniska kommunikationstjänster inte ska omfatta företag som tillhandahåller internetknutpunkter.

Remissinstanserna: *IT & Telekomföretagen* och *Svenskt Näringsliv* tillstyrker att mikro- och småföretag undantas från den nya lagens tillämpningsområde. *Netnod*, *Svenska Stadsnätsföreningen* och *Föreningen Swedish Network Users Society* anser inte att företag som tillhandahåller internetknutpunkter i Sverige ska omfattas av den nya lagen. Samma remissinstanser anser att de som redan är skyldiga att tillämpa bestämmelser med motsvarande krav som finns i den nya lagen uttryckligen bör undantas från tillämpningsområdet.

Skälen för regeringens förslag

Leverantörer av elektroniska kommunikationstjänster

Enligt artikel 1.3 i NIS-direktivet ska bestämmelserna i direktivet 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 (ramdirektiv). Artikel 13a 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 överträdelser av säkerheten

eller integriteten som i betydande omfattning påverkade driften av nät och tjänster. Artikel 13b innehåller bestämmelser om tillämpning och genomförande. Artiklarna 13a och 13b har genomförts i svensk rätt genom 5 kap. 6 b och c §§ LEK.

Den nya lagen bör liksom direktivet inte vara tillämplig på företag som omfattas av kraven i nämnda artiklar i ramdirektivet. För att underlätta för de som ska tillämpa lagen anser regeringen att undantaget bör avse företag som omfattas av de svenska bestämmelserna som genomför artikeln i fråga.

Internetknutpunkter anses i svensk rätt utgöra sådana allmänna kommunikationsnät som omfattas av 5 kap. 6 b och c §§ LEK. Företag som tillhandahåller internetknutpunkter är samtidigt en av de typer av leverantörer inom sektorn digital infrastruktur som uttryckligen omfattas av NIS-direktivet (bilaga 2). Utredningen har därför föreslagit att undantaget för företag som omfattas av kraven i LEK inte ska gälla internetknutpunkter. För att förhindra att företag som tillhandahåller internetknutpunkter omfattas av två motsvarande regleringar om säkerhetsåtgärder och incidentrapportering anser regeringen dock, liksom *Netnod*, *Svenska Stadsnätsföreningen* och *Föreningen Swedish Network Users Society*, att undantaget även bör omfatta företag som tillhandahåller internetknutpunkter.

Leverantörer av betrodda tjänster

Enligt artikel 1.3 i NIS-direktivet ska direktivet inte heller 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, kallad eIDAS-förordningen.

Med betrodda tjänster avses enligt eIDAS-förordningen 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.

Den nya lagen bör liksom direktivet inte vara tillämplig på leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 i eIDAS-förordningen.

Hänvisningar till EU-rättsakter i författningar kan göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. En dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen. Utredningen har föreslagit en statisk hänvisning, närmare bestämt att undantaget i den nya lagen ska gälla för de som omfattas av artikel 19 i eIDAS-förordningens ursprungliga lydelse. För att

säkerställa att eventuella ändringar i eIDAS-förordningen kan få genomslag utan en ändring i den nya lagen anser regeringen dock att hänvisningen bör vara dynamisk, dvs. avse den vid var tid gällande lydelsen av artikeln.

Leverantörer av digitala tjänster som är mikroföretag eller små företag

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 (artikel 16.11). Enligt rekommendationen är ett mikroföretag ett företag med färre än 10 anställda och en årsomsättning eller balansomslutning som understiger 2 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. Det bör införas ett undantag i den nya lagen som innebär att lagen inte ska tillämpas på leverantörer av digitala tjänster som utgör små företag eller mikroföretag.

5.4.2 Säkerhetskänslig verksamhet

Regeringens förslag: Den nya lagen ska inte gälla för säkerhetskänslig verksamhet.

Utredningens förslag stämmer i sak överens med regeringens. Utredningen har föreslagit att undantaget ska avse verksamhet som är av betydelse för Sveriges säkerhet.

Remissinstanserna: *Säkerhetspolisen* och *Försvarsmakten* tillstyrker att verksamhet av betydelse för Sveriges säkerhet undantas från den nya lagens tillämpningsområde. Flera remissinstanser efterfrågar klargöranden om vad undantaget för verksamhet som är av betydelse för Sveriges säkerhet innebär. *Stockholms universitet* och *Affärsverket Svenska kraftnät* anser inte att verksamhet av betydelse för Sveriges säkerhet bör undantas från tillämpningsområdet.

Skälen för regeringens förslag: Enligt artikel 1.6 påverkar NIS-direktivet 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.

Säkerhetspolisen och *Försvarsmakten* anser, i likhet med utredningen, att verksamhet av betydelse för Sveriges säkerhet bör undantas från den nya lagens tillämpningsområde. Säkerhetspolisen framhåller särskilt att det är viktigt att incidenter som ska rapporteras enligt säkerhetsskyddsregleringen inte rapporteras enligt det föreslagna nya regelverket. Med beaktande av att begreppet samhällsviktig tjänst ofta kan ligga nära begreppet Sveriges säkerhet pekar Säkerhetspolisen dock på att det finns en risk att tillämpningsområdet för den nya lagen blir mindre än vad som är syftet med NIS-direktivet. *Stockholms universitet* och *Affärsverket Svenska kraftnät* anser inte att verksamhet som är av betydelse för Sveriges

säkerhet bör undantas från den nya lagens tillämpningsområde. Som skäl anför Stockholms universitet bl.a. att ett sådant undantag skulle motverka syftet med lagen; att säkra samhällsviktiga tjänster till gagn för Sveriges säkerhet.

Med hänsyn till behovet av skydd för verksamhet av betydelse för Sveriges säkerhet anser regeringen liksom utredningen att det är motiverat att undanta verksamhet som omfattas av säkerhetsskyddsregleringen, dvs. säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633), från den nya lagens tillämpningsområde. Regeringen anser alltså att behovet av skydd för säkerhetskänslig verksamhet väger tyngre än behovet av att skydda kontinuiteten i samhällsviktiga och digitala tjänster. Det kan dock poängteras att säkerhetsskyddsåtgärderna i säkerhetsskyddsregleringen i många fall indirekt även skyddar kontinuiteten i aktuella verksamheter.

Utredningen har föreslagit att undantaget bör formuleras på så sätt att den nya lagen inte ska gälla för verksamhet med betydelse för Sveriges säkerhet. Flera remissinstanser, bland dem *Försvarsmakten*, *Linköpings kommun*, *Luftfartsverket*, *Netnod*, *SJ AB*, *Skåne läns landsting*, *Affärsverket Svenska kraftnät*, *Svenska Stadsnätsföreningen* och *Skåne läns landsting*, önskar klargörande av vilka som omfattas av undantaget. *Säkerhetspolisen* pekar på att otydlig gränsdragning mot säkerhetsskyddet bl.a. kan leda till tillämpningsproblem som i sin tur gör att exempelvis incidentrapporter skickas till fel myndighet. *Försvarsmakten* anser att den nuvarande säkerhetsskyddsregleringen inte ensamt kan anses utgöra det undantagna området, utan att även system som inte innehåller hemliga uppgifter men vars funktion eller tillgänglighet är av avgörande betydelse för totalförsvaret eller det militära försvaret bör ingå. Vidare pekar Försvarsmakten på att Utredningen om säkerhetsskyddslagen i sitt betänkande, SOU 2015:25, föreslår en ny säkerhetsskyddslag som kommer omfatta sådana system.

Som ovan anförts anser regeringen att undantaget bör avse verksamhet som omfattas av säkerhetsskyddsregleringen. Som remissinstanserna påpekar är det viktigt att undantaget är tydligt för att undvika tillämpningsproblem. Med hänsyn till det bör undantagsbestämmelsen uttryckligen hänvisa till säkerhetsskyddsregleringen. Bestämmelsen bör formuleras på så sätt att den nya lagen inte ska gälla för verksamhet som omfattas av krav på säkerhetsskydd enligt säkerhetsskyddslagen. Det innebär bl.a. att kraven på säkerhetsåtgärder och incidentrapportering enligt den nya lagen inte ska gälla för offentlig och enskild verksamhet som omfattas av krav på säkerhetsskydd. Det innebär också att incidenter som i dag ska rapporteras enligt 10 a § säkerhetsskyddsförordningen även fortsättningsvis ska rapporteras enligt den förordningen.

Som ovan nämnts har regeringen i propositionen Ett modernt och stärkt skydd för Sveriges säkerhet (prop. 2017/18:89) lämnat förslag på en ny säkerhetsskyddslag som ska träda i kraft den 1 april 2019. När den träder i kraft bör undantaget från den nya lagen anpassas till att avse verksamhet som omfattas av den nya säkerhetsskyddslagen.

Det bör poängteras att den omständigheten att en leverantör av samhällsviktiga eller digitala tjänster bedriver viss verksamhet som omfattas av säkerhetsskyddsregleringen inte nödvändigtvis innebär att hela

leverantörens verksamhet är undantagen. Om en annan del av leverantörens verksamhet inte är säkerhetskänslig kan den nya lagen vara tillämplig i de delarna. En leverantör av samhällsviktiga eller digitala tjänster kan därför, såsom vissa remissinstanser också påpekar, behöva tillämpa säkerhetsskyddsregleringen i en del av sin verksamhet och den nya lagen i en annan del av verksamheten.

5.4.3 Bestämmelser om informationssäkerhet i andra författningar

Regeringens förslag: Om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder och incidentrapportering, ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt den nya lagen.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningen har till skillnad från regeringen även föreslagit att enskilda bestämmelser om säkerhetsåtgärder eller incidentrapportering ska tillämpas framför motsvarande bestämmelser i den nya lagen om de minst har motsvarande verkan.

Remissinstanserna: *Netnod*, *Svenska Stadsnätsföreningen* och *Föreningen Swedish Network Users Society* anser att de leverantörer som redan omfattas av adekvata krav på säkerhetsåtgärder och incidentrapportering uttryckligen bör undantas från den nya lagens tillämpningsområde.

Skälen för regeringens förslag: Vissa sektorer, t.ex. sjöfartssektorn, banksektorn och sektorn för finansmarknadsinfrastruktur, regleras redan av sektorsspecifika EU-rättsakter som innehåller bestämmelser om säkerhetsåtgärder och incidentrapportering. Enligt artikel 1.7 i NIS-direktivet ska bestämmelser i sektorsspecifika EU-rättsakter, som innehåller krav på leverantörer av samhällsviktiga eller digitala tjänster att säkerställa säkerheten i sina nätverk och informationssystem eller att rapportera incidenter, tillämpas i stället för bestämmelserna i direktivet förutsatt att verkan av kraven i fråga minst motsvarar verkan av skyldigheterna enligt direktivet. I den nya lagen bör det införas en motsvarande bestämmelse om att den nya lagens bestämmelser inte ska tillämpas när det i annan författning finns bestämmelser om säkerhetsåtgärder och incidentrapportering vars verkan minst motsvarar skyldigheterna enligt den nya lagen. Undantaget bör gälla oavsett om bestämmelserna finns i EU-rättsakter eller i nationella författningar. *Netnod*, *Svenska Stadsnätsföreningen* och *Föreningen Swedish Network Users Society* anser att organisationer som redan i dag täcks av adekvata krav på säkerhetsåtgärder och incidentrapportering uttryckligen bör undantas från den nya lagens tillämpningsområde. Regeringen anser dock inte att det är lämpligt att införa fler uttryckliga undantag från lagens tillämpningsområde än de som finns i direktivet.

Vid bedömningen av om bestämmelser om säkerhetsåtgärder och incidentrapportering motsvarar verkan av skyldigheterna enligt den nya lagen, bör man bl.a. beakta bestämmelsernas omfattning och syfte samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna. Exempelvis skiljer sig bestämmelserna om säkerhetsåtgärder och incidentrapportering i förordningen om krisberedskap och

bevakningsansvariga myndigheters åtgärder vid höjd beredskap samt dataskyddsförordningen från den nya lagens bestämmelser på ett sådant sätt att de inte kan anses ha en motsvarande verkan. Leverantörer kan således behöva tillämpa dessa regelverk parallellt.

Till skillnad från utredningen anser regeringen inte att enstaka bestämmelser som innehåller krav på säkerhetsåtgärder eller incidentrapportering ska gälla i stället för motsvarande bestämmelser i den nya lagen. En sådan ordning vore inte ändamålsenlig. Dessutom finns det endast i mycket begränsad omfattning nationella bestämmelser som innehåller krav som kan anses motsvara kraven enligt NIS-direktivet.

5.5 Leverantörer av digitala tjänster ska i vissa fall utse en företrädare

Regeringens förslag: En juridisk person som erbjuder digitala tjänster i Sverige men som inte har sitt huvudsakliga etableringsställe inom EU ska utse en företrädare som är etablerad i en medlemsstat där tjänsterna erbjuds.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningens förslag innefattar inte krav på att företrädaren måste vara etablerad i en medlemsstat där tjänsterna erbjuds.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens förslag: Den nya lagen ska enligt regeringens förslag i avsnitt 5.3 omfatta leverantörer av digitala tjänster som har sitt huvudsakliga etableringsställe i Sverige eller som har utsett en företrädare som är etablerad här.

En leverantör av digitala tjänster som inte är etablerad inom EU men erbjuder tjänster inom unionen ska, enligt artikel 18.2 i NIS-direktivet, utse en företrädare som är etablerad i någon av de medlemsstater där tjänsterna erbjuds. En motsvarande bestämmelse bör införas i den nya lagen. Eftersom begreppet leverantör av digitala tjänster i den nya lagen, enligt regeringens förslag i avsnitt 5.3, avser leverantörer som har sitt huvudsakliga etableringsställe i Sverige eller som har utsett en företrädare som är etablerad här, bör bestämmelsen utformas så att skyldigheten avser juridiska personer som erbjuder digitala tjänster i Sverige men som inte har sitt huvudsakliga etableringsställe inom EU. Skyldigheten att utse en företrädare bör i enlighet med direktivet endast gälla om något undantag från lagens tillämpningsområde inte är tillämpligt.

En leverantör kan i enlighet med artikel 4.10 i direktivet utse en juridisk eller fysisk person som företrädare. Företrädaren ska utses uttryckligen och kunna agera på leverantörens vägnar i frågor som gäller de skyldigheter som leverantören har enligt NIS-direktivet.

För att fastställa om en leverantör erbjuder digitala tjänster inom EU bör i enlighet med skälen till direktivet det avgörande vara om det är uppenbart att leverantören har för avsikt att erbjuda tjänster till personer i en eller flera medlemsstater (skäl 65). Enbart den omständigheten att en leverantör använder sig av en webbplats som är tillgänglig inom EU är inte tillräckligt

för att fastställa en sådan avsikt. I enlighet med skälen till direktivet kan dock faktorer som att en leverantör använder sig av ett annat språk än det som används allmänt där leverantören är etablerad, men som används i en eller flera medlemsstater, och att det finns möjlighet att beställa tjänster på detta andra språk göra det uppenbart att leverantören planerar att erbjuda tjänster inom unionen.

Om en juridisk person erbjuder digitala tjänster i Sverige men inte har sitt huvudsakliga etableringsställe inom EU, ska denne alltså uttryckligen utse en företrädare som är etablerad i en medlemsstat där tjänsterna erbjuds. Om leverantören utser en företrädare som är etablerad i Sverige innebär det att leverantören är en sådan leverantör av digitala tjänster som omfattas av övriga bestämmelser i den nya lagen.

5.6 Uttryck i lagen

Regeringens förslag: Vissa uttryck som används i den nya lagen ska definieras. Definitionerna ska motsvara de som finns i NIS-direktivet.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen har till skillnad från regeringen föreslagit att uttryck som inte används i den nya lagen ska definieras och att fler uttryck än de som definieras i NIS-direktivet ska definieras i den nya lagen.

Remissinstanserna: Några remissinstanser anser att den nya lagen bör innehålla definitioner som är bättre anpassade till svenska förhållanden än motsvarande definitioner i NIS-direktivet.

Skälen för regeringens förslag: I artikel 4 i NIS-direktivet finns en lista med definitioner av uttryck som direkt eller indirekt används i direktivet. Motsvarande uttryck bör även definieras i den nya lagen under förutsättning att de ska användas i lagen. Till skillnad från vad utredningen har föreslagit anser regeringen alltså inte att uttryck som enbart ska finnas i förordning bör definieras i den nya lagen.

Det behöver inte heller – såsom utredningen föreslagit – införas någon definition av NIS-direktivet. Innebörden kommer att framgå med tillräcklig tydlighet av den nya lagens inledande bestämmelse.

Ett antal remissinstanser, t.ex. *Finansinspektionen*, anser att den nya lagen bör innehålla definitioner som i någon mån avviker från motsvarande definitioner i direktivet för att harmonisera med befintliga begrepp på nationell nivå.

För att säkerställa att begreppen i den nya lagen vid tillämpningen får samma betydelse som i direktivet anser regeringen att definitionerna som utgångspunkt inte bör avvika från motsvarande definitioner i direktivet för att passa in i en nationell kontext. När det gäller direktivets definition av uttrycket ”säkerhet i nätverk 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 […]”) bör dock ordet integritet ersättas med ordet autenticitet för att stämma överens med etablerad svensk terminologi. Av den engelska versionen av NIS-direktivet (”ability of network and information systems to resist, at a given level of confidence, any action that compromises the

availability, authenticity, integrity or confidentiality […]") framgår också att det utöver grundbegreppen som definierar informationssäkerhet – tillgänglighet, riktighet och konfidentialitet – inte är integritet som avses utan autenticitet.

6 Identifiering av leverantörer av samhällsviktiga tjänster

6.1 Inledande om NIS-direktivets krav på identifiering av leverantörer av samhällsviktiga tjänster

Medlemsstaterna ska, för varje sektor som NIS-direktivet omfattar, identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium. I direktivet påtalas vikten av ett enhetligt tillvägagångssätt och en konsekvent tillämpning i alla medlemsstater.

Vid förfarandet för identifiering ska medlemsstaterna först upprätta en förteckning över de tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, dvs. vad som utgör samhällsviktiga tjänster. Därefter ska medlemsstaterna bedöma vilka leverantörer som uppfyller kraven i direktivet för att anses vara leverantörer av samhällsviktiga tjänster.

Förteckningen över samhällsviktiga tjänster 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 som har identifierats i varje sektor och en uppgift om deras betydelse för sektorn ska inom samma tid lämnas till kommissionen.

6.2 Förteckning över samhällsviktiga tjänster

Regeringens förslag: Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vilka tjänster som utgör samhällsviktiga tjänster enligt den nya lagen.

Utredningens förslag stämmer i huvudsak överens med regeringens förslag. Utredningen har bedömt att det inte krävs ett bemyndigande för föreskrifter om vad som utgör samhällsviktiga tjänster.

Remissinstanserna: *Stockholms läns landsting* anser att det behövs en fördjupad genomgång av vad som kan anses vara samhällsviktigt och skyddsvärt inom hälso- och sjukvården innan någon myndighet får i uppdrag att bedöma vilka tjänster som är samhällsviktiga.

Skälen för regeringens förslag

NIS-direktivets krav på att upprätta en förteckning

Medlemsstaterna ska i ett första steg av identifieringsförfarandet upprätta en förteckning över samhällsviktiga tjänster som tillhandahålls av en sådan typ av leverantör som anges i bilaga 2 till NIS-direktivet (artikel 5.1 och 5.3).

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 (skäl 23). Vidare ska förteckningen utgöra grund för bedömningen av om en leverantör tillhandahåller en samhällsviktig tjänst. Vid den bedömningen ska det vara tillräckligt att undersöka om leverantören tillhandahåller en tjänst som finns upptagen i förteckningen (skäl 20).

Förteckningen tydliggör även medlemsstaternas respektive praxis när det gäller vad som utgör samhällsviktiga tjänster och kan därför användas för att säkerställa en övergripande enhetlighet i medlemsstaternas tillämpning (skäl 23). Den samarbetsgrupp som har inrättats genom direktivet ska hjälpa medlemsstaterna att tillämpa ett enhetligt tillvägagångssätt i förfarandet för identifieringen av samhällsviktiga tjänster (artiklarna 5.6 och 11.3 l). Samarbetsgruppen består av företrädare för medlemsstaterna, kommissionen och Enisa (EU:s nätverks- och informationssäkerhetsbyrå, artikel 11.2). Sverige företräds av Myndigheten för samhällsskydd och beredskap (MSB).

Vad avses med samhällsviktig tjänst?

Uttrycket samhällsviktig tjänst förekommer inte i svensk lagstiftning. I stället används andra närliggande uttryck såsom samhällsviktig verksamhet. Uttrycket samhällsviktig verksamhet används bl.a. i risk- och sårbarhetsanalysarbetet, vilket är en viktig del i statliga myndigheters krisberedskapsarbete. I MSB:s föreskrifter och allmänna råd om risk- och sårbarhetsanalyser (MSBFS 2015:4, MSBFS 2015:5 och MSBFS 2015:6) definieras uttrycket samhällsviktig verksamhet som en verksamhet som uppfyller minst ett av två villkor. Det första är att ett bortfall av eller en svår störning i verksamheten ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid kan leda till att en allvarlig kris inträffar i samhället. Det andra är att verksamheten ska vara 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 anges att med samhällsviktig verksamhet menas tjänster som är av avgörande betydelse för upprätthållandet av viktiga samhällsfunktioner såsom produktion och distribution av el, produktion och distribution av bränslen och drivmedel, läkemedels- och materielförsörjning, smittskydd för djur och människor, dricksvattenförsörjning, avloppshantering, väghållning och kollektivtrafik.

Vid bedömningen av om en tjänst är samhällsviktig kan ledning hämtas i de avvägningar som görs för att bedöma om en verksamhet är samhällsviktig. Det är dock viktigt att vara medveten om de olika regelverkens utgångspunkter. Regelverket om krisberedskap avser att skydda funk-

tioner som absolut behövs för upprätthållandet av viktiga samhällsfunktioner vid allvarliga händelser eller kriser. 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 bl.a. att uttrycket samhällsviktig tjänst kan omfatta fler funktioner än uttrycket samhällsviktig verksamhet.

Eftersom ett syfte med förteckningen är att säkerställa en övergripande enhetlighet mellan medlemsstaternas bedömning av samhällsviktiga tjänster, bör även beaktas hur andra medlemsstater gör sina bedömningar av vad som utgör samhällsviktiga tjänster. Medlemsstaternas bedömning av vad som utgör samhällsviktiga tjänster diskuteras som nämnts i den samarbetsgrupp som har inrättats genom direktivet och i vilken MSB företräder Sverige.

Som exempel på tjänster som kan anses som samhällsviktiga kan nämnas elöverföring, överföring och lagring av naturgas, infrastrukturförvaltning av järnväg, vattenförsörjning och tillhandahållande och förvaltning av internetdomännamn.

Utgångspunkten är att MSB ska upprätta en förteckning över samhällsviktiga tjänster

Sedan MSB grundades har myndigheten årligen fått uppdrag i regleringsbrev att redovisa en nationell bedömning av samhällets förmågor, risker, sårbarheter samt identifierade och genomförda åtgärder avseende krisberedskapen. I MSB:s uppdrag ingår också att stödja och samordna arbetet med samhällets informationssäkerhet samt att analysera och bedöma omvärldsutvecklingen inom området. Myndigheten har vidare en samordnande roll inom ramen för samhällets krisberedskap och en central funktion i de nätverk som finns inom krisberedskapsområdet. Dessutom har MSB genom sina uppdrag ett etablerat kontaktnät med merparten av de aktörer som kommer att beröras av bestämmelserna i NIS-direktivet.

Regeringen bedömer i likhet med utredningen att MSB, genom sitt uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet, är den myndighet som i nuläget är bäst lämpad att identifiera vilka samhällsviktiga tjänster som finns i Sverige inom de sektorer som omfattas av direktivet. Det kan poängteras att ingen remissinstans har uttryckt någon annan uppfattning. *Stockholms läns landsting* framför dock att det behövs mer precisa beskrivningar, särskilt när det gäller hälso- och sjukvården, för att MSB på ett bra sätt ska kunna identifiera vilka tjänster som kan anses vara samhällsviktiga. Regeringen bedömer emellertid att MSB genom sitt uppdrag har en sådan övergripande kännedom om de sektorer som direktivet omfattar, att MSB i vart fall med stöd av sektorsspecifika myndigheter kan upprätta förteckningen.

En förutsättning för att den nya lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ska kunna tillämpas vid ikraftträdandet är att förteckningen över samhällsviktiga tjänster då är sammanställd. Mot denna bakgrund och på inrådan av utredningen gav regeringen i slutet av

juni 2017 MSB i uppdrag att upprätta förteckningen med stöd av myndigheter med sektorsspecifik kunskap. MSB redovisade uppdraget den 15 januari 2018.

Förteckningen bör meddelas i form av föreskrifter. Enligt regeringens bedömning kommer föreskrifterna att behöva gå utöver vad regeringen eller den myndighet som regeringen bestämmer kan meddela med stöd av 8 kap. 7 § regeringsformen. Det bör därför införas ett bemyndigande i den nya lagen. Även om utgångspunkten är att MSB ska upprätta förteckningen bör det inte slås fast i den nya lagen utan regleras i förordning. Anledningen till det är att regeringen vid behov bör kunna ändra vilken myndighet som ska upprätta förteckningen. I den nya lagen bör det därför införas ett bemyndigande om att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka tjänster som är samhällsviktiga tjänster enligt lagen.

6.3 Bedömning av vilka leverantörer av samhällsviktiga tjänster som är etablerade i Sverige

Regeringens förslag: Leverantörer av samhällsviktiga tjänster ska utan dröjsmål anmäla sig till tillsynsmyndigheten. Av en anmälan ska det framgå om leverantören tillhandahåller samhällsviktiga tjänster i två eller flera medlemsstater inom EU.

Det ska i den nya lagen upplysas om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om verkställighet av den nya lagen.

Regeringens bedömning: Övriga bestämmelser om hur identifieringen av de leverantörer av samhällsviktiga tjänster som är etablerade i Sverige ska fullgöras bör meddelas i förordning eller myndighetsföreskrifter.

Utredningens förslag stämmer i huvudsak överens med regeringens förslag och bedömning. Utredningen har föreslagit att det i den nya lagen ska införas en bestämmelse om att de som tillhandahåller samhällsviktiga tjänster är skyldiga att undersöka om de omfattas av den nya lagen. Vidare har utredningen föreslagit att Sveriges skyldighet att i vissa fall samråda med andra medlemsstater innan beslut om identifiering fattas till viss del ska regleras i den nya lagen. Utredningen har inte föreslagit att leverantörer av samhällsviktiga tjänster ska anmäla sig till tillsynsmyndigheten och därvid även ange om de tillhandahåller samhällsviktiga tjänster i två eller flera medlemsstater.

Remissinstanserna: *Stiftelsen för internetinfrastruktur* och *Stockholms universitet* instämmer i att det bör åläggas de som tillhandahåller samhällsviktiga tjänster att undersöka om de omfattas av lagen. *Livsmedelsverket* och *MSB* anser att det bör införas en skyldighet för leverantörerna att anmäla sig till tillsynsmyndigheten om de anser sig uppfylla kraven för att omfattas av den nya lagen.

Skälen för regeringens förslag och bedömning

NIS-direktivets krav på bedömningen av vilka som är leverantörer av samhällsviktiga tjänster

Som framgår ovan ska medlemsstaterna, i ett första steg för att identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium, upprätta en förteckning över samhällsviktiga tjänster.

Det andra steget i identifieringsförfarandet är att bedöma vilka och följaktligen identifiera de leverantörer som uppfyller kraven i direktivet för att anses vara leverantörer av samhällsviktiga tjänster. För Sveriges del kommer det i praktiken handla om att fastställa vilka leverantörer av samhällsviktiga tjänster som omfattas av den nya lagen. Kriterierna för bedömningen är således att det är fråga om en leverantör som tillhandahåller en samhällsviktig tjänst, att leverantören är etablerad i Sverige samt att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten (artikel 5.2).

Tillhandahålls tjänsten i två eller flera medlemsstater ska berörda medlemsstater samråda med varandra. Detta samråd ska äga rum innan beslut om identifiering fattas (artikel 5.4).

Vid bedömningen av om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten ska medlemsstaterna beakta ett antal sektorsöverskridande faktorer och, i lämpliga fall, sektorsspecifika faktorer (artikel 6.2). Som framgår av avsnitt 5.3 kommer föreskrifter om vad som avses med en betydande störning att meddelas i förordning eller myndighetsföreskrifter. Föreskrifterna kommer i praktiken att utgöra tröskelvärden för vilka som är att anse som leverantörer av samhällsviktiga tjänster. Tröskelvärden för energileverantörer kan exempelvis avse mängden eller andelen av producerad nationell el, och för leverantörer inom hälso- och sjukvårdssektorn antalet patienter som leverantören vårdar per år.

Hur ska bedömningen gå till?

Medlemsstaterna kan välja att genomföra detta steg av identifieringsförfarandet på olika sätt. Genomförandet kan exempelvis ske genom upprättandet av ytterligare en förteckning som innehåller alla leverantörer av samhällsviktiga tjänster, eller genom antagandet av nationella bestämmelser som gör det möjligt att fastställa vilka leverantörer som omfattas av skyldigheterna i direktivet (skäl 25).

Utredningen har föreslagit att leverantörer som tillhandahåller samhällsviktiga tjänster ska åläggas att undersöka om de omfattas av den nya lagen och följaktligen om de bör identifieras som en leverantör av samhällsviktiga tjänster. Utredningen framhåller särskilt att bedömningen av vilka som är att anse som leverantörer av samhällsviktiga tjänster kräver verksamhetskunskap och att de flesta offentliga leverantörer inom de sektorer och delsektorer som anges i NIS-direktivet redan gör analyser utifrån liknande krav. Regeringen konstaterar dock att en sådan skyldighet som utredningen har föreslagit indirekt redan kommer att finnas genom den nya lagen. Leverantörer som tillhandahåller samhällsviktiga tjänster måste undersöka om de omfattas av den nya lagen för att få klarhet i om de har en skyldighet att vidta säkerhetsåtgärder och rapportera incidenter.

Vidare skulle ett sådan undersökningsskyldighet som utredningen har föreslagit innebära att ett stort antal leverantörer som tillhandahåller samhällsviktiga tjänster men som uppenbarligen inte är leverantörer av samhällsviktiga tjänster, exempelvis för att det står klart att en incident inte skulle medföra en betydande störning enligt de tröskelvärden som antagits, måste genomföra undersökningen. Regeringen anser mot den bakgrunden inte att det bör införas en skyldighet för de som tillhandahåller samhällsviktiga tjänster att undersöka om de omfattas av den nya lagen.

Däremot bör det övervägas om de som omfattas av den nya lagen ska åläggas att anmäla sig till tillsynsmyndigheten. *Livsmedelsverket* och *MSB* anser att det bör införas en anmälningsplikt, bl.a. för att det underlättar identifieringen. Myndigheterna anser också att en anmälningsplikt är nödvändig för att tillsynsmyndigheten ska veta vilka tillsynsobjekt den har. Med hänsyn både till behovet av att underlätta identifieringen av de leverantörer av samhällsviktiga tjänster som är etablerade i Sverige och till att tillsynsmyndigheten ska kunna utföra sitt tillsynsuppdrag på ett fullgott sätt anser regeringen att det i den nya lagen bör införas en bestämmelse om att leverantörer av samhällsviktiga tjänster utan dröjsmål ska anmäla sig till tillsynsmyndigheten. I bestämmelsen bör även anges att det av anmälan ska framgå om leverantören tillhandahåller samhällsviktiga tjänster i två eller flera medlemsstater, för att på så sätt underlätta bedömningen av om ett samråd med andra medlemsstater enligt artikel 5.4 ska ske innan ett beslut om identifiering fattas. Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om vilken information som en anmälan ska innehålla liksom föreskrifter om de närmare formerna för fullgörandet av anmälningsskyldigheten. För att upplysa om att det i anslutning till den nya lagen kan komma att meddelas verkställighetsföreskrifter, såsom bl.a. föreskrifter om anmälningsskyldigheten, bör den nya lagen innehålla en bestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om verkställighet av lagen.

Det behövs även andra föreskrifter för att fullgöra skyldigheten att bedöma och följaktligen identifiera vilka leverantörer av samhällsviktiga tjänster som är etablerade i Sverige. Det kan t.ex. vara fråga om bestämmelser om vilken eller vilka myndigheter som ska ansvara för identifieringen, hur processen närmare ska gå till och hur uppgifterna om vilka leverantörer som är identifierade ska hållas aktuella och läggas till grund för information till kommissionen. Vidare krävs att identifieringsprocessen genomför skyldigheten att enligt artikel 5.4 samråda med andra medlemsstater i vissa fall innan beslut om identifiering fattas. Utredningen har föreslagit att sistnämnda skyldighet bör regleras i den nya lagen. Regeringen anser dock att sådana bestämmelser, liksom andra föreskrifter som behövs för att fullgöra kraven på identifiering enligt direktivet, bör meddelas i förordning eller myndighetsföreskrifter.

7 Säkerhetsåtgärder och incidentrapportering för leverantörer av samhällsviktiga tjänster

NIS-direktivet ställer krav på leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster att vidta vissa säkerhetsåtgärder och att rapportera vissa incidenter.

I detta avsnitt behandlas kraven på leverantörer av samhällsviktiga tjänster. Kraven på leverantörer av digitala tjänster behandlas i avsnitt 8.

7.1 Säkerhetsåtgärder

7.1.1 Befintliga bestämmelser om säkerhetsåtgärder är inte tillräckliga

Regeringens bedömning: NIS-direktivet kräver nya bestämmelser om säkerhetsåtgärder.

Utredningens bedömning stämmer överens med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över bedömningen.

Skälen för regeringens bedömning: Enligt NIS-direktivet ska leverantörer av samhällsviktiga tjänster vidta säkerhetsåtgärder till skydd för säkerheten i nätverk och informationssystem.

Vissa leverantörer av samhällsviktiga tjänster som omfattats av NIS-direktivet omfattas redan i dag av rättsliga krav på säkerhetsåtgärder i nätverk och informationssystem. Exempelvis ska statliga myndigheter enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap se till att deras informationssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. För verksamhet som är av betydelse för Sveriges säkerhet finns i säkerhetsskyddsregleringen krav på att förebygga att uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Vidare finns mer sektorsspecifika bestämmelser i vissa av de sektorer som omfattas av NIS-direktivet. Inom sektorn finansmarknadsinfrastruktur finns exempelvis krav i lagen (2007:528) om värdepappersmarknaden på börser, dvs. företag som har fått tillstånd att driva en reglerad marknad, att identifiera och hantera de risker som kan uppstå i verksamheten och att ha säkra tekniska system. För samtliga leverantörer som omfattas av NIS-direktivet finns även krav i personuppgiftsregleringen på tekniska och organisatoriska åtgärder när det gäller personuppgiftsbehandling.

Befintlig reglering är inte heltäckande och i vissa fall är syftet med säkerhetsåtgärderna ett annat än det som anges i NIS-direktivet. Regeringens bedömning är därför att det måste införas bestämmelser med krav på säkerhetsåtgärder i den nya lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

7.1.2 Ett systematiskt arbete

Regeringens förslag: Leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandhålla samhällsviktiga tjänster.

Utredningens förslag stämmer i sak överens med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens förslag: Regeringen anser att en förutsättning för en väl anpassad säkerhet i nätverk och informationssystem är att det bedrivs ett systematiskt och riskbaserat informationssäkerhetsarbete. Föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete finns i dag för statliga myndigheter i Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet, MSBFS 2016:1. Ett systematiskt informationssäkerhetsarbete innebär bl.a. att arbetet bedrivs långsiktigt, kontinuerligt och metodiskt samt att det finns en tydlig rollfördelning med särskilt utpekat ansvar. På så vis kan verksamhetens ledning på ett systematiskt sätt styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering. En del i detta arbete är olika typer av analyser, t.ex. verksamhetsanalys, riskanalys och GAP-analys (analys som jämför nuvarande säkerhetsnivå med den önskade).

Mot denna bakgrund anser regeringen liksom utredningen att det bör införas krav på leverantörer av samhällsviktiga tjänster att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Till skillnad från utredningen anser regeringen dock att lagbestämmelsen bör utformas på så sätt att det tydligt framgår att kravet endast avser sådana nätverk och informationssystem som en leverantör använder för att tillhandahålla samhällsviktiga tjänster.

7.1.3 Riskanalys

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

Utredningens förslag stämmer överens med regeringens.

Remissinstanserna: *Norrköpings kommun* och *Svenskt vatten* tillstyrker förslaget. *Stockholms universitet* avstyrker förslaget och anser i stället att leverantörerna bör få välja vilken sorts analys som är lämplig att göra och om en åtgärdsplan ska ingå i analysen. *Jönköpings läns landsting* anser inte att riskanalyser ska behöva uppdateras så ofta som årligen.

Skälen för regeringens förslag: NIS-direktivets krav på säkerhetsåtgärder innebär i stort att leverantörer av samhällsviktiga tjänster ska vidta vissa ändamålsenliga och proportionella åtgärder för att hantera säkerhetsrisker i nätverk och informationssystem, se avsnitt 7.1.4 och

7.1.5. För att en leverantör ska kunna identifiera vilka åtgärder som är relevanta anser regeringen liksom utredningen att det är nödvändigt att leverantören genomför en riskanalys. *Stockholms universitet* anser att en leverantör ska få välja vilken sorts analys som är lämplig att göra i leverantörens verksamhet. Eftersom de säkerhetsåtgärder som NIS-direktivet ålägger leverantörer att vidta har till syfte att hantera risker är det emellertid en riskanalys som är relevant för att åstadkomma kvalitativa bedömningar av vilka säkerhetsåtgärder som är lämpliga. Leverantörer som tillhandahåller samhällsviktiga tjänster bör därför åläggas att göra en sådan analys som ska ligga till grund för valet av säkerhetsåtgärder.

För att riskanalysen ska bli ett beslutsstöd för prioriteringar och avvägningar mellan olika typer av säkerhetsåtgärder bör den innehålla beskrivningar och bedömningar av relevanta hot och risker. Den bör även innehålla bedömningar av hur effektiva befintliga säkerhetsåtgärder är i förhållande till riskerna. Dessutom bör det av analysen framgå vilka negativa konsekvenser en incident skulle kunna medföra. Som *Säkerhetspolisen* påpekar finns det inget som hindrar att arbetet med riskanalysen samordnas och integreras med sådant riskanalysarbete som sker enligt annan lagstiftning.

Stockholms universitet anser att leverantören bör få välja om en åtgärdsplan ska ingå i riskanalysen. *Jönköpings län* anser inte att leverantörer ska åläggas att uppdatera riskanalysen årligen utan vid behov. För att riskanalysen ska bli ett reellt och levande verktyg i arbetet med att vidta lämpliga säkerhetsåtgärder anser regeringen dock att analysen bör dokumenteras, innehålla en åtgärdsplan och uppdateras årligen. Ett sådant åliggande bör därför också föras in i den nya lagen.

7.1.4 Tekniska och organisatoriska åtgärder

Regeringens förslag: 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 för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till risken.

Utredningens förslag stämmer i sak överens med regeringens.

Remissinstanserna: *E-hälsomyndigheten* och *Stockholms universitet* tillstyrker förslaget. *Göteborgs kommun* vill att det tydliggörs vad syftet med säkerhetsåtgärder enligt NIS-direktivet är. Vissa remissinstanser pekar på att förslaget kan innebära omfattande åligganden för leverantörerna.

Regeringens bedömning: Enligt artikel 14.1 i NIS-direktivet ska leverantörer av samhällsviktiga tjänster 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.

Göteborgs kommun efterfrågar ett tydliggörande av vad syftet med säkerhetsåtgärderna enligt direktivet är. Syftet med åtgärderna är att säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till risken. 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 (artikel 4.2). Med risk avses en rimlig identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i nätverk och informationssystem (artikel 4.9). För säkerhetsåtgärden incidenthantering, se avsnitt 7.1.5, är syftet att säkerställa kontinuiteten i de tillhandahållna tjänsterna.

En bestämmelse som motsvarar artikel 14.1 i NIS-direktivet bör införas i den nya lagen. Att en sådan bestämmelse, såsom bl.a. *Tågoperatörerna* påpekar, kommer att innebära åligganden för leverantörerna kan inte föranleda någon annan bedömning.

I kravet på att vidta tekniska åtgärder kan ingå 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. I organisatoriska åtgärder kan bl.a. ingå att upprätta styrdokument, utforma rutiner, övervaka efterlevnad och genomföra uppföljningar.

Att leverantörens skyldighet att vidta åtgärder avser nätverk och informationssystem som leverantören använder, innebär i enlighet med skälen till direktivet att säkerhetskraven gäller oavsett om leverantören sköter underhållet av sina nätverk och informationssystem internt eller lägger ut uppgifterna på entreprenad (skäl 52).

Vid bedömningen av vad som är en lämplig nivå i förhållande till risken ska enligt NIS-direktivet bl.a. den senaste tekniska utvecklingen beaktas. Det innebär att leverantören ska beakta samtliga tekniska lösningar som vid var tid finns tillgängliga på marknaden. Teknisk utveckling kan därför dels medföra att behovet av säkerhetsåtgärder förändras, dels innebära nya möjligheter att vidta effektiva säkerhetsåtgärder. Kravet på att beakta den tekniska utvecklingen behöver enligt regeringens mening inte uttryckas i den nya lagen, utan ingår i att säkerhetsåtgärderna ska uppnå en lämplig säkerhetsnivå.

Med hänsyn till att vad som utgör en lämplig nivå på säkerheten i nätverk och informationssystem kan ändras över tid, exempelvis genom förändringar i den föreliggande risken eller genom nya tekniska lösningar, behöver leverantörer av samhällsviktiga tjänster regelbundet och vid behov se över vilka säkerhetsåtgärder som är lämpliga att vidta.

7.1.5 Incidenthantering

Regeringens förslag: Leverantörer av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

Utredningens förslag stämmer i sak överens med regeringens.

Remissinstanserna tillstyrker eller har inga invändningar mot förslaget.

Skälen för regeringens förslag: Enligt artikel 14.2 i NIS-direktivet ska leverantörer av samhällsviktiga tjänster 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.

En motsvarande bestämmelse bör införas i den nya lagen. Det innebär att leverantörer av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga incidenter och dess verkningar och för att begränsa en inträffad incidents verkan, i syfte att säkerställa kontinuiteten i de tillhandahållna tjänsterna. I arbetet med incidenthantering är det viktigt att dra lärdom av inträffade incidenter. Om en incident har inträffat bör det som regel medföra att säkerhetsåtgärderna skyndsamt ses över.

7.1.6 Ytterligare föreskrifter om säkerhetsåtgärder

Regeringens förslag: Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vad som krävs av leverantörer av samhällsviktiga tjänster för att de ska uppfylla kraven på säkerhetsåtgärder.

Regeringens bedömning: Bestämmelser som främjar användningen av europeiska eller internationellt accepterade standarder och specifikationer av relevans för säkerhetsåtgärder bör meddelas i förordning eller myndighetsföreskrifter.

Utredningens förslag stämmer i huvudsak överens med regeringens förslag och bedömning. Utredningen har till skillnad från regeringen endast föreslagit ett bemyndigande för föreskrifter om ett systematiskt och riskbaserat informationssäkerhetsarbete.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens förslag och bedömning: Det krävs relativt omfattande och detaljerade föreskrifter om vad leverantörer av samhällsviktiga tjänster ska göra för att fullgöra de ovan föreslagna kraven på säkerhetsåtgärder. Sådana föreskrifter bör meddelas i förordning eller myndighetsföreskrifter. Regeringen bedömer att det utöver möjligheten att meddela verkställighetsföreskrifter behövs ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer. Till skillnad från utredningen anser regeringen att ett bemyndigande behövs inte bara för föreskrifter om kravet på ett systematiskt och riskbaserat informationssäkerhetsarbete, utan även för övriga krav på säkerhetsåtgärder. Anledningen till det är att föreskrifter om exempelvis tekniska och organisatoriska säkerhetsåtgärder avses mer i detalj innehålla skyldigheter för de som träffas av lagen. Den nya lagen bör därför innehålla ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om kraven på ett systematiskt och riskbaserat informationssäkerhetsarbete, riskanalys, tekniska och organisatoriska åtgärder och incidenthantering.

Enligt artikel 19 i NIS-direktivet ska medlemsstaterna, med hänsyn till behovet av en enhetlig tillämpning av säkerhetsåtgärder inom EU, uppmuntra användningen av europeiska eller internationellt accepterade standarder och specifikationer av relevans för säkerheten i nätverk och informationssystem. Bestämmelser som främjar användningen av sådana standarder och specifikationer bör enligt regeringens bedömning meddelas i förordning eller myndighetsföreskrifter.

7.2 Incidentrapportering

7.2.1 Befintliga bestämmelser om incidentrapportering är inte tillräckliga

Regeringens bedömning: NIS-direktivet kräver nya bestämmelser om incidentrapportering.

Utredningens bedömning stämmer överens med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över bedömningen.

Skälen för regeringens bedömning: Enligt NIS-direktivet ska leverantörer av samhällsviktiga tjänster, 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 (artikel 14.3).

Leverantörer som omfattas av NIS-direktivet kan även omfattas av andra krav på rapportering av incidenter. Exempelvis är statliga myndigheter enligt förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap skyldiga att till MSB skyndsamt rapportera incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för. Vidare ska vissa incidenter enligt 10 a § säkerhetsskyddsförordningen (1996:633) anmälas till den myndighet som utövar tillsyn över säkerhetsskyddet. Det finns även sektorsspecifika krav på rapportering av incidenter i vissa av de sektorer som omfattas av NIS-direktivet. Exempelvis finns inom sektorn finansmarknadsinfrastruktur krav i lagen om värdepappersmarknaden om att rapportera händelser av väsentlig betydelse.

Från och med den 25 maj 2018 när dataskyddsförordningen ska börja tillämpas finns även en skyldighet enligt artikel 33 i den förordningen att anmäla s.k. personuppgiftsincidenter, dvs. en säkerhetsincident som oavsiktligt påverkar behandlingen av personuppgifter.

Den befintliga regleringen om incidentrapportering är inte heltäckande och motsvarar i vissa fall inte de krav som NIS-direktivet ställer. Regeringens bedömning är därför att det i den nya lagen måste införas bestämmelser med krav på incidentrapportering enligt NIS-direktivet.

7.2.2 Vilka incidenter ska rapporteras?

Regeringens förslag: Leverantörer av samhällsviktiga tjänster ska rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst de tillhandahåller.

Regeringens bedömning: Bestämmelser om vilka faktorer som ska beaktas vid bedömningen av om en incident har en betydande inverkan på kontinuiteten i en samhällsviktig tjänst, och därför medför krav på rapportering, bör meddelas i förordning eller myndighetsföreskrifter.

Utredningens förslag stämmer i huvudsak överens med regeringens förslag och bedömning. Utredningen har även föreslagit en bestämmelse om att leverantörer av samhällsviktiga tjänster ska rapportera varje inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller på grund av en incident som även har påverkat en tredjepartsleverantör av digitala tjänster. Vidare har utredningen föreslagit att vissa faktorer som ska beaktas för att bedöma om en incident har en betydande inverkan på kontinuiteten ska regleras i den nya lagen.

Remissinstanserna: *Post- och telestyrelsen* och *Stockholms universitet* tillstyrker förslaget. *Säkerhetspolisen* och *Försvarsmakten* anser att fler incidenter än vad som har föreslagits bör omfattas av krav på rapportering. *Energiföretagen Sverige* och *Jönköpings läns landsting* anser att kravet på att rapportera incidenter, oavsett om de har skett hos en tredjepartsleverantör av digitala tjänster, kan innebära att ett orimligt ansvar läggs på leverantörer av samhällsviktiga tjänster. Flera remissinstanser, bl.a. *Netnod*, efterfrågar tydliggörande av när rapportering ska ske enligt den nya lagen och enligt andra regelverk. Säkerhetspolisen anser att det bör klargöras vilken myndighet som ska avgöra enligt vilket regelverk en leverantör ska rapportera en incident om det inte råder konsensus mellan myndigheter. *Göteborgs stad* och *Sveriges Kommuner och Landsting* påpekar att det är viktigt med tydliga skrivningar om vilka incidenter som ska rapporteras.

Skälen för regeringens förslag och bedömning

Incidenter som har en betydande inverkan på kontinuiteten ska rapporteras

Enligt artikel 14.3 i NIS-direktivet ska leverantörer av samhällsviktiga tjänster rapportera incidenter som har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänster som de tillhandahåller. 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). Med en incident avses en händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem (artikel 4.7).

Försvarsmakten och *Säkerhetspolisen* anser att det bör införas krav på att rapportera fler incidenter än vad som krävs enligt NIS-direktivet. Försvarsmakten anser att även incidenter som inte har fått en omedelbar

effekt på kontinuiteten i de berörda tjänsterna, men som kan leda till en sådan inverkan bör omfattas av rapporteringskraven. Säkerhetspolisen anser att även andra incidenter än sådana som påverkar tjänstens kontinuitet bör omfattas av rapporteringsskyldigheten. Regeringen instämmer i att det kan finnas behov av bestämmelser om incidentrapportering med anledning av andra incidenter än de som regleras av NIS-direktivet. Regeringen anser emellertid inte att det finns beredningsunderlag för att hantera sådana mer övergripande frågor om informationssäkerhet inom ramen för detta lagstiftningsärende.

Enligt den nya lagen ska alltså incidenter med en betydande inverkan på kontinuiteten i samhällsviktiga tjänster rapporteras. Det innebär att incidenter som inverkar negativt på tjänsterna på andra sätt inte behöver rapporteras enligt den nya lagen. När det gäller sådana incidenter kan det dock finnas rapporteringskrav i andra regelverk. Vad som krävs för att en påverkan på kontinuiteten ska anses vara betydande utvecklas närmare nedan.

För att motsvara de krav som ställs i artiklarna 14.3 och 16.5 i NIS-direktivet bör bestämmelsen utformas så att den ålägger leverantörer att rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst de tillhandahåller. En sådan bestämmelse innebär att leverantörer ska rapportera incidenter oavsett var incidenten har skett. Leverantörer av samhällsviktiga tjänster kommer därför även att ha en skyldighet att rapportera incidenter hos exempelvis en tredjepartsleverantör och följdincidenter på grund av en sådan incident, under förutsättning att incidenten har en betydande inverkan på den samhällsviktiga tjänst som leverantören tillhandahåller. Regeringen ser därför inget behov av en sådan särskild bestämmelse om skyldighet att rapportera påverkan på kontinuiteten på grund av en incident som även har påverkat en tredjepartsleverantör av digitala tjänster som utredningen har föreslagit.

Energiföretagen Sverige och *Jönköpings läns landsting* anser att skyldigheten att rapportera incidenter hos en tredjepartsleverantör av digitala tjänster kan innebära att ett orimligt ansvar läggs på leverantören av den samhällsviktiga tjänsten. Energiföretagen Sverige menar att kravet innebär att leverantörer av samhällsviktiga tjänster måste stå som garant för tredjepartsleverantörens säkerhet samt ha full överblick över tredjepartsleverantörens risker. Jönköpings läns landsting efterfrågar klargöranden av hur långt ansvaret för tredjepartsleverantörens säkerhet sträcker sig. Med anledning av Energiföretagen Sverige och Jönköpings läns landstings synpunkter finns det anledning att poängtera att leverantörer av samhällsviktiga tjänster inom ramen för det egna säkerhetsarbetet kan ha anledning att beakta eventuella risker som är kopplade till en tredjepartsleverantör som leverantören är beroende av för att tillhandahålla den samhällsviktiga tjänsten. Däremot innebär kravet på att rapportera incidenter som härrör från en tredjepartsleverantör inte att leverantörer av samhällsviktiga tjänster övertar tredjepartsleverantörens skyldigheter att vidta säkerhetsåtgärder. Det är också naturligt att leverantörer inte alltid kommer ha förutsättningar att kunna rapportera närmare detaljer kring en incident som har sitt ursprung hos en tredjepartsleverantör.

Flera remissinstanser, bl.a. *Netnod*, vill att det tydliggörs när rapportering ska ske enligt den nya lagen och enligt andra regelverk. Som fram-

går av avsnitt 5.4 ska vissa leverantörer av betrodda tjänster, vissa leverantörer av elektroniska kommunikationstjänster och leverantörer som omfattas av krav i annan författning som motsvarar skyldigheterna i den nya lagen inte tillämpa den nya lagen alls. Sådana leverantörer ska således inte rapportera incidenter enligt den nya lagen. Rapporteringskraven i den nya lagen ska inte heller gälla för säkerhetskänslig verksamhet. Incidenter i sådan verksamhet ska även fortsättningsvis rapporteras enligt säkerhetsskyddsregleringen. Vidare ska de nu föreslagna rapporteringskraven inte gälla för leverantörer av digitala tjänster som är mikroföretag eller små företag. I övrigt ersätter inte rapporteringskrav i andra regelverk de krav på incidentrapportering som nu föreslås. Vissa leverantörer kan därför, vilket flera remissinstanser såsom *Stockholms läns landsting* också påpekar, vara tvungna att rapportera samma incident enligt flera regelverk.

Om en leverantör av samhällsviktiga tjänster är osäker på vilket eller vilka regelverk som gäller för en inträffad incident bör berörda tillsynsmyndigheter kontaktas. Råder det tveksamhet om en incident ska rapporteras enligt säkerhetsskyddsregleringen bör leverantören i första hand kontakta Säkerhetspolisen eller Försvarsmakten för vägledning. Om en incident som rör Sveriges säkerhet felaktigt rapporteras enligt den nya lagen bör vidare leverantören uppmärksammas på detta. Regeringen förutsätter att berörda myndigheter kan samverka kring vart och enligt vilket regelverk incidentrapportering ska ske och ser därför inget behov av att, såsom *Säkerhetspolisen* föreslår, reglera att någon myndighet ska ha tolkningsföreträde i det avseendet.

Föreskrifter om vad som är en betydande inverkan på kontinuiteten

Vid bedömningen av om en incident har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten ska, enligt artikel 14.4 i NIS-direktivet, hänsyn framför allt tas till ett antal angivna faktorer. De faktorer som är av betydelse vid bedömningen är det antal användare som påverkas av störningen i den samhällsviktiga tjänsten, hur länge incidenten varar och hur stort geografiskt område som påverkas av incidenten.

Som *Göteborgs stad* och *Sveriges Kommuner och Landstings* påpekar är det viktigt med tydlighet i fråga om vilka incidenter som ska rapporteras. Enligt regeringen kan det därför behövas ytterligare vägledning för att berörda leverantörer ska kunna avgöra om en incident kan anses ha en betydande inverkan på kontinuiteten. Förutom de redan angivna faktorerna bör även sektorsspecifika förhållanden kunna beaktas.

Utredningen har föreslagit att bestämmelser som motsvarar artikel 14.4 bör införas i den nya lagen och att andra bestämmelser om vilka faktorer som ska beaktas för att avgöra om en incident har betydande inverkan på kontinuiteten bör meddelas i förordning eller myndighetsföreskrifter. För att inte onödigt tynga den nya lagen med detaljerade bestämmelser anser regeringen dock att samtliga bestämmelser om vilka faktorer som ska beaktas bör meddelas i förordning eller myndighetsföreskrifter. Sådana föreskrifter ska, i enlighet med förslaget i avsnitt 7.2.7, få meddelas av regeringen eller den myndighet som regeringen bestämmer.

7.2.3 Till vilken myndighet ska incidentrapporteringen göras?

Regeringens bedömning: Incidentrapporteringen bör göras till den s.k. CSIRT-enheten.

Regeringens förslag: I den nya lagen ska det anges att incidentrapporteringen ska göras till den myndighet som regeringen bestämmer.

Utredningens förslag stämmer i sak överens med regeringens förslag och bedömning. Utredningen har föreslagit att det i den nya lagen ska anges att incidentrapporteringen ska göras till CSIRT-enheten.

Remissinstanserna: *Livsmedelsverket* anser att rapportering bör ske till både CSIRT-enheten och tillsynsmyndigheten. Flera remissinstanser efterfrågar samordning av incidentrapportering enligt olika regelverk.

Skälen för regeringens förslag och bedömning: Enligt artikel 14.3 i NIS-direktivet ska incidentrapporteringen ske till den behöriga myndigheten, dvs. tillsynsmyndigheten, eller CSIRT-enheten. Frågan är därför om leverantörer av samhällsviktiga tjänster ska rapportera till tillsynsmyndigheten eller till CSIRT-enheten.

I avsnitt 9.1 gör regeringen bedömningen att det som utgångspunkt ska utses en tillsynsmyndighet för varje sektor. Tillsynsmyndigheterna ska utöva tillsyn över tillämpningen av den nya lagen. Information som framkommer vid en incidentrapportering är ett av de viktigaste verktygen i tillsynsmyndigheternas arbete. Det talar för att rapporteringen ska ske till respektive tillsynsmyndighet.

I avsnitt 11.2 gör regeringen bedömningen att MSB som utgångspunkt ska vara CSIRT-enhet (Computer Security Incident Response Team). CSIRT-enhetens uppgifter ska enligt direktivet omfatta bl.a. övervakning av incidenter på nationell nivå, tillhandahållande av tidiga varningar, informationsspridning till relevanta aktörer vid incidenter, åtgärder vid incidenter, tillhandahållande av dynamisk risk- och incidentanalys samt deltagande i CSIRT-nätverket (bilaga 1). CSIRT-nätverket är ett nätverk som har inrättats genom direktivet och som består av företrädare för medlemsstaternas CSIRT-enheter och CERT-EU (incidenthanteringsorganisationen för EU:s institutioner, organ och kontor). MSB deltar för närvarande i nätverket för Sveriges räkning. CSIRT-nätverket ska på olika sätt bidra till utveckling av förtroende och tillit mellan medlemsstaterna och främja ett snabbt och effektivt operativt samarbete (artikel 12.1).

Mot bakgrund av CSIRT-enhetens roll och uppdrag när det gäller hantering av incidenter är regeringens bedömning att incidentrapportering enligt den nya lagen bör göras till CSIRT-enheten. För att tillgodose tillsynsmyndigheternas behov av information om incidenter bör det dock i förordning införas bestämmelser om att CSIRT-enheten ska överlämna information om incidenter till den tillsynsmyndighet som utövar tillsyn över den rapporterande leverantören, se avsnitt 11.2. Rapporteringen bör inte, som *Livsmedelsverket* förespråkar, ske även till tillsynsmyndigheten eftersom det skulle innebära att fler myndigheter behöver ta fram och bekosta sådan infrastruktur som behövs för att på ett lämpligt sätt kunna ta emot incidentrapporter. Uttrycket CSIRT-enheten bör inte användas i lagtext. I den nya lagen ska därför anges att rapporteringen ska ske till den myndighet som regeringen bestämmer.

Flera remissinstanser, såsom *Stockholms läns landsting*, *Svenska bankföreningen* och *Sveriges Kommuner och Landsting*, efterfrågar samordning av incidentrapportering enligt olika regelverk. Sveriges Kommuner och Landsting menar exempelvis att en myndighet borde ta emot incidentrapporter enligt flera regelverk och sedan skicka vidare till andra berörda myndigheter. Regeringen instämmer i att det – i den mån det är möjligt – kan finnas fördelar med att samordna rapportering enligt olika regelverk. Det finns dock inte beredningsunderlag för att genomföra en sådan samordning som remissinstanserna efterfrågar inom ramen för detta lagstiftningsärende.

7.2.4 När i tiden ska leverantörer rapportera incidenter?

Regeringens förslag: Rapporteringen ska göras utan onödigt dröjsmål.

Utredningens förslag stämmer överens med regeringens.

Remissinstanserna: *Energigas Sverige* och *Swedegas AB* tillstyrker förslaget. *Nasdaq Stockholm AB* anser att det bör klargöras vad som menas med utan onödigt dröjsmål. *Bodens kommun* och *Luleå kommun* anser att det bör sättas en bestämd tidsgräns för när rapportering ska ske.

Skälen för regeringens förslag: Enligt artikel 14.3 i NIS-direktivet ska rapportering av incidenter ske utan onödigt dröjsmål. I den nya lagen bör införas en motsvarande bestämmelse.

Nasdaq Stockholm AB anser att det bör klargöras vad som menas med utan onödigt dröjsmål. Någon närmare precisering anges inte i direktivet. Att CSIRT-enheten ska underrättas utan onödigt dröjsmål när en incident som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten har inträffat bör dock innebära att den berörda leverantören ska rapportera så snart de uppgifter som ska lämnas finns tillgängliga. Mot bakgrund av direktivets syfte att säkerställa kontinuiteten i de samhällsviktiga tjänsterna är det dock inte rimligt att leverantören, för att fullgöra sin rapporteringsskyldighet, tvingas att prioritera ned arbetet med att hantera den inträffade incidenten. Rapporteringen bör därför ske efter att de första kritiska åtgärderna för att avhjälpa incidenten har vidtagits. Om en incident påverkar fler leverantörer eller om en incident är gränsöverskridande bör dock rapporteringen ske snarast för att konsekvenserna ska kunna begränsas. Med hänsyn till att innebörden av utan onödigt dröjsmål kan variera kraftigt bör någon absolut tidsgräns – såsom *Bodens kommun* och *Luleå kommun* efterfrågar – inte införas i den nya lagen. Närmare bestämmelser om när i tiden rapportering ska ske kan meddelas av regeringen eller den myndighet som regeringen bestämmer.

7.2.5 Vilken information ska en incidentrapport innehålla?

Regeringens bedömning: Bestämmelser om vilken information en incidentrapport ska innehålla bör meddelas i förordning eller myndighetsföreskrifter.

Utredningens förslag stämmer delvis överens med regeringens bedömning. Utredningen har föreslagit att vissa bestämmelser om vilken information som en incidentrapport ska innehålla ska tas in i den nya lagen. Vidare har utredningen föreslagit att det i den nya lagen ska införas en bestämmelse om att incidentrapportering inte ska medföra ökat ansvar för den rapporterande parten.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens bedömning: Enligt artikel 14.3 i NIS-direktivet ska en incidentrapport innehålla uppgifter som gör det möjligt för CSIRT-enheten att fastställa incidentens eventuella gränsöverskridande verkningar. Några andra uttryckliga krav på vad en incidentrapport ska innehålla ställs inte i NIS-direktivet. För att uppfylla syftet med incidentrapporteringen bör dock en rapport innehålla information som gör att tillsynsmyndigheterna och den nationella kontaktpunkten kan fullgöra sina uppgifter, se avsnitt 9.2 och 11.1. Det innebär att en incidentrapport behöver innehålla bl.a. en beskrivning av incidenten och de åtgärder som har vidtagits för att hantera den. Rapporterna bör vidare så långt det är möjligt utformas på samma sätt för samtliga sektorer.

Utredningen har föreslagit att kravet på att incidentrapporter ska innehålla information som gör det möjligt för CSIRT-enheten att fastställa incidentens eventuella gränsöverskridande verkningar bör meddelas i lag och att andra bestämmelser om t.ex. vad rapporterna ska innehålla och de närmare formerna för rapporteringen ska meddelas i förordning eller myndighetsföreskrifter. Regeringen anser emellertid att det är lämpligare att meddela samtliga sådana bestämmelser i förordning eller myndighetsföreskrifter. I avsnitt 7.2.7 föreslår regeringen ett bemyndigande om att regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om incidentrapportering.

I artikel 14.3 anges vidare att incidentrapportering inte ska medföra ett utökat ansvar för den rapporterande parten, dvs. ett ansvar utöver det som följer av NIS-direktivet. Det innebär bl.a. att det inte går att ställa krav på leverantören att utreda händelsen åt CSIRT-enheten. Utredningen har föreslagit en uttrycklig bestämmelse om att incidentrapporteringen inte får medföra utökat ansvar för den rapporterande parten. Regeringen anser emellertid att en sådan bestämmelse är obehövlig eftersom de av regeringen ovan föreslagna bestämmelserna om incidentrapportering inte innebär att den rapporterande parten åläggs ett ansvar utöver det som följer av NIS-direktivet. Med andra ord uppfyller den nya lagen även utan en sådan bestämmelse som utredningen har föreslagit kraven i artikel 14.3.

7.2.6 Frivillig rapportering av incidenter

Regeringens bedömning: Bestämmelser om frivillig rapportering av incidenter bör meddelas i förordning eller myndighetsföreskrifter.

Utredningens förslag stämmer i sak överens med regeringens bedömning.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens bedömning: Enligt artikel 20 i NIS-direktivet ska leverantörer som inte har identifierats som leverantörer av samhällsviktiga tjänster och som inte är leverantörer av digitala tjänster ges möjlighet att på frivillig grund rapportera incidenter som har en betydande inverkan på kontinuiteten i de tjänster som de tillhandahåller. Vid behandlingen av sådana rapporter ska medlemsstaterna enligt samma artikel 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.

Bestämmelser om frivillig rapportering av incidenter bör enligt regeringens bedömning meddelas i förordning eller myndighetsföreskrifter.

7.2.7 Bemyndigande

Regeringens förslag: Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vad som krävs av leverantörer av samhällsviktiga tjänster för att uppfylla kravet på incidentrapportering.

Utredningens förslag stämmer i sak överens med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens förslag: Utöver de övergripande bestämmelserna om skyldigheten för leverantörer av samhällsviktiga tjänster att rapportera incidenter som regeringen föreslår, krävs det ytterligare föreskrifter om vad skyldigheten innebär. Regeringen bedömer att det utöver verkställighetsföreskrifter, såsom närmare bestämmelser om när i tiden incidentrapportering ska ske och de närmare formerna för rapporteringen, finns behov av ett bemyndigande när det gäller t.ex. vilka faktorer som ska beaktas vid bedömningen av om en incident ska rapporteras, se avsnitt 7.2.2. Sådana föreskrifter avses nämligen mer i detalj specificera skyldigheten att rapporterna en incident som har en betydande inverkan. Den som underlåter att fullgöra skyldigheten kan dessutom påföras sanktionsavgift.

Mot denna bakgrund bör den nya lagen innehålla ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om skyldigheten för leverantörer av samhällsviktiga tjänster att rapportera incidenter.

Det bör poängteras att den samarbetsgrupp som inrättats genom NIS-direktivet får utarbeta och anta riktlinjer om under vilka omständigheter som leverantörer av samhällsviktiga tjänster ska rapportera incidenter (artikel 14.7). I den utsträckning samarbetsgruppen utarbetar och antar sådana riktlinjer bör dessa beaktas i föreskriftsarbetet.

8 Säkerhetsåtgärder och incidentrapportering för leverantörer av digitala tjänster

Enligt NIS-direktivet ska medlemsstaterna säkerställa att leverantörer av digitala tjänster vidtar vissa säkerhetsåtgärder och att de rapporterar incidenter som har en avsevärd inverkan på tillhandahållandet av den digitala tjänsten. Leverantörer av digitala tjänster omfattas i dag inte av någon nationell lagstiftning motsvarande bestämmelserna i direktivet. Det måste därför införas bestämmelser med krav på säkerhetsåtgärder och incidentrapportering för leverantörer av digitala tjänster i den nya lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

NIS-direktivets krav på säkerhetsåtgärder och incidentrapportering är i viss mån mer begränsade för leverantörer av digitala tjänster än för leverantörer av samhällsviktiga tjänster. Anledningen till skillnaden är enligt skälen till direktivet att risken för samhällspåverkan i praktiken är lägre för leverantörer av digitala tjänster än för leverantörer av samhällsviktiga tjänster (skäl 49). Medlemsstaterna får enligt artikel 16.10 i NIS-direktivet inte heller införa ytterligare säkerhets- eller rapporteringskrav för leverantörer av digitala tjänster utöver de som anges i direktivet.

Kraven i direktivet på leverantörer av digitala tjänster att vidta säkerhetsåtgärder och att rapportera incidenter har i enlighet med artikel 16.8 specificerats i kommissionens genomförandeförordning (EU) 2018/151 av den 30 januari 2018 om tillämpningsföreskrifter för NIS-direktivet, kallad genomförandeförordningen. Kommissionen får enligt artikel 16.9 också anta genomförandeakter för att reglera format och förfaranden för incidentrapporteringen.

8.1 Säkerhetsåtgärder

Regeringens förslag: Leverantörer av digitala tjänster ska vidta de tekniska och organisatoriska åtgärder som de anser ändamålsenliga och proportionella och som hanterar risker som hotar säkerheten i nätverk och informationssystem som de använder när de tillhandahåller digitala tjänster inom EU. Åtgärderna ska säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till risken.

Leverantörer av digitala tjänster ska vidta åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder. Skyldigheten gäller endast verkningar som en sådan incident har på digitala tjänster som leverantören erbjuder inom EU. Syftet med åtgärderna ska vara att säkerställa kontinuiteten i tjänsterna.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om kraven på tekniska och organisatoriska åtgärder och incidenthantering.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningen har till skillnad från regeringen inte föreslagit något bemyndigande.

Remissinstanserna: Endast *Stockholms universitet* har yttrat sig, och tillstyrker förslaget.

Skälen för regeringens förslag

Tekniska och organisatoriska åtgärder

Enligt artikel 16.1 i NIS-direktivet ska leverantörer av digitala tjänster 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 digitala tjänster inom EU. 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, 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.

Faktorerna som anges i artikel 16.1 a–e specificeras i artikel 2 i genomförandeförordningen.

Leverantörer av digitala tjänster ska alltså vidta tekniska och organisatoriska säkerhetsåtgärder. Vad som avses med begreppet tekniska och organisatoriska åtgärder behandlas i avsnitt 7.1.4. Åtgärderna ska hantera säkerhetsrisker i nätverk och informationssystem och säkerställa en nivå på säkerheten som är lämplig i förhållande till den föreliggande risken. Vad som avses med uttrycken säkerhet i nätverk och informationssystem och risk behandlas också i avsnitt 7.1.4. En bestämmelse som motsvarar artikel 16.1 bör införas i den nya lagen.

Leverantörens skyldighet omfattar åtgärder för nätverk och informationssystem som leverantören använder vid tillhandahållet av digitala tjänster inom EU. Det innebär bl.a. att säkerhetskraven gäller oavsett om leverantören sköter underhållet av sina nätverk och informationssystem internt eller lägger ut uppgifterna på entreprenad (skäl 52).

Till skillnad från vad som gäller för leverantörer av samhällsviktiga tjänster anges i direktivet att leverantörer av digitala tjänster ska ”utarbeta” ändamålsenliga och proportionella tekniska och organisatoriska åtgärder. Det innebär bl.a. att medlemsstaterna inte får reglera närmare på vilket sätt säkerhetsarbetet ska bedrivas. Vidare innebär det att leverantören avgör vilka tekniska och organisatoriska åtgärder som är ändamålsenliga och proportionella, dvs. vilka konkreta åtgärder som ska vidtas, under förutsättning att åtgärderna hanterar säkerhetsrisker i nätverk och informationssystem och, med beaktande av de särskilt angivna faktorerna, säkerställer en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till den föreliggande risken (skäl 49). Bestämmelsen i den nya lagen bör utformas på ett sätt som klargör detta.

Vid bedömningen av vad som är en lämplig nivå i förhållande till risken ska enligt NIS-direktivet hänsyn tas till den senaste tekniska utvecklingen.

Det innebär att leverantören ska beakta samtliga tekniska lösningar som vid var tid finns tillgängliga på marknaden. I enlighet med bedömningen i avsnitt 7.1.4, avseende motsvarande krav på leverantörer av samhällsviktiga tjänster, behöver kravet på att beakta den tekniska utvecklingen enligt regeringens mening inte uttryckas i den nya lagen, utan ingår i att säkerhetsåtgärderna ska uppnå en lämplig säkerhetsnivå. När det gäller de övriga uttryckliga faktorerna som leverantörerna ska beakta, som anges artikel 16.1 a–e, anser regeringen – till skillnad från utredningen – att de bör meddelas i förordning eller myndighetsföreskrifter. Anledningen till det är att den nya lagen inte bör tyngas med alltför många detaljföreskrifter.

Incidenthantering

Enligt artikel 16.2 i NIS-direktivet ska leverantörer av digitala tjänster vidta åtgärder för att förebygga och minimera den inverkan som incidenter som påverkar säkerheten i deras nätverk och informationssystem har på de digitala tjänster som erbjuds inom unionen, i syfte att säkerställa kontinuiteten i dessa tjänster.

En bestämmelse som motsvarar artikel 16.2 bör införas i den nya lagen. Det innebär att leverantörer av digitala tjänster ska vidta åtgärder för att förebygga den inverkan som potentiella incidenter har och för att begränsa en inträffad incidents inverkan, i syfte att säkerställa kontinuiteten i de tillhandahållna tjänsterna. Skyldigheten gäller endast åtgärder som motverkar incidenters verkningar på digitala tjänster som leverantören erbjuder inom EU. Om en leverantör av digitala tjänster t.ex. tillhandahåller molntjänster till användare över hela världen, gäller skyldigheten således endast åtgärder som motverkar sådan inverkan som en incident har eller kan ha på molntjänster som erbjuds inom EU.

Bemyndigande

Som framgår ovan bör de övriga uttryckliga faktorerna som leverantörer av digitala tjänster enligt artikel 16.1 a–e ska beakta vid utformningen av tekniska och organisatoriska åtgärder meddelas i förordning eller myndighetsföreskrifter. Det kan även behövas ytterligare föreskrifter om kravet på incidenthantering. I likhet med regeringens bedömning i avsnitt 7.1.6 beträffande motsvarande krav på samhällsviktiga tjänster, anser regeringen att det behövs ett bemyndigande i den nya lagen om att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om tekniska och organisatoriska åtgärder och incidenthantering.

8.2 Incidentrapportering

Regeringens förslag: Leverantörer av digitala tjänster ska utan onödigt dröjsmål rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av en digital tjänst som de erbjuder inom EU. I den nya lagen ska det anges att incidentrapporteringen ska göras till den myndighet som regeringen bestämmer.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vad som krävs av leverantörer av digitala tjänster för att uppfylla kravet på incidentrapportering.

Regeringens bedömning: Incidentrapporteringen bör göras till den s.k. CSIRT-enheten.

Utredningens förslag stämmer i huvudsak överens med regeringens förslag och bedömning. Utredningen har till skillnad från regeringen föreslagit att vissa faktorer som ska beaktas för att bedöma om en incident har en avsevärd inverkan på tillhandahållandet av en digital tjänst ska regleras i den nya lagen. Utredningen har även föreslagit att det i den nya lagen ska anges att incidentrapporteringen ska göras till CSIRT-enheten och att rapporteringen inte ska medföra ett ökat ansvar för den rapporterande parten. Vidare har utredningen föreslagit att vissa bestämmelser om vilken information som en incidentrapport ska innehålla ska tas in i den nya lagen. Utredningen har dessutom inte föreslagit något bemyndigande.

Remissinstanserna: *Stockholms universitet* tillstyrker förslaget. *Försvarsmakten* och *Säkerhets- och försvarsföretagen* anser att leverantörer av digitala tjänster bör åläggas att rapportera fler incidenter än vad som krävs enligt NIS-direktivet.

Skälen för regeringens förslag och bedömning

Vilka incidenter ska rapporteras?

I artikel 16.3 i NIS-direktivet stadgas att leverantörer av digitala tjänster ska rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av en digital tjänst som de erbjuder inom unionen.

Försvarsmakten anser att leverantörer av digitala tjänster även bör rapportera incidenter som endast riskerar att påverka tillhandahållandet av en digital tjänst. *Säkerhets- och försvarsföretagen* är av uppfattningen att leverantörer av digitala tjänster bör ha samma krav på att incidentrapportera som leverantörer av samhällsviktiga tjänster.

Enligt artikel 16.10 i NIS-direktivet får medlemsstaterna inte införa ytterligare säkerhets- eller rapporteringskrav för leverantörer av digitala tjänster än vad som anges i direktivet. En bestämmelse som motsvarar artikel 16.3 i direktivet bör därför införas i den nya lagen.

För att fastställa om en incident har en avsevärd inverkan ska, enligt artikel 16.4 i NIS-direktivet, hänsyn framför allt 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 incidenter gäller enligt artikel 16.4 endast om leverantören har tillgång till den information som behövs för att bedöma en incidents verkningar mot bakgrund av de angivna faktorerna.

Faktorerna som ska beaktas vid bedömningen av vad som utgör en avsevärd inverkan specificeras i artikel 3 i genomförandeförordningen. I artikel 4 i genomförandeförordningen anges vidare ett antal situationer då en incident ska anses ha en avsevärd inverkan, t.ex. när incidenten gör att den digitala tjänst som tillhandahålls är otillgänglig under mer än 5 000 000 användartimmar eller när incidenten orsakar materiella skador som uppgår till över 1 000 000 euro.

Utredningen har föreslagit att bestämmelser som motsvarar artikel 16.4 ska införas i den nya lagen. För att inte tynga den nya lagen med alltför många detaljföreskrifter anser regeringen dock att sådana bestämmelser bör meddelas i förordning eller myndighetsföreskrifter.

Till vilken myndighet ska incidentrapporteringen göras?

Enligt artikel 16.3 i NIS-direktivet ska leverantörer av digitala tjänster rapportera incidenter till tillsynsmyndigheten eller CSIRT-enheten. Rapporteringen bör, i enlighet med förslaget i avsnitt 7.2.3 om incidentrapportering när det gäller leverantörer av samhällsviktiga tjänster, göras till CSIRT-enheten. Uttrycket CSIRT-enheten bör inte användas i lagtext. I den nya lagen ska därför anges att rapporteringen ska göras till den myndighet som regeringen bestämmer.

När i tiden ska leverantörer rapportera incidenter?

Enligt artikel 16.3 i NIS-direktivet ska rapportering av incidenter ske utan onödigt dröjsmål. Med hänsyn till att innebörden av uttrycket utan onödigt dröjsmål kan variera kraftigt bör någon fast tidsgräns inte införas i den nya lagen. I den nya lagen bör följaktligen anges att rapportering ska ske utan onödigt dröjsmål.

Vilken information ska en incidentrapport innehålla?

Artikel 16.3 i NIS-direktivet stadgar att en incidentrapport ska innehålla information som gör det möjligt för den behöriga myndigheten eller CSIRT-enheten att fastställa vilken betydelse eventuell gränsöverskridande inverkan har. Utredningen har föreslagit att det i den nya lagen ska införas en bestämmelse om att incidentrapporter ska innehålla sådan information och att andra bestämmelser om vad rapporterna ska innehålla och om de närmare formerna för rapporteringen ska meddelas i förordning eller myndighetsföreskrifter. Liksom beträffande leverantörer av samhällsviktiga tjänster, se avsnitt 7.2.5, anser regeringen att bestämmelser om vilken information som rapporterna ska innehålla och om de närmare formerna för fullgörandet av skyldigheten att rapportera incidenter, bör meddelas i förordning eller myndighetsföreskrifter.

I artikel 16.3 stadgas vidare att rapportering inte ska medföra ökat ansvar för den rapporterande parten, dvs. ett ansvar utöver vad som följer av NIS-direktivet. Utredningen har föreslagit en uttrycklig bestämmelse om att incidentrapporteringen inte får medföra ökat ansvar för den rapporterande parten. Regeringen anser emellertid inte att en sådan bestämmelse behövs eftersom de föreslagna bestämmelserna om incidentrapportering inte innebär att den rapporterande parten åläggs ett ansvar utöver det som följer av NIS-direktivet.

Ytterligare föreskrifter om incidentrapportering

Utöver de mer övergripande bestämmelserna om skyldigheten att rapportera incidenter som regeringen föreslår, krävs det ytterligare föreskrifter om vad skyldigheten innebär. Sådana föreskrifter kan till viss del meddelas av regeringen eller den myndighet som regeringen bestämmer med stöd av 8 kap. 7 § regeringsformen, såsom bestämmelser om de närmare formerna för rapporteringen. Till skillnad från utredningen anser regeringens dock även att det finns behov av föreskrifter som går utöver denna normgivningskompetens. Exempelvis behövs ett bemyndigande när det gäller bestämmelser motsvarande artikel 16.4 om vilka faktorer som ska beaktas vid bedömningen av om en incident ska rapporteras och om begränsningar i skyldigheten att rapportera med hänsyn till den information som en leverantör har tillgång till. Bestämmelser om vilka faktorer som ska beaktas bör inte meddelas med stöd av 8 kap. 7 § regeringsformen eftersom de mer i detalj kommer specificera skyldigheten för leverantörer att rapportera en incident som har en avsevärd inverkan. Den som underlåter att fullgöra skyldigheten att rapportera incidenter kan dessutom påföras sanktionsavgift. Föreskrifter om begränsningar av skyldigheten att rapportera med hänsyn till den information som en leverantör har tillgång till kan inte meddelas med stöd av 8 kap. 7 § eftersom sådana föreskrifter innebär en begränsning av en lagstadgad skyldighet.

Mot denna bakgrund bör den nya lagen innehålla ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om skyldigheten för leverantörer av digitala tjänster att rapportera incidenter.

9 Tillsyn

9.1 Tillsynens övergripande utformning

Regeringens förslag: Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Regeringens bedömning: Bestämmelser om vilken eller vilka myndigheter som ska vara tillsynsmyndighet bör meddelas i förordning.

Utredningens förslag stämmer i sak överens med regeringens förslag och bedömning.

Remissinstanserna: Ingen remissinstans uttalar sig om förslaget att regeringen ska utse vilken eller vilka myndigheter som ska vara tillsynsmyndighet. Flera remissinstanser har emellertid synpunkter på om regeringen bör utse en eller flera tillsynsmyndigheter. *Svea hovrätt* har synpunkter på lagbestämmelsens utformning.

Skälen för regeringens förslag och bedömning

Utgångspunkten är en tillsynsmyndighet för varje sektor

Varje medlemsstat ska enligt artikel 8.1 och 8.2 i NIS-direktivet utse en eller flera myndigheter som ska övervaka tillämpningen av direktivet på nationell nivå. I skälen till direktivet anges att medlemsstaterna vid behov bör kunna använda eller anpassa befintliga organisationsstrukturer vid tillämpningen av direktivet (skäl 37).

NIS-direktivet omfattar tre typer av leverantörer av digitala tjänster och leverantörer av samhällsviktiga tjänster inom sju olika sektorer. I detta avsnitt benämns för enkelhetens skull även de tre typerna av digitala tjänster som en sektor.

Det finns i dag flera olika system för tillsyn inom de sektorer som omfattas av NIS-direktivet. Verksamheterna inom sektorerna har i många fall flera olika tillsynsmyndigheter att förhålla sig till. I de flesta fall avser tillsynen inte säkerhet i nätverk och informationssystem.

Vid genomförandet av NIS-direktivets bestämmelser om tillsyn bör man utgå från de förutsättningar som gäller för det specifika tillsynsområdet. Det går inte att bortse ifrån att många tillsynsområden har väsentligen olika förutsättningar som påverkar hur tillsynsregelverket bör utformas för en ändamålsenlig och effektiv tillsyn.

NIS-direktivet omfattar verksamheter av vitt skilda slag, såsom vårdgivare, kreditinstitut och registreringsenheter för toppdomäner. Detta talar för att ha olika tillsynsmyndigheter för respektive sektor.

Ett system med en tillsynsmyndighet per sektor har vidare fördelen att sådana tillsynsmyndigheter har kunskap om verksamhet i sektorn. Verksamhetskunskap är av betydelse t.ex. för vilka säkerhetsåtgärder som är lämpliga att vidta. Vidare minskar verksamhetskunskap risken för att de krav på säkerhetsåtgärder som finns i olika regelverk kommer att motverka varandra.

Inom de olika sektorerna finns dessutom 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 fall finns tydliga EU-rättsakter på området. Även om den nu föreslagna lagstiftningen utformas på ett enhetligt sätt kommer kraven på säkerhetsåtgärder och incidentrapportering inom de olika sektorerna att se olika ut beroende på vilken verksamhet som regleras, vilket också kommer att påverka utformningen av tillsynen. Även detta talar för att utse en tillsynsmyndighet för varje sektor.

Det som främst talar för att utse en tillsynsmyndighet för samtliga sektorer är, såsom flera remissinstanser påpekar, att tillsyn när det gäller säkerhet i nätverk och informationssystem kräver särskild kunskap. Det finns i dag inte myndigheter inom alla sektorer med sådan kompetens som krävs. Flera remissinstanser, däribland *Advenica*, *Inspektionen för vård och omsorg*, *Kiruna kommun* och *Sveriges advokatsamfund*, föreslår också med hänsyn till detta att det endast utses en tillsynsmyndighet för samtliga sektorer. Regeringen anser emellertid att det inom de nu berörda sektorerna är viktigt att höja kompetensen när det gäller informationssäkerhet. Det är därför inte orimligt att kräva att tillsynsmyndigheterna skaffar den kompetens som krävs.

Med hänsyn särskilt till de skilda förhållanden som råder inom sektorerna och att förutsättningarna för en effektiv tillsyn förbättras om tillsynsmyndigheten har kunskap om den verksamhet som är föremål för tillsynen och om annan närliggande reglering, anser regeringen att utgångspunkten för tillsynens utformning bör vara att det ska finnas en tillsynsmyndighet för varje sektor. Ett sådant tillsynssystem bidrar enligt regeringen till en ändamålsenlig tillsyn som höjer nivån på säkerheten i nätverk och informationssystem. Flera remissinstanser, såsom *Energigas Sverige*, *Förvaltningsrätten i Stockholm*, *Statskontoret*, *Stiftelsen för internetinfrastruktur*, *Svea hovrätt*, *Swedegas AB* och *Sveriges Kommuner och Landsting*, delar denna uppfattning.

Bestämmelser om vilken eller vilka myndigheter som ska vara tillsynsmyndighet bör meddelas i förordning. Det möjliggör för regeringen att kunna ändra både antalet tillsynsmyndigheter och vilka myndigheter som ska utses. I den nya lagen om informationssäkerhet för samhällsviktiga och digitala tjänster bör det därför endast införas en bestämmelse om att den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Svea hovrätt anser att lagbestämmelsen bör utformas i plural, dvs. att *de myndigheter* som regeringen bestämmer ska vara nationell behörig myndighet, med hänsyn till att tanken är att flera tillsynsmyndigheter ska utses. Den föreslagna skrivningen i singular innebär emellertid att regeringen kan utse en eller flera tillsynsmyndigheter. Med hänsyn till det anser regeringen inte att det finns skäl att utforma bestämmelsen på något annat sätt än vad utredningen har föreslagit.

Samordning mellan tillsynsmyndigheterna

Mot bakgrund av att tanken är att utse flera tillsynsmyndigheter och att kunskapen om informationssäkerhet i nätverk och informationssystem ibland är låg, anser flera remissinstanser, såsom *Kungliga tekniska högskolan*, *Malmö kommun*, *SJ AB*, *SME-D*, *Swedish Association of Civil Security*, *Sveriges Kommuner och Landsting* och *Trafikverket*, att det finns ett stort behov av samordning mellan tillsynsmyndigheterna.

Utredningen har föreslagit att Myndigheten för samhällsskydd och beredskap (MSB) inom ramen för sitt nuvarande uppdrag ska leda ett samarbetsforum där samtliga tillsynsmyndigheter ingår. I uppdraget att leda samarbetsforumet bör enligt utredningen ingå att uppmärksamma frågor kring tillsynsmetoder och annat som forumet finner viktigt att samordna när det gäller säkerhet i nätverk och informationssystem. Forumet kan enligt utredningen också t.ex. identifiera behovet av vägledningar och diskutera gemensamma frågor om föreskrifter, säkerhetsåtgärder och incidentrapporter. Vidare anser utredningen att MSB inom ramen för forumet bör tillhandahålla metodstöd i syfte att tillsynsmyndigheterna så långt det är möjligt ska använda samma tillsynsmetoder. Utredningen har inte ansett att uppdraget ska författningsregleras.

Flera remissinstanser, t.ex. *Advenica*, *E-hälsomyndigheten*, *MSB*, *Statskontoret*, *Stiftelsen för internetinfrastruktur* och *Säkerhets- och försvarsföretagen*, anser att ett sådant samarbetsforum som utredningen har föreslagit är viktigt för en effektiv och enhetlig tillsyn. För att samarbetsforumet ska fungera anser MSB att det är väsentligt att myndigheten ges

ett tydligt uppdrag att leda och inrikta arbetet samt att det i respektive tillsynsmyndighets instruktion införs krav på deltagande.

Som remissinstanserna anför kan samordning i någon form vara viktigt för en effektiv och enhetlig tillsyn. En brist på samordning kan i förlängningen leda till en ojämn nivå på informationssäkerheten i samhället. För att säkerställa att syftet med NIS-direktivet uppfylls, dvs. en hög gemensam nivå på säkerheten i nätverk och informationssystem, bör det i det fortsatta förordningsarbetet övervägas om och i så fall hur samordningen bör regleras.

9.2 Tillsynsmyndighetens uppdrag

Regeringens förslag: Tillsynsmyndigheten ska utöva tillsyn över att den nya lagen och föreskrifter som har meddelats i anslutning till lagen följs.

Tillsynsåtgärder i förhållande till leverantörer av digitala tjänster ska få vidtas endast när tillsynsmyndigheten har befogad anledning att anta att en sådan leverantör inte uppfyller de krav på säkerhetsåtgärder och incidentrapportering som lagen ställer.

Regeringens bedömning: Bestämmelser om att tillsynsmyndigheten i vissa fall ska samarbeta med tillsynsmyndigheter i andra medlemsstater och Datainspektionen samt lämna stöd till Sveriges representant i den samarbetsgrupp som inrättats genom NIS-direktivet bör meddelas i förordning.

Utredningens förslag stämmer i huvudsak överens med regeringens förslag och bedömning. Utredningen har föreslagit att tillsynsåtgärder i förhållande till leverantörer av digitala tjänster ska få vidtas endast när tillsynsmyndigheten har fått kännedom om att leverantören inte uppfyller den nya lagens krav.

Remissinstanserna: *Säkerhetspolisen* anser inte att tillsynsuppdraget beträffande leverantörer av digitala tjänster bör vara mer begränsat än uppdraget för leverantörer av samhällsviktiga tjänster.

Skälen för regeringens förslag och bedömning

Tillsyn över att den nya lagen följs

Enligt artikel 8.2 i NIS-direktivet ska den eller de tillsynsmyndigheter som en medlemsstat har utsett övervaka tillämpningen av direktivet på nationell nivå. En bestämmelse om att tillsynsmyndigheteten ska utöva tillsyn över att den nya lagen och föreskrifter som har meddelats i anslutning till lagen följs bör därför införas. Det innebär bl.a. att tillsynsmyndigheten ska utöva tillsyn över att leverantörer uppfyller kraven på säkerhetsåtgärder och incidentrapportering.

När det gäller tillsyn över leverantörer av digitala tjänster ska tillsynsmyndigheten enligt NIS-direktivet inte ha någon allmän skyldighet att utöva tillsyn. Medlemsstaterna ska i stället enligt artikel 17 säkerställa att tillsynsmyndigheterna 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. Bakgrunden till skillnaderna i

tillsynsuppdragen enligt NIS-direktivet är enligt skälen att leverantörer av digitala tjänster bör omfattas av mindre ingripande, reaktiv efterhandstillsyn som är anpassad till deras tjänsters och verksamheters art (skäl 60).

Säkerhetspolisen anser inte att tillsynsuppdraget avseende leverantörer av digitala tjänster ska begränsas i enlighet med direktivet, utan att tillsynsmyndigheten ska ha ett allmänt tillsynsuppdrag även när det gäller sådana leverantörer. Regeringen anser inte att det i nuläget finns skäl att frångå direktivet i detta avseende. En bestämmelse som motsvarar artikel 17 bör därför införas i den nya lagen. Utredningen har föreslagit att tillsynsmyndigheten måste ha fått kännedom om en överträdelse innan den får vidta tillsynsåtgärder. Enligt regeringens uppfattning bör det dock inte krävas full vetskap om en överträdelse för att tillsynsmyndigheten ska få vidta tillsynsåtgärder. Regeringen anser att bestämmelsen, för att motsvara artikel 17, bör utformas på så sätt att tillsynsåtgärder i förhållande till leverantörer av digitala tjänster får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att leverantören inte uppfyller de krav som lagen ställer. Det innebär att tillsynsmyndigheten måste ha uppgifter som ger stöd för att en leverantör inte följer den nya lagen. Sådana uppgifter kan tillsynsmyndigheten få t.ex. av leverantören av digitala tjänster själv, från en annan tillsynsmyndighet eller från en tjänsteanvändare, särskilt efter en incident. Även incidentrapporteringen kan innehålla information som gör att tillsynsmyndigheten har befogad anledning att anta att den nya lagen inte följs.

Samarbete på nationell nivå

I NIS-direktivet finns vissa krav på att tillsynsmyndigheterna ska samarbeta med andra nationella aktörer.

Enligt artikel 8.6 i NIS-direktivet ska tillsynsmyndigheterna, när så är lämpligt och i överensstämmelse med nationell rätt, samråda och samarbeta med dataskyddsmyndigheterna. I artikel 15.4 finns dessutom ett krav på samarbete med dataskyddsmyndigheterna när tillsynsmyndigheterna åtgärdar incidenter som medför personuppgiftsincidenter. Bakgrunden till båda kraven om samarbete med dataskyddsmyndigheterna är att säkerheten för personuppgifter ofta undergrävs till följd av incidenter (skäl 63). För att genomföra direktivet i dessa delar anser regeringen att det i förordning bör införas bestämmelser om att tillsynsmyndigheten ska samarbeta med Datainspektionen när den handlägger incidenter som också utgör personuppgiftsincidenter. Vidare finns det anledning att införa krav på tillsynsmyndigheten att samverka med Datainspektionen innan den utfärdar förelägganden. Den frågan behandlas i avsnitt 10.2.

Enligt artikel 8.5 i NIS-direktivet ska medlemsstaterna se till att företrädarna i den samarbetsgrupp som inrättats genom direktivet, se avsnitt 11.3, samarbetar på ett effektivt och säkert sätt. Regeringen anser därför att det i förordning bör införas bestämmelser om att tillsynsmyndigheten ska ha i uppgift att lämna stöd till Sveriges representant i samarbetsgruppen, dvs. MSB.

I artikel 8.6 stadgas vidare att tillsynsmyndigheterna när så är lämpligt och i överensstämmelse med nationell rätt, ska samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna. Dessutom ska

de, enligt artikel 10.1 samarbeta med CSIRT-enheterna när det gäller fullgörandet av NIS-direktivet. Skyldigheter motsvarande artiklarna 8.6 och 10.1 finns redan genom ett generellt krav på myndigheters samverkan i förvaltningslagen (2017:900). Enligt 8 § förvaltningslagen ska en myndighet inom sitt verksamhetsområde samverka med andra myndigheter. Regeringens uppfattning är mot den bakgrunden att det inte behöver införas bestämmelser i svensk rätt för att genomföra artiklarna 8.6 och 10.1 i NIS-direktivet.

Samarbete med tillsynsmyndigheter i andra medlemsstater när det gäller leverantörer av digitala tjänster

I artikel 17.3 i NIS-direktivet finns krav på att tillsynsmyndigheter i olika medlemsstater ska ha ett visst samarbete i fråga om leverantörer av digitala tjänster. Det gäller när 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. Tillsynsmyndigheten i den medlemsstat där det huvudsakliga etableringsstället eller företrädaren finns och tillsynsmyndigheterna i dessa andra medlemsstater ska då samarbeta och vid behov bistå varandra. Detta bistånd och samarbete kan bl.a. omfatta informationsutbyte mellan tillsynsmyndigheterna och begäran om att leverantören av digitala tjänster ska tillhandahålla information eller åtgärda underlåtenhet att incidentrapportera. Tillsynsmyndighetens uppgift i detta avseende bör regleras i förordning.

9.3 Tillsynsmyndighetens undersökningsbefogenheter

I detta avsnitt behandlas befogenheter som tillsynsmyndigheten ska ha för att kunna utöva en effektiv tillsyn, närmare bestämt rätt att få information och tillträde till lokaler, samt åtgärder som tillsynsmyndigheten ska kunna vidta om leverantören inte samarbetar. Tillsynsmyndighetens befogenheter att besluta om åtgärdsförelägganden och sanktionsavgift vid överträdelse av den nya lagens bestämmelser behandlas i avsnitt 10.

9.3.1 Tillgång till information

Regeringens förslag: Den som står under tillsyn ska på begäran ge tillsynsmyndigheten den information som behövs för tillsynen.

Regeringens bedömning: Närmare bestämmelser om vilken information som leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster ska vara skyldiga att tillhandahålla tillsynsmyndigheten bör meddelas i förordning eller myndighetsföreskrifter.

Utredningens förslag stämmer i sak överens med regeringens förslag och bedömning. Utredningen har föreslagit att närmare bestämmelser om vilken information som leverantörer ska tillhandahålla tillsynsmyndigheten ska införas i den nya lagen.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens förslag och bedömning: Enligt artikel 15.2 i NIS-direktivet ska tillsynsmyndigheterna 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 enligt samma artikel uppge syftet med begäran och precisera vilken information som krävs.

Beträffande leverantörer av digitala tjänster ska de behöriga myndigheterna, enligt artikel 17.2 a i NIS-direktivet, 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.

Nämnda artiklar innebär enligt regeringens uppfattning att medlemsstaterna ska ålägga leverantörer att på begäran av tillsynsmyndigheten tillhandahålla sådan information som behövs för tillsynen. Detta bör regleras i den nya lagen. Till skillnad från utredningen anser regeringen emellertid att närmare bestämmelser om vilken information som leverantörer ska vara skyldiga att tillhandahålla och krav på hur tillsynsmyndigheten ska framställa sin begäran lämpligen bör meddelas i förordning. Syftet är att inte tynga den nya lagen med alltför mycket detaljföreskrifter.

För att en tillsynsmyndighet ska kunna utöva en effektiv tillsyn behöver den även ha tillgång till information från incidentrapporter för sin sektor. CSIRT-enheten ska ansvara för att överlämna sådan information till respektive tillsynsmyndighet, se avsnitt 11.2.

9.3.2 Tillträdesrätt till lokaler

Regeringens förslag: Om det behövs för tillsynen ska tillsynsmyndigheten ha rätt att få tillträde till områden, lokaler och andra utrymmen som används i verksamhet som omfattas av den nya lagen. Tillträdesrätten ska dock inte omfatta bostäder.

Utredningens förslag stämmer i sak överens med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens förslag: Enligt artikel 15.1 i NIS-direktivet ska tillsynsmyndigheterna ha de befogenheter och medel som de behöver för att bedöma om leverantörer av samhällsviktiga tjänster uppfyller sina skyldigheter enligt direktivet. För att kunna utöva en effektiv tillsyn kan

tillsynsmyndigheten behöva tillträde till lokaler och liknande. Exempelvis kan tillsynsmyndigheten behöva tillträde för att kontrollera att en leverantör har vidtagit erforderliga tekniska säkerhetsåtgärder.

Med hänsyn till behovet av en effektiv tillsyn anser regeringen att tillsynsmyndigheten, i den utsträckning det behövs för tillsynen, ska ha rätt att få tillträde till områden, lokaler och andra utrymmen där verksamhet som omfattas av lagen bedrivs. Tillträdesrätten bör dock av integritetsskäl inte omfatta bostäder.

I detta avseende finns det inte anledning att göra skillnad mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. Behovet av tillträde vid tillsyn finns avseende båda typer av leverantörer. I avsnitt 9.2 ovan föreslås att tillsynsmyndigheten när det gäller leverantörer av digitala tjänster endast ska få vidta tillsynsåtgärder när den har befogad anledning att anta att en leverantör inte uppfyller den nya lagens krav. Det är alltså först då som tillträdesrätten uppkommer när det gäller sådana leverantörer.

9.3.3 Förelägganden och handräckning

Regeringens förslag: Tillsynsmyndigheten ska få förelägga den som står under tillsyn att tillhandahålla information och att ge tillträde till lokaler och liknande. Ett sådant föreläggande ska få förenas med vite.

Tillsynsmyndigheten ska få begära handräckning av Kronofogdemyndigheten för att genomföra tillsynsåtgärder.

Utredningens förslag stämmer i sak överens med regeringens.

Remissinstanserna: *Svea hovrätt* anser att det inte framgår klart av utredningens förslag till lagtext att tillsynsmyndigheten ska kunna förelägga en leverantör att ge tillträdesrätt till lokaler och liknande.

Skälen för regeringens förslag: I avsnitt 9.3.1 och 9.3.2 föreslår regeringen att tillsynsmyndigheten ska ha rätt att få tillgång till viss information och tillträdesrätt till lokaler och liknande. I linje med de förslagen bör tillsynsmyndigheten även kunna meddela de förelägganden som behövs för att förmå leverantörer som inte samarbetar att tillhandahålla den information och ge det tillträde som behövs för tillsynen. Som *Svea hovrätt* anför bör det av lagtexten tydligt framgå vad tillsynsmyndigheten får meddela förelägganden om. Ett beslut om föreläggande bör kunna förenas med vite.

Om en leverantör ändå vägrar att ge tillsynsmyndigheten information eller tillträde till en lokal 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. För att tillsynsmyndigheten i en sådan situation ska kunna genomföra sin tillsyn bör myndigheten kunna begära handräckning av Kronofogdemyndigheten.

10 Ingripanden och sanktioner

10.1 Straffbestämmelser bör inte införas

Regeringens bedömning: Överträdelser av bestämmelser i den nya lagen bör inte vara straffsanktionerade.

Utredningens bedömning stämmer överens med regeringens.

Remissinstanserna: De remissinstanser som yttrar sig delar bedömningen, däribland *Förvaltningsrätten i Stockholm*, *Skåne läns landsting*, *Statskontoret*, *Stockholms universitet* och *Svea hovrätt*.

Skälen för regeringens bedömning: Enligt artikel 21 i NIS-direktivet ska medlemsstaterna fastställa regler om sanktioner för överträdelse av bestämmelser som har antagits enligt direktivet. Det anges inte vilka sanktioner som ska införas, mer än att sanktionerna ska säkerställa efterlevnaden och vara effektiva, proportionella och avskräckande.

De sanktionsverktyg som normalt står till buds för staten är straff och sanktionsavgifter samt vite, förbud och återkallelse av tillstånd.

Kriminalisering som metod för att försöka hindra överträdelser av olika normer i samhället bör användas med försiktighet. Ett skäl till detta är att en alltför omfattande kriminalisering riskerar att undergräva straffsystemets brottsavhållande verkan, särskilt om rättsväsendet inte kan beivra alla brott på ett effektivt sätt. Ett annat skäl är att kriminalisering innebär påtagliga inskränkningar i medborgarnas valfrihet och ingripande tvångsåtgärder mot dem som begår brott.

När det gäller överträdelser av bestämmelserna i den nya lagen om informationssäkerhet för leverantörer av samhällsviktiga och digitala tjänster kan straff inte heller anses vara den mest effektiva sanktionen. De leverantörer som ska tillämpa den nya lagen utgörs av statliga myndigheter, kommuner, landsting och företag. Straffansvar kan enligt svensk rätt endast träffa fysiska personer. Om straff införs skulle det i många fall vara svårt att identifiera en fysisk person som ansvarig för överträdelsen och att leda i bevis att denne haft uppsåt eller varit oaktsam på det sätt som krävs för straffbarhet.

För att nå syftet med NIS-direktivets sanktionsbestämmelser, dvs. att säkerställa att leverantörer vidtar säkerhetsåtgärder och rapporterar incidenter enligt direktivet, är det enligt regeringens bedömning effektivare och även i övrigt lämpligare med administrativa sanktioner än med straff. De sanktioner som bör komma i fråga för överträdelser av den nya lagens bestämmelser bör därför vara av administrativt slag. Någon straffbestämmelse bör alltså inte tas in i den nya lagen.

10.2 Vilka administrativa sanktioner och andra möjligheter till ingripande ska införas?

Regeringens förslag: Tillsynsmyndigheten ska få meddela de förelägganden som behövs för att leverantörerna ska uppfylla kraven på utseende av företrädare, vissa säkerhetsåtgärder och incidentrapportering enligt den nya lagen och enligt föreskrifter som har meddelats i anslutning till lagen. Ett sådant föreläggande ska få förenas med vite.

Tillsynsmyndigheten ska även kunna besluta om sanktionsavgift för vissa överträdelser.

Regeringens bedömning: Bestämmelser om att tillsynsmyndigheten ska samverka med Datainspektionen innan ett åtgärdsföreläggande meddelas bör meddelas i förordning.

Utredningens förslag stämmer delvis överens med regeringens förslag och bedömning. Utredningen har även föreslagit en bestämmelse om att tillsynsmyndigheten – om det finns skäl att misstänka att en leverantör av samhällsviktiga tjänster inte följer den nya lagen eller föreskrifter som har meddelats i anslutning till den – ska underrätta leverantören om detta förhållande och ge denne möjlighet att yttra sig inom skälig tid. Vidare har utredningen föreslagit att tillsynsmyndigheten – vid sidan av möjligheten att besluta om åtgärdsföreläggande och sanktionsavgift – genom påpekanden och liknande ska försöka förmå leverantörer som inte följer den nya lagen eller föreskrifter som har meddelats i anslutning till den att vidta rättelse. Utredningen har till skillnad från regeringen inte föreslagit att tillsynsmyndigheten ska få meddela åtgärdsföreläggande avseende kravet på att utse en företrädare.

Remissinstanserna: *E-hälsomyndigheten*, *Statskontoret*, *Stiftelsen för internetinfrastruktur* och *Stockholms universitet* tillstyrker förslaget. *Skåne läns landsting* tillstyrker att tillsynsmyndigheten ska kunna besluta om sanktionsavgift.

Skälen för regeringens förslag och bedömning

Förutom kravet i NIS-direktivet att medlemsstaterna ska införa sanktioner finns i artikel 15.3 krav på att tillsynsmyndigheter ska ha befogenhet att utfärda bindande anvisningar till leverantörer av samhällsviktiga tjänster om hur de ska avhjälpa identifierade brister. Vidare ska, enligt artikel 17.2, tillsynsmyndigheter som utövar tillsyn över leverantörer av digitala tjänster ha de befogenheter som krävs för att ålägga leverantörer av digitala tjänster att åtgärda varje underlåtenhet att uppfylla kraven i direktivet. Frågan är då vilka administrativa sanktioner och andra ingripandemöjligheter som ska införas för att säkerställa den nya lagens efterlevnad.

Exempel på ingripande är varning, åtgärdsföreläggande som kan förenas med vite, rättelse på den enskildes bekostnad, återkallelse av tillstånd, förbud mot fortsatt verksamhet och sanktionsavgift. Både sanktionsavgift och återkallelse av tillstånd är i huvudsak tillbakaverkande sanktioner som är handlingsdirigerande genom att verka avskräckande. Återkallelse av tillstånd kan även ses som en framåtriktad sanktion, i den mån återkallelsen syftar till att förhindra fortsatt bristande efterlevnad av ett regelverk.

Åtgärdsföreläggande som kan förenas med 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. Mot den bakgrunden är de ingripanden som bör övervägas enligt regeringens mening åtgärdsföreläggande och sanktionsavgifter.

Tillsynsmyndigheten ska kunna besluta om åtgärdsföreläggande i förening med vite

Åtgärdsföreläggande är ett effektivt och flexibelt ingripande som finns i de flesta tillsynssystem. Regeringen anser även att åtgärdsföreläggande uppfyller kraven i artiklarna 15.3 och 17.2 i NIS-direktivet om att tillsynsmyndigheterna ska ha befogenhet att utfärda bindande anvisningar gentemot leverantörer av samhällsviktiga tjänster och att de ska ha de befogenheter som krävs för att ålägga leverantörer av digitala tjänster att åtgärda underlåtenhet att uppfylla direktivets krav.

Enligt regeringen bör tillsynsmyndigheten därför kunna meddela åtgärdsföreläggande. Till skillnad från utredningen anser regeringen att förelägganden inte bara bör kunna utfärdas för att säkerställa att kraven på riskanalys, tekniska och organisatoriska åtgärder, incidenthantering och incidentrapportering är uppfyllda. För att tillsynsmyndigheten ska ha effektiva befogenheter behöver den även kunna utfärda bindande förelägganden som tar sikte på skyldigheten för juridiska personer som erbjuder digitala tjänster i Sverige att i vissa fall utse en företrädare.

Åtgärdsföreläggande brukar som regel få förenas med vite. Behovet av att åtgärdsförelägganden enligt den nya lagen ska vara tillräckligt handlingsdirigerande och bindande talar för att de ska få förenas med vite. Enligt regeringen tillgodoser sanktionen vite NIS-direktivets krav på effektiva, proportionella och avskräckande sanktioner. Vitets storlek kan anpassas efter vilken typ av åsidosättande det är fråga om så att det kan utgöra ett tillräckligt påtryckningsmedel mot aktören i fråga. Åtgärdsförelägganden bör därför få förenas med vite.

När vite föreläggs ska det enligt 3 § lagen (1985:206) om viten, kallad 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 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 tillsynsmyndigheten behöva upprepa föreläggandet. Det kan i dessa fall vara lämpligt att höja vitesbeloppet.

Samarbete med Datainspektionen innan ett föreläggande meddelas

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 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.

Tillsynsmyndigheten ska kunna besluta om sanktionsavgift

Sanktionsavgift är en ekonomisk sanktion som vanligen riktar sig mot en konstaterad överträdelse av en författningsbestämmelse. Om sanktionsavgiften riskerar att innebära en kostnad eller förlust som är lika stor som eller större än den besparing som görs genom att regelverket inte följs, skapar avgiften incitament att undvika överträdelser.

Sanktionsavgifter finns inom en rad rättsområden. De har olika syfte och utformning. Tillämpningsområdet varierar också. I vissa fall är sanktionsavgift den enda sanktionen för en överträdelse, men i andra fall kan avgift tas ut vid sidan av eller i stället för straff. I vissa fall är sanktionsavgift ett komplement till andra åtgärder och kan användas för att i enskilda fall nyansera ingripandet. Sanktionsavgift har ofta använts för att genomföra unionsrättsliga krav på sanktioner.

Enbart möjligheten att utfärda åtgärdsföreläggande är enligt regeringens bedömning inte tillräckligt för att sanktionssystemet som helhet ska kunna anses effektivt och avskräckande på det sätt som NIS-direktivet kräver. Enligt regeringens bedömning skulle risken att som leverantör drabbas av sanktionsavgift verka avskräckande på ett annat sätt än åtgärdsföreläggande. Risken att drabbas av sanktionsavgift borde också öka incitamenten för ansvariga verksamhetsutövare att satsa på förebyggande åtgärder och att avsätta tillräckliga resurser för att säkerställa att säkerhetskraven och kraven på incidentrapportering tillgodoses. Sanktionsavgift bör därför införas som ett komplement till möjligheten att meddela åtgärdsföreläggande i förening med vite. Det bör påpekas att det finns både för- och nackdelar med en sådan reglering som ger tillsynsmyndigheten möjlighet att välja mellan att genomdriva en åtgärd med vite eller att i efterhand påföra sanktionsavgift. En nackdel är att sanktionssystemet inte blir så förutsägbart som man kan önska. Det är dock av stor vikt att tillsynsmyndigheten kan använda en ändamålsenlig och effektiv sanktion i varje enskilt fall för att uppnå de krav som ställs.

Beslut om sanktionsavgift fattas som huvudregel av en tillsynsmyndighet eller av en domstol efter ansökan från tillsynsmyndigheten.

Generellt sett anses en tillsynsmyndighet lämpad att besluta om sanktionsavgift när reglerna är relativt enkla att tillämpa, beslutsfattandet är förhållandevis schabloniserat och sanktionsbestämmelserna bygger på strikt ansvar. En domstol brukar anses mer lämpad att besluta om sanktionsavgift om det är aktuellt att pröva subjektiva rekvisit eller andra svårbedömda rekvisit. En fördel med att tillsynsmyndigheten 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 leverantör har underlåtit att följa den nya lagen eller föreskrifter som har meddelats i anslutning till den. Det bör därför vara tillsynsmyndigheten som beslutar om sanktionsavgift.

Med hänsyn till att bestämmelser om sanktionsavgift reglerar förhållandet mellan enskilda och det allmänna och avser ingrepp i enskildas ekonomiska förhållanden, bör bestämmelserna som utgångspunkt tas in den nya lagen.

10.3 Sanktionsavgift

10.3.1 Ett sanktionsavgiftssystem med strikt ansvar

Regeringens förslag: En sanktionsavgift ska tas ut av den som underlåter att göra en anmälan till tillsynsmyndigheten, vidta vissa säkerhetsåtgärder eller incidentrapportera enligt den nya lagen eller föreskrifter som har meddelats i anslutning till den.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningen har inte föreslagit att sanktionsavgift ska tas ut av leverantörer av samhällsviktiga tjänster som underlåter att anmäla sig till tillsynsmyndigheten.

Remissinstanserna: Några remissinstanser, bl.a. *Svea hovrätt* och *Sveriges Kommuner och Landsting*, anser inte att den föreslagna lagtexten är tillräckligt tydlig och förutsebar när det gäller vilka åtgärder som leverantörer ska vidta för att inte påföras sanktionsavgift. *Livsmedelsverket* anser att regeringen bör överväga att införa sanktionsavgift även för leverantörer av samhällsviktiga tjänster som underlåter att anmäla sig till tillsynsmyndigheten.

Skälen för regeringens förslag

Överträdelser som ska kunna föranleda sanktionsavgift

Kraven på säkerhetsåtgärder och incidentrapportering i NIS-direktivet är centrala för att uppnå syftet med direktivet, vilket talar för att överträdelser av bestämmelserna i den nya lagen som genomför kraven bör kunna föranleda sanktionsavgift. *Svea hovrätt* och *Sveriges Kommuner och Landsting* anser dock att bestämmelserna i den nya lagen inte är tillräckligt tydliga för att kunna föranleda sanktionsavgift.

Sanktionsavgifter bör som regel endast införas för överträdelser som är relativt lätta att bedöma. Underlåtenhet att incidentrapportera är förhållandevis lätt att konstatera, även om det krävs en bedömning av om en

incident har haft en betydande inverkan på kontinuiteten i den tillhandahållna tjänsten. Även en underlåtenhet att göra en riskanalys är i de flesta fall enkel att fastställa. När det gäller kraven på tekniska och organisatoriska åtgärder och incidenthantering kan det vara svårare att bedöma en eventuell underlåtenhet, bl.a. eftersom en aktörs skyldighet att vidta dessa säkerhetsåtgärder är kopplad till den risk som hotar säkerheten. Säkerhetskraven kommer dock att preciseras genom bestämmelser i förordning och föreskrifter. Utan en sanktion såsom sanktionsavgift för överträdelser av bestämmelser som genomför NIS-direktivets säkerhetskrav är det vidare tveksamt om syftet med NIS-direktivet och dess krav på ändamålsenliga och avskräckande sanktioner uppfylls.

Mot denna bakgrund anser regeringen att sanktionsavgift ska kunna beslutas för överträdelser av kraven på riskanalys, tekniska och organisatoriska åtgärder, incidenthantering och incidentrapportering. I likhet med utredningen anser regeringen inte att kravet på leverantörer av samhällsviktiga tjänster att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete är av sådan karaktär att en överträdelse bör kunna föranleda sanktionsavgift.

Vidare anser regeringen, liksom *Livsmedelsverket*, att leverantörer av samhällsviktiga tjänster som underlåter att enligt förslaget i avsnitt 6.3 anmäla sig till tillsynsmyndigheten bör kunna påföras sanktionsavgift. Om leverantörer av samhällsviktiga tjänster inte riskerar sanktionsavgift vid sådan underlåtelse kan skyldigheten i praktiken bli verkningslös.

Ska sanktionsavgift alltid tas ut?

Bestämmelser om sanktionsavgift är oftast obligatoriska, dvs. utformade så att sanktionsavgift ska tas ut när förutsättningarna för det är uppfyllda. Med hänsyn till behovet av likabehandling, objektivitet och proportionalitet bör tillsynsmyndighetens möjligheter till mer skönsmässiga bedömningar som utgångspunkt vara begränsade. Behovet av att säkerställa likabehandling är särskilt starkt när det gäller sanktionsavgifter enligt den nya lagen eftersom utgångspunkten är att flera tillsynsmyndigheter ska tillämpa bestämmelserna. Bestämmelserna om sanktionsavgift bör därför formuleras på så sätt att sanktionsavgift ska tas ut om förutsättningarna för det är uppfyllda. Tillsynsmyndigheten bör dock ha möjlighet att i vissa fall helt eller delvis efterge sanktionsavgiften, se avsnitt 10.3.3.

Sanktionsavgiftssystemet ska bygga på strikt ansvar

Huvudregeln är att sanktionsavgift bygger på strikt ansvar, dvs. att avgiften ska tas ut oberoende av om överträdelsen har varit uppsåtlig eller berott på oaktsamhet. Beträffande de aktuella överträdelserna finns det ett starkt stöd för en presumtion om att överträdelser inte kan förekomma annat än som en följd av uppsåt eller oaktsamhet. Regeringen anser därför att det inte finns anledning att frångå huvudregeln om strikt ansvar i den nya lagen.

Skrivningar om att avgiftsskyldigheten bygger på strikt ansvar bör inte tas med i lagtexten. I motsats till vad som gäller för straffbestämmelser finns det nämligen inte något formellt krav på uppsåt eller oaktsamhet för att besluta om sanktionsavgift. Det bör därför inte i lagtext upplysas om

att sanktionsavgift får tas ut även om en överträdelse inte har skett uppsåtligen eller av oaktsamhet.

10.3.2 Sanktionsavgiftens storlek

Regeringens förslag: Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst 10 miljoner kronor.

Utredningens förslag stämmer överens med regeringens.

Remissinstanserna: *Statskontoret* tillstyrker förslaget.

Skälen för regeringens förslag: Sanktionsavgifter kan vara utformade som på förhand bestämda belopp, oavsett vem som begått överträdelsen, eller vara kopplade till årsomsättning i näringsverksamhet. Med hänsyn främst till att vissa aktörer som kommer omfattas av den nya lagen är myndigheter är det inte lämpligt att koppla sanktionsavgiften till omsättning. Ett system med bestämda beloppsintervall är därför att föredra.

För att uppfylla kravet på effektiva, proportionella 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.

Inom svensk lagstiftning finns i dag sanktionsavgifter på bl.a. miljöområdet och arbetsmiljöområdet. På dessa områden är det lägsta belopp som kan beslutas vid en överträdelse 1 000 kronor och det högsta beloppet 1 miljon kronor. För upphandlingsskadeavgift enligt lagen (2016:1145) om offentlig upphandling är det lägsta beloppet 10 000 kronor och det högsta 10 miljoner kronor. Avgiften får dock aldrig överstiga en viss andel av upphandlingens värde.

Även dataskyddsförordningen (Europaparlamentets och rådets förordning [EU] 2016/679) innehåller bestämmelser om sanktionsavgifter för överträdelser av förordningens bestämmer. Dataskyddsförordningen ska börja tillämpas den 25 maj 2018 och kommer att utgöra grunden för generell personuppgiftsbehandling inom EU. Enligt dataskyddsförordningen kan sanktionsavgifter tas ut för överträdelse enligt två nivåer – en lägre nivå vid överträdelser som betraktas som mindre allvarliga och en högre nivå vid allvarligare överträdelser. För de olika nivåerna gäller maximibelopp på 10 miljoner euro respektive 20 miljoner euro. I propositionen Ny dataskyddslag (prop. 2017/18:105) föreslås att sanktionsavgifter även ska kunna tas ut av statliga och kommunala myndigheter. Avgifterna ska enligt förslaget uppgå till högst 5 miljoner kronor för mindre allvarliga överträdelser och till högst 10 miljoner kronor för allvarligare överträdelser.

Regeringen bedömer att det är rimligt att det lägsta belopp som ska kunna beslutas i sanktionsavgift är 5 000 kronor. 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. Enligt regeringens bedömning skulle en avgift om 10 miljoner kronor utgöra en effektiv, proportionell och avskräckande sanktion också mot allvarliga överträdelser av NIS-direktivet. Det högsta

belopp som ska kunna beslutas i sanktionsavgift bör därför bestämmas till 10 miljoner kronor.

10.3.3 Hur sanktionsavgiften ska bestämmas i det enskilda fallet

Regeringens förslag: När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till den skada eller risk för skada som uppstått till följd av överträdelsen, till om leverantören tidigare begått en överträdelse och till de kostnader som leverantören undvikit till följd av överträdelsen.

Sanktionsavgiften ska få sättas ned helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Utredningens förslag stämmer i sak överens med regeringens.

Remissinstanserna: *Statskontoret* och *Stockholms universitet* tillstyrker förslaget. *Svea hovrätt* har synpunkter på bestämmelsens utformning.

Skälen för regeringens förslag: När storleken på sanktionsavgiften ska bestämmas i det enskilda fallet bör hänsyn tas till alla relevanta omständigheter. Det är inte möjligt att i den nya lagen ange samtliga relevanta omständigheter som kan behöva beaktas i enskilda fall. Däremot bör den nya lagen innehålla en bestämmelse som anger omständigheter som särskilt ska beaktas. De omständigheter som är särskilt viktiga att beakta och som bör anges i den nya lagen är enligt regeringens mening den skada eller risk för skada som uppstått till följd av överträdelsen, om aktören tidigare begått en överträdelse och de kostnader som aktören undvikit till följd av regelöverträdelsen. Dessa omständigheter kan påverka beloppets storlek både i försvårande och förmildrande riktning. Någon anledning att särskilt ange omständigheter som ska verka försvårande respektive förmildrande, som *Svea hovrätt* föreslår, finns därför inte enligt regeringens mening. Som exempel på andra relevanta omständigheter som kan påverka beloppets storlek men som inte behöver tas in i den nya lagen kan nämnas hur länge överträdelsen pågått. Om aktören tidigare har gjort sig skyldig till en överträdelse kan det bli aktuellt att beakta om överträdelserna är likartade och den tid som gått mellan överträdelserna. Det kan också vara relevant att beakta bestämmelsens betydelse för tillsynsområdet. Att en aktör samarbetat med tillsynsmyndigheten för att komma till rätta med överträdelser kan vara en sådan omständighet som ska påverka beloppets storlek i mildrande riktning.

Att avgiftsskyldigheten bygger på strikt ansvar gör att det behöver finnas utrymme för att jämka eller helt sätta ned sanktionsavgiften. Det bör därför införas en bestämmelse som ger tillsynsmyndigheten utrymme att jämka eller helt efterge avgiften om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Sanktionsavgiften bör kunna sättas ned helt eller delvis om exempelvis 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. Den samlade reaktionen skulle, beroende på överträdelsens art, totalt sett kunna bli alltför betungande. En annan situation som kan innebära att det framstår som oskäligt att besluta om sanktionsavgift är om en leverantör, på grund av avtal med t.ex. en underleverantör, är skyldig att betala skadestånd för samma brist. Om regelverket överträtts på ett sådant sätt att det har varit närmast omöjligt för leverantören att upptäcka överträdelsen skulle överträdelsen kunna anses ursäktlig och det därför finnas grund för jämkning. Möjligheten att sätta ner avgiften bör tillämpas restriktivt och endast när det skulle te sig oskäligt att ta ut avgiften.

10.3.4 Hinder mot sanktionsavgift

Regeringens förslag: Tillsynsmyndigheten ska inte få besluta om sanktionsavgift om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Utredningens förslag stämmer överens med regeringens.

Remissinstanserna: *Statskontoret* och *Stockholms universitet* tillstyrker förslaget.

Skälen för regeringens förslag: Enligt Europakonventionen och EU:s stadga om de grundläggande rättigheterna finns en rätt att inte bli lagförd eller straffad två gånger för samma brott (gärning), det s.k. dubbelprövningsförbudet. Som regeringen har konstaterat i flera lagstiftningsärenden får begreppet straff i den mening som avses i Europakonventionen anses omfatta vite (se prop. 2007/08:107 s. 24 och prop. 2012/13:143 s. 69). 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 anses vara när det inleds en domstolsprocess angående frågan om utdömande av vite (jfr prop. 2016/17:22 s. 228). Ett föreläggande om vite bör därför inte hindra ett senare ingripande med sanktionsavgift så länge som tillsynsmyndigheten inte har ansökt om utdömande av vitet. När tillsynsmyndigheten har ansökt om utdömande av vitet bör tillsynsmyndigheten dock vara förhindrad att besluta om sanktionsavgift för en överträdelse som omfattas av vitesföreläggandet. En bestämmelse om detta bör tas in i den nya lagen.

10.3.5 Förfarandebestämmelser

Regeringens förslag: En sanktionsavgift ska endast få tas ut om den som anspråket riktas mot har getts tillfälle att yttra sig inom två år från det att överträdelsen ägde rum. Beslut om sanktionsavgift ska delges.

Sanktionsavgiften ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas inom denna tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Vid indrivning ska verkställighet få ske enligt utsökningsbalken. En beslutad sanktionsavgift ska falla bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft. Sanktionsavgifter ska tillfalla staten.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningen har inte föreslagit någon bestämmelse om att beslut om sanktionsavgift ska delges. Utredningen har till skillnad från regeringen föreslagit bestämmelser om att den som ett sanktionsbeslut kommer att riktas mot ska få tillfälle att yttra sig och att ett beslut ska vara skriftligt och innehålla skälen för beslutet.

Remissinstanserna: *Stockholms universitet* och *Statskontoret* tillstyrker förslaget. *Förvaltningsrätten i Stockholm* pekar på att utredningens förslag om att den som ett sanktionsbeslut kommer att riktas mot ska få tillfälle att yttra sig och att ett sanktionsbeslut ska vara skriftligt och innehålla skäl behöver motiveras med tanke på att förvaltningslagen (2017:900) innehåller bestämmelser om kommunicering och motiveringsskyldighet. *Svea hovrätt* anser att den föreslagna bestämmelsen om att sanktionsavgift endast ska få tas ut om den som anspråket riktas mot har getts tillfälle att yttra sig inom två år är otydlig.

Skälen för regeringens förslag: Utredningen har föreslagit att det ska införas bestämmelser om att tillsynsmyndigheten ska bereda den som ett sanktionsbeslut kommer att riktas mot tillfälle att yttra sig och att ett beslut ska vara skriftlig och innehålla skälen för beslutet. Som *Förvaltningsrätten i Stockholm* påpekar framgår det dock av 25 § förvaltningslagen att en myndighet – innan den fattar ett beslut i ett ärende – ska underrätta den som är part om allt material av betydelse och ge parten tillfälle att yttra sig över materialet, om det inte är uppenbart obehövligt. Av 9 och 32 §§ i samma lag framgår vidare att handläggningen som utgångspunkt ska vara skriftlig och att ett beslut som kan antas påverka någons situation på ett inte obetydligt sätt ska innehålla en klargörande motivering, om det inte är uppenbart obehövligt. Dessa bestämmelser fyller i allt väsentligt samma funktion som utredningens förslag. Några bestämmelser med den innebörd som utredningen har föreslagit bör därför inte införas i den nya lagen.

Beslut om administrativa sanktionsavgifter är en särskilt ingripande åtgärd. Sådana beslut bör därför delges den betalningsskyldige enligt delgivningslagen (2010:1932). En bestämmelse om detta bör tas in i den nya lagen.

På grund av sanktionsavgiftens ingripande natur bör det finnas en bortre tidsgräns för när en sanktionsavgift får beslutas. Utredningen har föreslagit att sanktionsavgift inte ska få tas ut om den som anspråket riktas mot inte inom två år från det att överträdelsen ägde rum har getts tillfälle att yttra

sig. *Svea hovrätt* anser att det inte står klart från vilken tidpunkt tvåårsfristen ska räknas. Hovrätten anser att ett alternativ skulle kunna vara en bestämmelse i linje med 5 kap. 14 § lagen (2016:1306) om kompletterande bestämmelser till EU:s marknadsmissbruksförordning, enligt vilken ingripande inte får ske med mindre än att den som ingripandet riktas mot har delgetts upplysning härom inom två år från det att överträdelsen ägt rum. Regeringen anser emellertid att bestämmelsen som utredningen har föreslagit är tillräckligt tydlig. Den innebär att om kommunikation enligt 25 § förvaltningslagen med den som avgiften ska tas ut av inte har skett inom två år från överträdelsen, får en sanktionsavgift inte tas ut. Tidsfristen ska räknas från när överträdelsen ägde rum, i likhet med vad som gäller enligt den av hovrätten nämnda lagen. Bevisbördan för att kommunikation har skett ligger på tillsynsmyndigheten. Någon anledning att frångå förvaltningslagens bestämmelser och kräva delgivning av underrättelse finns inte. Regeringen anser liksom utredningen att sanktionsavgift endast ska få tas ut om den som anspråket riktas mot har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Betalning av sanktionsavgift bör ske till tillsynsmyndigheten inom trettio dagar från det att beslutet om sanktionsavgift vunnit laga kraft eller annars inom den längre tid som anges i beslutet. Om avgiften inte betalas inom denna tid bör tillsynsmyndigheten vara skyldig att lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

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 om att en sanktionsavgift som inte betalats inom angiven tid får verkställas enligt utsökningsbalken.

Sanktionsavgifter bör som brukligt tillfalla staten, vilket bör framgå av den nya lagen.

I allmänhet gäller för den här typen av avgifter att de preskriberas i den utsträckning verkställighet inte har skett inom fem år. Regeringen bedömer att det saknas anledning att införa någon annan preskriptionstid än den som i allmänhet används. En bestämmelse om att en beslutad sanktionsavgift faller bort om avgiften inte har verkställts inom fem år från det att beslutet fått laga kraft bör därför införas.

10.4 Omedelbar verkställbarhet av förelägganden

Regeringens förslag: Tillsynsmyndigheten ska få bestämma att ett beslut om föreläggande ska gälla omedelbart.

Utredningens förslag stämmer överens med regeringens.

Remissinstanserna: *Statskontoret* tillstyrker förslaget.

Skälen för regeringens förslag: Om tillsynsmyndigheten har konstaterat att det finns skäl för att ingripa genom beslut om åtgärdsföreläggande kan det i många fall finnas behov av att beslutet blir gällande genast.

Vidare kan det ofta vara angeläget att tillsynsmyndighetens beslut om tillträde till lokaler eller om utlämnande av information som behövs för tillsynen 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. Bestämmelser om inhibition finns i 28 § förvaltningsprocesslagen (1971:291) och behöver inte tas in i den nya lagen.

10.5 Överklagande

Regeringens förslag: Tillsynsmyndighetens beslut enligt den nya lagen ska kunna överklagas till allmän förvaltningsdomstol. I den nya lagen ska det anges att tillsynsmyndigheten vid ett sådant överklagande är motpart i domstolen. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningen har till skillnad från regeringen förslagit att kammarrättens avgörande i ett mål enligt den nya lagen inte ska få överklagas.

Remissinstanserna: *Statskontoret* tillstyrker förslaget. *Förvaltningsrätten i Stockholm* och *Kammarrätten i Stockholm* ifrågasätter om det är en lämplig ordning att ha kammarrätt som slutinstans med tanke på att det – i avsaknad av forumregler – kommer innebära att flera kammarrätter blir slutinstanser för mål enligt den nya lagen.

Skälen för regeringens förslag: En tillsynsmyndighets beslut om föreläggande och sanktionsavgift måste kunna överklagas. Eftersom det är fråga om förvaltningsbeslut bör besluten kunna överklagas till allmän förvaltningsdomstol. Av tydlighetsskäl bör det framgå av bestämmelsen att tillsynsmyndigheten har ställning som motpart i ett mål hos domstolen som gäller överklagande av tillsynsmyndighetens beslut. Vidare bör det anges att prövningstillstånd krävs vid överklagande till kammarrätten. Formerna för överklagande av tillsynsmyndighetens beslut, vilken överklagandefrist som ska gälla, vem som har talerätt m.m., bör inte avvika från förvaltningslagens bestämmelser. Regeringen föreslår därför inte några särskilda bestämmelser om detta.

Utredningen har föreslagit att kammarrättens avgörande inte ska få överklagas. Förutsatt att inga forumregler införs i den nya lagen skulle det – som *Förvaltningsrätten i Stockholm* och *Kammarrätten i Stockholm* påpekar – innebära att de allmänna bestämmelserna i 14 § lagen (1971:289) om allmänna förvaltningsdomstolars behörighet blir tillämplig. Enligt den paragrafen ska beslut överklagas till den förvaltningsrätt inom vars domkrets ärendet först har prövats. Om flera tillsynsmyndigheter utses, i enlighet med utgångspunkten i avsnitt 9.1, kommer det innebära att beslut enligt den nya lagen kommer att prövas i olika förvaltningsrätter runt om i landet med följd att flera kammarrätter blir slutinstanser för mål enligt

lagen. Det är inte en lämplig ordning. För att avsteg ska göras från den normala instansordningen bör det vidare krävas att det finns särskilda skäl. Några sådana har enligt regeringens uppfattning inte framkommit. Mot denna bakgrund bör det inte göras avsteg från den normala instansordningen. Kammarrättens avgörande bör således kunna överklagas.

11 Nationell kontaktpunkt, CSIRT-enhet och samarbetsgrupp

11.1 Nationell kontaktpunkt

Regeringens bedömning: Bestämmelser om vilken myndighet som ska vara nationell kontaktpunkt och vilka uppgifter som den nationella kontaktpunkten ska ha bör meddelas i förordning.

Utredningens förslag stämmer i sak överens med regeringens bedömning. Utredningen har föreslagit att det i den nya lagen ska anges att den myndighet som regeringen bestämmer ska vara nationell kontaktpunkt.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens bedömning: Medlemsstaterna ska enligt artikel 8.3 i NIS-direktivet utse en gemensam nationell kontaktpunkt för säkerhet i nätverk och informationssystem.

Den nationella kontaktpunkten har flera uppgifter enligt direktivet. Enligt artikel 8.4 ska den nationella kontaktpunkten utgöra en sambandsfunktion för att säkerställa gränsöverskridande samarbete mellan medlemsstaternas myndigheter samt med den samarbetsgrupp som inrättas genom NIS-direktivet och CSIRT-nätverket. Den nationella kontaktpunkten ska även på begäran av CSIRT-enheten vidarebefordra incidentrapporter till nationella kontaktpunkter i andra medlemsstater som påverkats av en incident hos en leverantör av samhällsviktiga tjänster (artikel 14.5). Vidare ska den nationella kontaktpunkten senast den 9 augusti 2018, och därefter en gång om året, lämna en sammanfattande rapport till samarbetsgruppen om de incidentrapporter som mottagits (artikel 10.3).

Förutom nämnda uppgifter ska den nationella kontaktpunkten enligt artikel 8.6, när så är lämpligt och i överensstämmelse med nationell rätt, samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna. I skälen till direktivet anges att medlemsstaterna bör uppmuntra leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster att rapportera incidenter som misstänks ha samband med brottslighet till de relevanta rättsvårdande myndigheterna (skäl 62). I 8 § förvaltningslagen (2017:900) finns redan en skyldighet för myndigheter att inom sitt verksamhetsområde samverka med andra myndigheter. Det bör dock övervägas om det ska införas en skyldighet för den myndighet som är nationell kontaktpunkt, CSIRT-enhet eller annan aktör att uppmana

leverantörer att anmäla vissa incidenter till Polismyndigheten. Det bör dessutom övervägas om den nationella kontaktpunkten ska ha i uppgift att i vissa fall samråda med andra medlemsstater innan det fattas ett beslut om identifiering av en leverantör av samhällsviktiga tjänster (artikel 5.4).

När det gäller vilken myndighet som ska vara nationell kontaktpunkt kan det konstateras att Myndigheten för samhällsskydd och beredskap (MSB) har den struktur och kompetens som krävs både för att samordna frågor angående säkerhet i nätverk och informationssystem och för att ansvara för kommunikation och gränsöverskridande samarbete i anslutning till detta. Utgångspunkten bör därför vara att MSB ska ha rollen som nationell kontaktpunkt.

Regeringen anser liksom utredningen att bestämmelser om vilken myndighet som ska vara nationell kontaktpunkt och de uppgifter som myndigheten ska ha bör regleras i förordning. Det möjliggör för regeringen att vid behov ändra vilken myndighet som ska vara nationell kontaktpunkt och vilka uppgifter som myndigheten ska ha i den rollen. Till skillnad från utredningen anser regeringen emellertid inte att det i den nya lagen om informationssäkerhet för samhällsviktiga och digitala tjänster bör införas en bestämmelse som anger att den myndighet som regeringen bestämmer ska vara nationell kontaktpunkt. Anledningen till det är att regeringen till skillnad från utredningen inte föreslår att någon av de uppgifter som den nationella kontaktpunkten bör ha ska regleras i den nya lagen.

11.2 CSIRT-enhet i Sverige

Regeringens bedömning: Bestämmelser om vilken myndighet som ska vara CSIRT-enhet och om vilka befogenheter och uppgifter som CSIRT-enheten ska ha bör meddelas i förordning.

Utredningens förslag stämmer i huvudsak överens med regeringens bedömning. Utredningen har till skillnad från regeringen föreslagit att den nya lagen ska innehålla en bestämmelse om att CSIRT-enheten får begära att en leverantör av digitala tjänster informerar allmänheten om en incident. Utredningen har även föreslagit att det i den nya lagen ska anges att den myndighet som regeringen bestämmer ska vara CSIRT-enhet.

Remissinstanserna: Ingen remissinstans har synpunkter på vilka bestämmelser som bör meddelas i lag respektive i förordning. Däremot har ett flertal remissinstanser synpunkter på vilken myndighet som bör utses till CSIRT-enhet och vilka uppgifter som CSIRT-enheten ska ha.

Skälen för regeringens bedömning

CSIRT-enhetens uppgifter enligt NIS-direktivet

Varje medlemsstat ska enligt artikel 9.1 i NIS-direktivet utse en eller flera incidenthanteringsorgan, s.k. CSIRT-enheter (Computer Security Incident Response Team).

CSIRT-enhetens uppgifter anges bl.a. i punkt 2 i bilaga 1 till NIS-direktivet. Det är uppgifter som rör övervakning av incidenter på nationell nivå, tillhandahållande av varningar om risker och incidenter, åtgärder till

följd av incidenter, samverkan med privat sektor och deltagande i CSIRT-nätverket. CSIRT-nätverket består av företrädare för medlemsstaternas CSIRT-enheter och CERT-EU. Nätverket ska bidra till förtroende och tillit mellan medlemsstaterna och främja ett snabbt och effektivt operativt samarbete (artikel 12).

I NIS-direktivet finns även bestämmelser om uppgifter som ska åligga antingen CSIRT-enheten eller annan aktör.

Enligt artiklarna 14.5 och 16.6 ska CSIRT-enheten eller tillsynsmyndigheten i vissa fall informera den eller de andra medlemsstater som har påverkats av en incident. CSIRT-enheten eller tillsynsmyndigheten ska också i vissa fall förse en leverantör av samhällsviktiga tjänster som har rapporterat en incident med relevant information om uppföljningen av rapporten, såsom information som skulle kunna bidra till effektiv hantering av incidenten (artikel 14.5). Vidare får tillsynsmyndigheten eller CSIRT-enheten informera allmänheten om enskilda incidenter om incidentens avslöjande omfattas av allmänintresset (artiklarna 14.6 och 16.7).

Livsmedelsverket anser att tillsynsmyndigheten och inte CSIRT-enheten bör vara den myndighet som informerar allmänheten om incidenter, eftersom det är tillsynsmyndigheten som har den löpande kontakten med tillsynsobjekten. Med hänsyn till CSIRT-enhetens roll i det operativa arbetet kring incidenthantering anser regeringen dock att CSIRT-enheten som utgångspunkt bör vara den myndighet som informerar allmänheten, andra medlemsstater och leverantörer om incidenter.

I avsnitt 7.2.3 och 8.2 bedömer regeringen att incidentrapportering ska ske till CSIRT-enheten. Även tillsynsmyndigheten behöver dock tillgång till information i incidentrapporter för att kunna utöva en effektiv tillsyn. I förordning bör därför införas bestämmelser om att CSIRT-enheten ska överlämna information om incidenter till respektive tillsynsmyndighet.

MSB bör som utgångspunkt vara CSIRT-enhet

Dataskydd.se, *Föreningen Swedish Network Users Society*, *Netnod* och *Svenska Stadsnätsföreningen* anser att Post- och telestyrelsen (PTS) ska vara CSIRT-enhet, bl.a. med hänsyn till att PTS enligt utredningens förslag ska vara tillsynsmyndighet för sektorn digital infrastruktur och för leverantörer av digitala tjänster. Att en myndighet är tilltänkt tillsynsmyndighet för vissa leverantörer är dock inget starkt skäl för att den också ska vara CSIRT-enhet. CSIRT-enheten ska ha uppgifter som rör alla leverantörer som omfattas av den nya lagen. Bedömningen av vilken myndighet som ska vara CSIRT-enhet bör göras utifrån faktorer såsom vilken myndighet som har förutsättningar att på ett bra sätt klara av de uppgifter som CSIRT-enheten ska ha och som till den nya lagens ikraftträdande kan uppfylla de krav som ställs på CSIRT-enheter enligt direktivet. I artikel 9 och i punkt 1 i bilaga 1 till direktivet ställs bl.a. krav på tillgång till lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur, säkerhet avseende lokaler och informationssystem, driftskontinuitet och möjligheter att delta i internationella samarbetsnätverk.

Utredningen har föreslagit att MSB ska vara CSIRT-enhet. MSB har i uppgift att svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera incidenter.

Arbetet sker genom MSB:s CERT-verksamhet (Computer Emergency Response Team) som har benämningen CERT-SE. Till CERT-SE:s uppgifter hör bl.a. att agera skyndsamt vid inträffade incidenter genom att sprida information, vid behov arbeta med samordning av åtgärder, medverka i arbetet med att avhjälpa eller lindra effekter av det inträffade och att samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet. MSB är genom CERT-SE Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder och mot den CERT-organisation som ansvarar för incidenthantering inom EU:s institutioner, CERT-EU, och ska utveckla samarbetet och informationsutbytet med dessa funktioner. Det är också MSB som tar emot de rapporter som statliga myndigheter lämnar med anledning av den obligatoriska incidentrapporteringen enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. I avvaktan på att ett tekniskt rapporteringsverktyg är driftsatt tillhandahåller MSB i dag en kryptolösning för säker kommunikation vid överföring av incidentrapporterna. Rapporteringsverktyget är tänkt att tas i bruk under våren 2018.

Mot bakgrund av det uppdrag MSB har på informationssäkerhetsområdet och den kompetens som finns inom myndigheten bedömer regeringen, liksom bl.a. *Statskontoret* och *Affärsverket Svenska kraftnät*, att MSB som utgångspunkt ska vara Sveriges CSIRT-enhet. MSB har också tillgång till sådan lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur som avses i NIS-direktivet (artikel 9.3).

Netnod, *Stiftelsen för internetinfrastruktur* och *Svenska Stadsnätsföreningen* anser att det vid sidan av CSIRT-enheten bör inrättas en haverikommission som i vissa fall ska utreda incidenter och ta reda på hur incidenter ska kunna förhindras eller lindras. Det finns dock inte beredningsunderlag för att inrätta en haverikommission inom ramen för detta lagstiftningsärende. Remissinstansernas synpunkter kan därför inte tillgodoses.

Normgivningsnivå

Utredningen har föreslagit att det i den nya lagen ska tas in en bestämmelse om att den myndighet som regeringen bestämmer ska vara CSIRT-enhet. Vidare har utredningen föreslagit att en bestämmelse som motsvarar delar av artikel 16.7 i NIS-direktivet, om att CSIRT-enheten får begära att en leverantör av digitala tjänster informerar allmänheten om en incident, ska föras in i den nya lagen.

Regeringen anser inte att det finns skäl att i den nya lagen föra in en bestämmelse som upplyser om att regeringen får utse CSIRT-enhet. Vidare innebär artikel 16.7 enligt regeringens uppfattning inte någon skyldighet för enskilda. Det finns därför inte heller någon anledning att föra in en bestämmelse i den nya lagen som motsvarar artikel 16.7. Bestämmelser om vilken myndighet som ska vara CSIRT-enhet och CSIRT-enhetens befogenheter och uppgifter bör således enligt regeringens bedömning meddelas i förordning. Flera remissinstanser har synpunkter på hur CSIRT-enhetens uppgifter närmare bör utformas. Dessa synpunkter kommer att beaktas i det fortsatta förordningsarbetet.

11.3 NIS-direktivets samarbetsgrupp

Regeringens bedömning: Bestämmelser om vilken myndighet som ska företräda Sverige i den samarbetsgrupp som inrättats genom NIS-direktivet och de uppgifter som företrädaren ska ha bör meddelas i förordning.

Utredningens förslag stämmer överens med regeringens bedömning.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens bedömning: Genom NIS-direktivet inrättades en samarbetsgrupp, bl.a. för att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna (artikel 1.2 b).

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 (artikel 11.2).

Samarbetsgruppen har de uppgifter som följer av artikel 11.3 i direktivet. Det rör sig om uppgifter såsom att utbyta information och bästa praxis om forskning och utveckling vad gäller säkerhet i nätverk och informationssystem, årligen diskutera de sammanfattande rapporter om incidenter som de nationella kontaktpunkterna ska ge till samarbetsgruppen och att hjälpa medlemsstaterna att tillämpa ett enhetligt tillvägagångssätt i förfarandet för identifiering av leverantörer av samhällsviktiga tjänster.

MSB företräder för närvarande Sverige i samarbetsgruppen. Med hänsyn till det och mot bakgrund av det uppdrag som MSB har i dag på informationssäkerhetsområdet, bör MSB som utgångspunkt företräda Sverige i samarbetsgruppen även fortsättningsvis. Utredningen har inte föreslagit någon författningsreglering avseende vilken myndighet som ska vara Sveriges företrädare och de uppgifter som företrädaren ska ha. I det fortsatta förordningsarbetet bör det dock övervägas om uppgiften bör regleras i myndighetsinstruktion eller i annan förordning.

12 Sekretess

12.1 Behövs ett starkare skydd för uppgifter som leverantörer ska rapportera vid en incident och tillhandahålla vid tillsyn?

Regeringens bedömning: Befintliga bestämmelser om sekretess i offentlighets- och sekretesslagen utgör ett tillräckligt skydd för uppgifter som leverantörer ska rapportera med anledning av en incident och tillhandahålla vid tillsyn. Någon förändring av bestämmelserna behövs därför inte.

Utredningens bedömning stämmer överens med regeringens.

Remissinstanserna: Några remissinstanser, såsom *Dataskydd.net*, *Journalistförbundet*, *Norrköpings kommun* och *Utgivarna*, delar utredningens bedömning eller anser att befintligt sekretesskydd bör vara svagare. Ett flertal remissinstanser, bland dem *Datainspektionen*, *Försvarets radioanstalt*, *Försvarsmakten*, *Myndigheten för samhällsskydd- och beredskap (MSB)* och *Sveriges advokatsamfund* menar att befintligt sekretesskydd, särskilt sekretessen enligt 18 kap. 8 § 3 offentlighets- och sekretesslagen, förkortad OSL, bör vara starkare.

Skälen för regeringens bedömning

Uppgifter som leverantörer ska överlämna till myndigheter vid en incident och vid tillsyn

Leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster kommer enligt den nya lagen om informationssäkerhet för samhällsviktiga och digitala tjänster vara skyldiga att rapportera incidenter till den myndighet som regeringen bestämmer. Utgångspunkten är att rapporteringen ska ske till CSIRT-enheten vid MSB och att CSIRT-enheten sedan ska överlämna information om incidenter till aktuell tillsynsmyndighet. Det kan röra sig om uppgifter om namn och kontaktuppgifter på den som rapporterat, beskrivning av incidenten, uppgift om incidenten är pågående eller avslutad samt en bedömning av incidentens konsekvenser.

Som framgår av avsnitt 9.3.1 kommer leverantörer även att till tillsynsmyndigheten behöva tillhandahålla information som är nödvändig för tillsynen, såsom uppgifter om säkerhets- och bevakningsåtgärder, styrande dokument och resultat av genomförda säkerhetsrevisioner.

Med anledning av att den information som leverantörer kommer vara skyldiga att överlämna till olika myndigheter kan vara skyddsvärd, finns det anledning att överväga om de sekretessbestämmelser som kan bli tillämpliga ger ett väl avvägt skydd eller om någon av dem bör ändras.

Befintligt sekretesskydd

Den i sammanhanget kanske mest relevanta sekretessbestämmelsen finns i 18 kap. 8 § 3 OSL. Enligt den bestämmelsen gäller sekretess för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd som avser system för automatiserad behandling av information, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs. Bestämmelsen är tillämplig både hos en myndighet som upprättar och skickar in en incidentrapport och hos den myndighet som tar emot en incidentrapport. Motsvarande gäller när sådana uppgifter tillhandahålls i samband med en tillsyn.

Som exempel på säkerhets- eller bevakningsåtgärder nämns i förarbetena 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. Som exempel på uppgifter som kan bidra till att lämna upplysningar om säkerhets- eller bevakningsåtgärder nämns t.ex. uppgift om vilken typ och

version av operativsystem som använts. Sådana uppgifter kan enligt förarbetena 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, eftersom en utomstående genom uppgifterna kan få information om hur man kringgår de vidtagna skyddsåtgärderna. Enligt förarbetena kan bestämmelsen också innebära att uppgifter om vem som gett in en incidentrapport avseende säkerhetsbrister i it-system omfattas av sekretess, eftersom det innebär en uppgift om att ingivarens it-system är sårbart (prop. 2003/04:93 s. 82 f.).

Förutom uppgifter om säkerhets- och bevakningsåtgärder 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. Enligt 18 kap. 9 § OSL gäller sekretess 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 att göra det möjligt att kontrollera om data i elektronisk form har förvanskats.

Inom ramen för incidentrapportering och tillsyn kan leverantörer även behöva lämna uppgifter som rör deras ekonomiska verksamhet. Enligt 30 kap. 23 § 1 OSL gäller sekretess, i den utsträckning regeringen meddelar föreskrifter om det, i en statlig myndighets verksamhet som består i tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt för uppgift om en enskilds affärs- eller driftförhållanden, om det kan antas att den enskilde lider skada om uppgiften röjs. Det bör noteras att tillsynsbegreppet i OSL är vitt. Det omfattar i stort alla de fall där en myndighet har en övervakande eller styrande funktion i förhållande till näringslivet. Den typ av uppgifter som det i första hand handlar om att sekretessbelägga med stöd av bestämmelsen är uppgifter som typiskt sett kan vara av intresse för konkurrenter och som skulle skada verksamheten om de blev kända. Regeringen har i 9 § offentlighets- och sekretessförordningen (2009:641) och i bilagan till förordningen meddelat föreskrifter om i vilken utsträckning sekretess enligt 30 kap. 23 § 1 OSL gäller. I bilagan listas bl.a. tillsyn och stödverksamhet hos MSB och tillsyn hos Post- och telestyrelsen och Transportstyrelsen. I det fortsatta förordningsarbetet, i vilket det bl.a. ska fastslås vilka myndigheter som ska vara tillsynsmyndigheter, kommer regeringen att överväga om och hur offentlighets- och sekretessförordningen behöver ändras för att skydd för leverantörers affärs- eller driftförhållanden ska finnas hos samtliga myndigheter som kommer att ta emot incidentrapporter eller utöva tillsyn enligt den nya lagen.

Förutom ovan nämnda bestämmelser finns det flera andra sekretessbestämmelser som kan aktualiseras. Bland annat kan bestämmelserna om sekretess för det allmännas ekonomiska intresse i 19 kap. 1 § OSL, utrikessekretess i 15 kap. 1 § OSL, sekretess i det internationella samarbetet i 15 kap. 1 a § OSL och försvarssekretess i 15 kap. 2 § OSL vara tillämpliga i vissa situationer. Försvarssekretess kan exempelvis aktualiseras hos MSB i egenskap av CSIRT-enhet och hos tillsynsmyndigheten. 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. MSB kan i egenskap av CSIRT-enhet t.ex. komma att hantera uppgifter om incidenter som sammantaget ger en sådan bild av samhällets infrastruktur att det kan antas utgöra en sådan fara för Sveriges säkerhet om de röjs att försvarssekretess gäller.

Är det befintliga sekretesskyddet tillräckligt starkt?

Befintliga bestämmelser om sekretess i OSL är enligt regeringens mening tillräckligt omfattande. Frågan är i stället om befintligt sekretesskydd är tillräckligt starkt.

Flera remissinstanser, såsom *Datainspektionen*, *Försvarsmakten*, *Försvarets radioanstalt*, *MSB*, *Socialstyrelsen*, *Stiftelsen för internetinfrastruktur*, *Svenskt Näringsliv*, *Svenskt vatten* och *Trafikverket*, anser att det krävs eller kan finnas behov av ett starkare skydd. De flesta av dessa remissinstanser påtalar särskilt behovet av ett starkare skydd för säkerhets- och bevakningsåtgärder i 18 kap. 8 § OSL. Som skäl för att sekretesskyddet bör vara starkare anför bl.a. Datainspektionen, Försvarsmakten, MSB, Socialstyrelsen och Stiftelsen för internetinfrastruktur att en för svag sekretess kan göra att aktörer väljer att inte incidentrapportera eller att lämna knapphändig information i sina incidentrapporter. Andra remissinstanser, såsom Försvarets radioanstalt och Socialstyrelsen, pekar på svårigheten att i ett tidigt skede bedöma om uppgifter i incidentrapporter är säkerhetskänsliga och att – för det fall en säkerhetskänslig uppgift röjs – skadan är svår att reparera i efterhand. Det finns också ett antal remissinstanser som anser att befintligt skydd är tillräckligt starkt, bland dem *Dataskydd.net*, *Journalistförbundet* och *Utgivarna*. De framhäver i stället behovet av att incidenter och andra sårbarheter offentliggörs, bl.a. för att det finns ett allmänintresse av att it-relaterade hot uppmärksammas och utreds, men också för att främja kunskapsutvecklingen på området och för att skapa incitament till egenkontroll.

Sekretessens styrka bestäms i regel med hjälp av s.k. skaderekvisit. Man skiljer mellan raka och omvända skaderekvisit. Samtliga ovan nämnda bestämmelser är, i likhet med flertalet sekretessbestämmelser i OSL, försedda med raka skaderekvisit. Det innebär att utgångspunkten är att uppgifterna är offentliga och att sekretess bara gäller om det kan antas att en viss skada uppkommer om uppgiften röjs. Ett rakt skaderekvisit innebär normalt att det är uppgifternas karaktär som får avgöra om sekretess gäller eller inte. Om uppgiften är sådan att den genomsnittligt sett måste betraktas som harmlös ska den alltså normalt anses vara offentlig. Om uppgiften i stället typiskt sett måste betraktas som känslig omfattas den normalt av sekretess. Bestämmelser med omvända skaderekvisit är utformade med utgångspunkt att sekretess gäller, om det inte står klart att uppgiften kan röjas utan att viss skada uppstår. Sekretessen enligt en bestämmelse kan även vara absolut. Vid absolut sekretess ska uppgifter som omfattas av bestämmelsen hemlighållas oavsett skada. Någon skadeprövning ska alltså inte göras i dessa fall.

Den omständigheten att samtliga ovan beskrivna sekretessbestämmelser är försedda med ett rakt skaderekvisit innebär inte att sekretesskyddet är svagt. Ett rakt skaderekvisit innebär visserligen att en presumtion för

offentlighet gäller. Presumtionen för offentlighet bryts emellertid om det kan antas att en sådan skada som anges i sekretessbestämmelsen uppstår om uppgiften röjs. Uppgiften är då sekretessbelagd och får inte utan särskilt lagstöd lämnas ut eller röjas muntligen.

Vad specifikt avser det skydd som det raka skaderekvisitet i 18 kap. 8 § 3 OSL innebär, kan konstateras att en uppgift om vem som har lämnat en incidentrapport i många fall är en upplysning om att ingivarens nätverk och informationssystem är sårbara för attacker. Uppgiften om vem som har lämnat in en sådan rapport utgör alltså i sig en uppgift som kan omfattas av sekretessens föremål enligt 18 kap. 8 § 3 OSL, eftersom den lämnar upplysning om att ingivarens säkerhetsåtgärder har brister. I många fall kan det antas att leverantörens säkerhetsåtgärder motverkas om det framkommer att dessa har brister. Bestämmelsens skaderekvisit är i sådana situationer uppfyllt, varvid sekretess gäller. Som flera remissinstanser påpekar kan det vara svårt att i ett tidigt skede bedöma om uppgifter i incidentrapporter är säkerhetskänsliga. Det är dock en svårighet som de flesta sekretessprövningar är behäftad med och motiverar inte i sig ett starkare skydd. Det har inte heller framkommit exempel på att 18 kap. 8 § 3 OSL har tillämpats på ett sådant sätt att det i sig motiverar en starkare sekretess. Det kan även konstateras att regeringen i propositionen Ny dataskyddslag (prop. 2017/18:105) har bedömt att 18 kap. 8 § 3 OSL ger ett tillräckligt skydd för uppgifter som kommer att rapporteras till Datainspektionen vid en personuppgiftsincident, dvs. en säkerhetsincident som oavsiktligt påverkar behandlingen av personuppgifter.

Enligt regeringens mening tillgodoser konstruktionen med ett rakt skaderekvisit i de relevanta sekretessbestämmelserna allmänhetens berättigade intresse av insyn i CSIRT-enhetens och tillsynsmyndighetens verksamhet, eftersom harmlösa uppgifter får lämnas ut. Samtidigt tillgodoser bestämmelserna leverantörers berättigade intresse av diskretion, eftersom uppgifter inte får röjas om det kan antas leda till skada.

Mot denna bakgrund anser regeringen att befintliga sekretessbestämmelser i OSL ger ett väl avvägt skydd. Remissinstansernas argument om att det finns en risk för att vissa leverantörer kommer att avstå från att rapportera incidenter eller endast lämna knapphändig information föranleder inte någon annan bedömning. Någon förändring av bestämmelserna i OSL behövs därför inte. Det bör dock framhållas att det är viktigt att det görs en noggrann prövning enligt relevanta sekretessbestämmelser innan uppgifter lämnas ut.

12.2 Behövs ytterligare reglering för att tillgodose NIS-direktivets krav på informationsutbyte med andra medlemsstater och kommissionen?

Regeringens bedömning: Befintliga bestämmelser i offentlighets- och sekretesslagen tillgodoser NIS-direktivets krav på utlämnande av uppgifter till andra medlemsstater och till kommissionen. Detsamma gäller för kraven på skydd av uppgifter som mottagits från andra medlemsstater.

Utredningens bedömning stämmer överens med regeringens.

Remissinstanserna: Ingen remissinstans motsätter sig utredningens bedömning.

Skälen för regeringens bedömning

Utlämnande av information till andra medlemsstater och kommissionen

I NIS-direktivet finns bestämmelser om samarbete som innebär att information som helt eller delvis omfattas av sekretess kan behöva lämnas ut till andra medlemsstater. Som framgår av avsnitt 11.1 och 11.2 kommer den svenska regleringen som genomför direktivet bl.a. innebära att den nationella kontaktpunkten ska lämna uppgifter om incidenter till den samarbetsgrupp som inrättats genom direktivet och att CSIRT-enheten ska informera andra medlemsstater om vissa incidenter. Vidare ska Sverige enligt direktivet lämna uppgifter till kommissionen om genomförandet av direktivet.

Av 8 kap. 3 § OSL framgår att en uppgift för vilken sekretess gäller får röjas för en utländsk myndighet eller en mellanfolklig organisation, om utlämnande sker i enlighet med särskild föreskrift i lag eller förordning. EU-direktiv jämställs med lag vid tillämpningen av OSL. Sekretess utgör således inget hinder för informationsutbyte med andra medlemsstater och kommissionen enligt NIS-direktivet, den nya lagen eller föreskrifter som meddelats i anslutning till lagen. Något behov av ytterligare reglering i detta avseende finns alltså inte.

Innan ett informationsutbyte sker måste dock beaktas att ett utlämnande av uppgifter inte får riskera Sveriges säkerhet. En incident som skulle ha rapporterats enligt säkerhetsskyddsregleringen men som felaktigt rapporterats enligt den nya lagen ska exempelvis inte rapporteras till andra medlemsstater eller kommissionen, eftersom de inte omfattas av NIS-direktivets rapporteringsskyldighet. Detsamma gäller för uppgifter i incidentrapporter som var för sig inte rör Sveriges säkerhet, men som tillsammans utgör en ny uppgift som är av betydelse för Sveriges säkerhet (aggregerad information).

Skydd för information från andra medlemsstater

Kommissionen, CSIRT-enheter och andra relevanta myndigheter har enligt NIS-direktivet en skyldighet att vid mellanstatligt informationsutbyte enligt direktivet bevara informationens konfidentialitet och att skydda leverantörers säkerhetsintressen och kommersiella intressen

(artiklarna 1.5, 14.5 och 16.6). När exempelvis den svenska CSIRT-enheten eller den nationella kontaktpunkten får sekretesskyddad information om en incident från en annan medlemsstat finns alltså krav på att det ska finnas skydd för informationen även i Sverige.

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, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten försämras om uppgiften röjs. Med bindande EU-rättsakt avses förordning, direktiv eller beslut. Information som tas emot från en annan medlemsstat till följd av bestämmelserna i NIS-direktivet kan således omfattas av sekretess enligt 15 kap. 1 a § OSL. Med hänsyn till det anser regeringen att befintliga regler tillgodoser kraven på att skydda leverantörers säkerhetsintressen och kommersiella intressen samt att bevara konfidentialiteten hos tillhandahållen information. Något behov av ytterligare reglering finns därför inte.

13 Ikraftträdande

Regeringens förslag: Den nya lagen ska träda i kraft den 1 augusti 2018. Ändringen i den nya lagen med anledning av förslaget till ny säkerhetsskyddslag ska träda i kraft den 1 april 2019.

Utredningens förslag stämmer inte överens med regeringens. Utredningen har föreslagit att den nya lagen ska träda i kraft den 10 maj 2018. Utredningen har inte föreslagit någon ändring i den nya lagen med anledning av förslaget till ny säkerhetsskyddslag och därför inte heller något ikraftträdande för ändringen.

Remissinstanserna: Ett antal remissinstanser påpekar att det av utredningen föreslagna ikraftträdandet endast ger berörda aktörer en mycket kort tid för att anpassa sig efter de krav på säkerhetsåtgärder och incidentrapportering som den nya lagen innebär.

Skälen för regeringens förslag: 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. Den nya lagen bör därför, även med beaktande av att ett snabbt ikraftträdande ger berörda aktörer en relativt kort tid att förbereda sig, träda i kraft så snart som lagstiftningsprocessen medger. Med hänsyn till den tid som de olika leden i lagstiftningsprocessen kan förväntas ta, anser regeringen att ett ikraftträdande är möjligt tidigast den 1 augusti 2018. Den nya lagen föreslås således träda i kraft det datumet.

Regeringen föreslår även en ändring i den nya lagen med anledning av ett förslag om ny säkerhetsskyddslag (prop. 2017/18:89). Den ändringen bör följaktligen träda i kraft samtidigt som den nya säkerhetsskyddslagen.

14 Konsekvenser

Regeringens bedömning: Säkerheten i nätverk och informationssystem stärks genom förslagen vilket medför samhällsekonomiska vinster på kort och lång sikt.

Förslagen innebär vissa ökade förvaltningskostnader för de myndigheter som får en särskild roll, t.ex. som CSIRT-enhet, nationell kontaktpunkt eller tillsynsmyndighet.

För myndigheter, kommuner, landsting och enskilda som kommer att omfattas av den nya lagens krav på säkerhetsåtgärder och incidentrapportering kan förslagen innebära något ökade kostnader och administrativa bördor. Förslagen innebär även att de allmänna förvaltningsdomstolarna får något fler arbetsuppgifter. Kostnaderna för statliga myndigheter och de allmänna förvaltningsdomstolarna bör rymmas inom befintliga ekonomiska ramar.

Utredningens bedömning stämmer i huvudsak överens med regeringens. Utredningen har till skillnad från regeringen bedömt att förslagen inte får några ekonomiska konsekvenser för de kommuner, landsting och företag som kommer att omfattas av krav på säkerhetsåtgärder och incidentrapportering.

Remissinstanserna: Flera remissinstanser instämmer i att förslagen kommer att innebära en ökad informationssäkerhet med samhällsekonomiska vinster som följd. De flesta remissinstanser som yttrar sig poängterar vikten av att tillräckliga resurser avsätts för genomförandet av NIS-direktivet. *Finansinspektionen, Myndigheten för samhällsskydd och beredskap (MSB), Livsmedelsverket* och andra myndigheter som av utredningen har pekats ut till att ha en särskild roll, poängterar vikten av att de tillförs medel som står i proportion till ökade arbetsuppgifter. Flera remissinstanser, såsom *Energiföretagen Sverige, Svenskt Näringsliv, Svenskt vatten, Trafikverket, Tågoperatörerna, Sveriges Kommuner och Landsting* och ett antal kommuner och landsting, anser till skillnad från utredningen att förslagen om krav på säkerhetsåtgärder och incidentrapportering kommer att innebära kostnader för statliga myndigheter, kommuner, landsting och företag. *Kammarrätten i Stockholm* anser att det kan ifrågasättas om de ökade kostnaderna för de allmänna förvaltningsdomstolarna kan finansieras inom befintliga ekonomiska ramar.

Skälen för regeringens bedömning

Stärkt säkerhet i nätverk och informationssystem

Säkerheten i nätverk och informationssystem är grundläggande för ekonomisk och samhällelig verksamhet och i synnerhet för Sveriges och den inre marknadens funktion. Regeringens förslag om krav på bl.a. säkerhetsåtgärder och incidentrapportering bidrar till att åka säkerheten i nätverk och informationssystem. Eftersom åtgärderna har till syfte att säkerställa kontinuiteten i samhällsviktiga och digitala tjänster, kommer de särskilt att öka försörjningstryggheten i tjänsterna. En ökad försörjningstrygghet är till fördel för såväl myndigheter, kommuner och landsting som enskilda.

Förslagen har därför samhällsekonomiska vinster på både kort och lång sikt.

Ekonomiska konsekvenser för myndigheter som får en särskild roll

Som framgår av det föregående kommer ett antal myndigheter att få en särskild roll i genomförandet av NIS-direktivet, såsom CSIRT-enhet, nationell kontaktpunkt eller tillsynsmyndighet. Medlemsstaterna ska enligt NIS-direktivet säkerställa att CSIRT-enheterna, de nationella kontaktpunkterna och tillsynsmyndigheterna har tillräckliga resurser för att på ett effektivt sätt kunna utföra de uppgifter som de tilldelas (artiklarna 8.5, 9.2, 15.2 och 17.2).

CSIRT-enheten ska bl.a. ta emot incidentrapporter från leverantörer, övervaka incidenter på nationell nivå och vara en del i hanteringen av inträffade incidenter. Den nationella kontaktpunkten ska vara en sambandsfunktion för gränsöverskridande samarbete. Utgångspunkten är att MSB ska utses till CSIRT-enhet och nationell kontaktpunkt. MSB har redan i dag i uppdrag att ta emot och hantera statliga myndigheters incidentrapportering. I det uppdraget har också ingått att ta fram en säker kommunikations- och informationsstruktur samt att analysera inrapporterade incidenter och vid behov varna andra aktörer. Även om MSB till viss del redan har liknande uppgifter innebär uppdraget som CSIRT-enhet och nationell kontaktpunkt att MSB kommer att få utökade arbetsuppgifter. Vidare kommer regeringen i det fortsatta förordningsarbetet att överväga om MSB även ska ha andra roller, såsom att leda ett samarbetsforum för tillsynsmyndigheter som t.ex. ska bistå med metodstöd i tillsynsfrågor. Som bl.a. *MSB* påpekar är det viktigt att de medel som tillförs står i proportion till de ökade arbetsuppgifter som myndigheten får genom den nya regleringen. Det är dock förenat med svårigheter att i nuläget bedöma hur stora kostnaderna för MSB kommer att bli.

Förslagen kan även komma att innebära ökade kostnader för de tillsynsmyndigheter som ska övervaka att leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster uppfyller sina skyldigheter. Hur stora kostnaderna blir för respektive tillsynsmyndighet beror på om den aktuella tillsynsmyndigheten redan i dag utövar en likartad tillsyn. En annan viktig faktor är hur många leverantörer som tillsynsmyndighetens uppdrag omfattar. Kostnaderna för ett tillsynsuppdrag som omfattar ett fåtal leverantörer blir avsevärt lägre än ett uppdrag som omfattar flera hundra leverantörer. Oavsett antalet leverantörer kommer det initialt att uppstå kostnader för att utfärda nya föreskrifter, bygga upp ett nytt system för tillsyn alternativt komplettera ett system som redan används samt att rekrytera eller utveckla ny kompetens inom informationssäkerhetsområdet. Kostnaderna kan därför komma att bli högre i en initial fas. Att fastställa de initiala och löpande kostnaderna för tillsyn är förenat med svårigheter. En av anledningarna till det är att det är svårt att bedöma hur många leverantörer som respektive tillsynsmyndighet kommer att ha tillsyn över. Som flera remissinstanser påpekar, bland dem *Finansinspektionen* och *Livsmedelsverket*, är det viktigt att tillsynsmyndigheterna ges förutsättningar att fullgöra sina skyldigheter på ett fullgott sätt.

Med anledningen av svårigheterna att bedöma de ekonomiska konsekvenserna för tillsynen föreslog utredningen att regeringen skulle ge Statskontoret i uppdrag att utreda frågan. Regeringen gav därför den 19 oktober 2017 Statskontoret i uppdrag att utreda de ekonomiska konsekvenserna av tillsynen. I uppdraget ingår även att utreda MSB:s kostnader. Statskontoret ska redovisa uppdraget till regeringen den 15 mars 2018.

Regeringen avser att återkomma till riksdagen när det gäller kostnaderna för de myndigheter som kommer att få en särskild roll.

Ekonomiska konsekvenser för leverantörer

Den föreslagna regleringen innebär krav på leverantörer av samhällsviktiga tjänster inom sju olika sektorer och leverantörer av tre typer av digitala tjänster. Det kan röra sig om såväl offentliga aktörer, dvs. statliga myndigheter, kommuner och landsting, som företag. Förslagen om säkerhetsåtgärder medför små förändringar för vissa leverantörer eftersom de redan i dag omfattas av liknande krav, och större förändringar för andra. För de flesta av leverantörerna, med undantag för bl.a. de som är statliga myndigheter, kommer kravet på att rapportera incidenter att vara en ny uppgift. Förslagen kommer vidare att ställa högre krav på dokumentation och administrativ hantering när det gäller bedömning av lämpliga säkerhetsåtgärder samt incidentrapportering. Administrativa kostnader kommer även att uppkomma för leverantörer som blir föremål för tillsyn.

Som utredningen har påpekat kan förslagen också i viss mån bidra till minskade kostnader för leverantörer. Information om incidenter kommer bli mer tillgänglig. Vidare kommer de erfarenheter som kan dras från inträffade incidenter både nationellt och inom EU att kunna användas i det förebyggande och systematiska informationssäkerhetsarbetet. Med hänsyn till det och de föreslagna kraven på säkerhetsåtgärder kommer fler incidenter att förhindras och kostnader för och andra konsekvenser av inträffade incidenter att minska. Utredningen har med hänsyn till bl.a. nämnda kostnadsbegränsande faktorer bedömt att förslagen inte kommer att få några ekonomiska konsekvenser för leverantörerna. Regeringen anser dock, liksom bl.a. *Energiföretagen Sverige*, *Svenskt Näringsliv*, *Svenskt vatten*, *Trafikverket*, *Sveriges Kommuner och landsting*, *Tågoperatörerna* och ett antal kommuner och landsting, att förslagen ändå kan innebära vissa kostnader för leverantörer. Kostnaderna för statliga myndigheter bedöms kunna hanteras inom befintliga ekonomiska ramar. För kommuner och landsting bedöms kostnaderna vara begränsade.

Ekonomiska konsekvenser för domstolarna

Tillsynsmyndighetens beslut om föreläggande och sanktionsavgift får enligt regeringens förslag överklagas till allmän förvaltningsdomstol, vilket kan medföra en ökning av antalet mål där. Hur stor ökningen av antalet mål och följaktligen hur stora kostnaderna kommer bli är svårt att bedöma. *Kammarrätten i Stockholm* har också ifrågasatt om kostnaderna kan finansieras inom befintliga ekonomiska ramar. Regeringen bedömer ändå i nuläget att det kommer vara fråga om ett sådant begränsat antal mål att kostnaderna bör rymmas inom befintliga ekonomiska ramar.

Övriga konsekvenser

Förslagen innebär att kommuner och landsting kan bli skyldiga att vidta säkerhetsåtgärder och att rapportera incidenter. Dessa nya åligganden för kommuner och landsting innebär enligt regeringens bedömning en viss inskränkning i självstyrelsen. Med hänsyn till det stora intresset av att öka säkerheten i nätverk och informationssystem bedömer regeringen att inskränkningen måste anses nödvändig.

Kraven på säkerhetsåtgärder och incidentrapportering förebygger både avsiktliga angrepp och s.k. handhavandefel. Förslagen bör enligt regeringens mening därför leda till att it-relaterade brott förebyggs och förhindras.

Regeringen anser inte att förslagen bör medföra konsekvenser för jämställdheten mellan män och kvinnor.

15 Författningskommentar

15.1 Förslaget till lag om informationssäkerhet för samhällsviktiga och digitala tjänster

Syftet med lagen

1 §

Paragrafen tydliggör lagens syfte och att lagen genomför NIS-direktivet. Lagen reglerar inte Sveriges skyldighet enligt artikel 7 i NIS-direktivet att anta en nationell strategi för säkerhet i nätverk och informationssystem.

Paragrafen behandlas i avsnitt 5.1 och 5.2.

Uttryck i lagen

2 §

Paragrafen genomför artikel 4 i NIS-direktivet. I paragrafen anges vad som avses med vissa ord och uttryck som används i lagen.

Paragrafen behandlas i avsnitt 5.3 och 5.6.

Lagens tillämpningsområde

3 §

Paragrafen, som genomför artiklarna 5.1, 5.2, 18.1 och 18.2 i NIS-direktivet, reglerar lagens tillämpningsområde.

Av *första stycket 1* framgår att leverantörer av samhällsviktiga tjänster omfattas av lagen. För att en leverantör ska anses vara en leverantör av samhällsviktiga tjänster krävs för det första att leverantören är av det slag

som anges i bilaga 2 till NIS-direktivet. I bilagan anges olika typer av leverantörer fördelat på sju sektorer.

För det andra krävs att leverantören tillhandahåller en samhällsviktig tjänst. Vilka tjänster som ska anses som samhällsviktiga enligt lagen ska med stöd av 4 § anges i förordning eller myndighetsföreskrifter.

Vidare krävs att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Vid bedömningen av om en incident skulle innebära en betydande störning ska bl.a. beaktas det antal användare som är beroende av den samhällsviktiga tjänsten, leverantörens marknadsandel, hur stort geografiskt område som skulle kunna påverkas av en incident och hur beroende andra sektorer är av den samhällsviktiga tjänst som leverantören tillhandahåller.

Slutligen krävs att leverantören är etablerad i Sverige. För att en leverantör av samhällsviktiga tjänster ska anses vara etablerad i Sverige krävs att leverantören bedriver en faktisk och reell verksamhet med hjälp av en stabil struktur här. Den rättsliga formen för en sådan struktur är inte en avgörande faktor.

Både offentliga aktörer, som statliga myndigheter, landsting och kommuner, och privata aktörer kan utgöra leverantörer av samhällsviktiga tjänster.

Enligt *första stycket 2* omfattas även leverantörer av digitala tjänster av lagen. Med en leverantör av digitala tjänster avses en juridisk person som tillhandahåller en digital tjänst. Uttrycket digital tjänst definieras i 2 § 4. Näringsidkare som tillhandahåller egna varor och tjänster på en webbplats (e-butik) eller jämförelsesajter är inte leverantörer av digitala tjänster enligt lagen.

För att en leverantör av digitala tjänster ska omfattas av lagen krävs att leverantören har sitt huvudsakliga etableringsställe i Sverige, eller har utsett en företrädare som är etablerad här i landet. I vilka fall en leverantör ska utse en företrädare regleras i 10 §. Det huvudsakliga etableringsstället ska anses vara där leverantören har sitt faktiska huvudkontor. Att nätverk och informationssystem är fysiskt belägna på en viss plats innebär inte att det är fråga om ett huvudsakligt etableringsställe.

I *andra stycket* finns en upplysning om att lagen innehåller en bestämmelse som gäller för andra leverantörer än de som uppfyller kriterierna för att vara leverantörer av samhällsviktiga eller digitala tjänster enligt första stycket.

Paragrafen behandlas i avsnitt 5.3.

4 §

Paragrafen behandlas i avsnitt 5.3 och 6.2.

Undantag från lagens tillämpningsområde

Leverantörer av elektroniska kommunikationstjänster

5 §

Paragrafen genomför första ledet i artikel 1.3 i NIS-direktivet.

Genom paragrafen undantas företag som omfattas av kraven i 5 kap. 6 b och c §§ lagen (2003:389) om elektronisk kommunikation från lagens tillämpningsområde.

Paragrafen behandlas i avsnitt 5.4.1.

Leverantörer av betrodda tjänster

6 §

Paragrafen genomför andra ledet i artikel 1.3 i NIS-direktivet.

Genom paragrafen undantas leverantörer av betrodda tjänster som omfattas av kraven i den angivna förordningen från lagens tillämpningsområde. Med betrodda tjänster avses enligt förordningen 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.

Paragrafen behandlas i avsnitt 5.4.1.

Leverantörer av digitala tjänster som är mikroföretag eller små företag

7 §

Paragrafen genomför andra ledet i artikel 16.11 i NIS-direktivet.

Genom paragrafen undantas leverantörer av digitala tjänster som är mikroföretag eller små företag enligt definitionen i kommissionens rekommendation 2003/361/EG. Enligt rekommendationen är ett mikroföretag ett företag med färre än 10 anställda och en årsomsättning eller balansomslutning som understiger 2 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.

Paragrafen behandlas i avsnitt 5.4.1.

Säkerhetskänslig verksamhet

8 §

Paragrafen genomför artikel 1.6 i NIS-direktivet.

Genom paragrafen undantas verksamhet som omfattas av krav på säkerhetsskydd enligt säkerhetsskyddslagen (1996:627) från lagens tillämpningsområde. Det innebär bl.a. att incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen (1996:663) inte ska rapporteras enligt lagen.

Att en leverantör av samhällsviktiga eller digitala tjänster bedriver verksamhet som omfattas av säkerhetsskyddslagens krav på säkerhetsskydd betyder inte nödvändigtvis att all verksamhet är undantagen från denna lags tillämpningsområde. Om leverantören även bedriver verksamhet som inte är säkerhetskänslig kan lagen bli tillämplig i de delarna.

Paragrafen behandlas i avsnitt 5.4.2.

Leverantörer som omfattas av krav på informationssäkerhet i andra författningar

9 §

Paragrafen genomför artikel 1.7 i NIS-direktivet.

Paragrafen innebär att lagen inte ska tillämpas om det i lag eller annan författning finns bestämmelser om krav på säkerhetsåtgärder och incidentrapportering vars verkan minst motsvarar verkan av skyldigheterna enligt lagen. Med lag eller annan författning avses bl.a. EU-förordningar och myndighetsföreskrifter.

Vid bedömningen av om bestämmelser i en annan författning motsvarar verkan av skyldigheterna i lagen, bör bl.a. beaktas bestämmelsernas omfattning och syfte samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna. Motsvarande bestämmelser om säkerhetsåtgärder och incidentrapportering finns t.ex. inom sjöfartssektorn, banksektorn och sektorn för finansmarknadsinfrastruktur. Däremot motsvarar inte kraven enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap eller kraven i dataskyddsförordningen (Europaparlamentets och rådets förordning [EU] 2016/679) skyldigheterna i lagen.

Paragrafen behandlas i avsnitt 5.4.3.

Utseende av företrädare

10 §

Paragrafen genomför artikel 18.2 i NIS-direktivet.

Paragrafen reglerar skyldigheten för juridiska personer att i vissa fall utse en företrädare som är etablerad inom EU. Skyldigheten gäller för de juridiska personer som erbjuder digitala tjänster i Sverige men som inte har huvudkontor inom EU. En företrädare kan enligt definitionen i 2 § 8 vara såväl en fysisk som en juridisk person. Företrädaren ska utses uttryckligen, t.ex. genom en skriftlig fullmakt från leverantören att agera på dess vägnar när det gäller leverantörens skyldigheter enligt lagen eller NIS-direktivet. Om en juridisk person utser en företrädare som är etablerad i Sverige innebär det att den juridiska personen är en sådan leverantör av digitala tjänster som omfattas av lagen.

Paragrafen behandlas i avsnitt 5.5.

Säkerhetsåtgärder

Skyldigheter för leverantörer av samhällsviktiga tjänster

11 §

Enligt paragrafen ska leverantörer av samhällsviktiga tjänster bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete när det gäller sådana nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Det innebär att arbetet ska bedrivas lång-

siktigt, kontinuerligt och metodiskt samt att arbetet bör ha en tydlig rollfördelning med särskilt utpekat ansvar. I arbetet bör europeiska och internationellt godkända standarder beaktas. Styrande dokument som en leverantör har antagit för det systematiska informationssäkerhetsarbetet utgör sådan information som leverantören ska tillhandahålla tillsynsmyndigheten enligt 24 §.

Paragrafen behandlas i avsnitt 7.1.2.

12 §

Enligt paragrafen ska leverantörer av samhällsviktiga tjänster göra en riskanalys. Riskanalysen ska ligga till grund för valet av säkerhetsåtgärder, vilket innebär att den ska användas som beslutsstöd för leverantörers prioriteringar och avvägningar mellan olika typer av säkerhetsåtgärder.

Riskanalysen ska dokumenteras, uppdateras årligen och innehålla en åtgärdsplan. Analysen är exempel på sådan information som leverantören ska tillhandahålla tillsynsmyndigheten enligt 24 §.

Paragrafen behandlas i avsnitt 7.1.3.

13 §

Paragrafen genomför artikel 14.1 i NIS-direktivet.

Paragrafen ålägger leverantörer av samhällsviktiga tjänster att vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem. Uttrycken säkerhet i nätverk och informationssystem respektive risk definieras i 2 § 2 och 10. Tekniska åtgärder innefattar bl.a. åtgärder till skydd mot oönskad förändring av, obehörig insyn i och åtkomst till nätverk och informationssystem samt skydd av personer, lokaler och utrustning av betydelse för informationssäkerheten. I organisatoriska åtgärder ingår bl.a. att utforma rutiner, övervaka åtgärders efterlevnad och att genomföra uppföljningar. Säkerhetskraven gäller de nätverk och informationssystem som leverantören använder vid tillhandahållandet av samhällsviktiga tjänster, oavsett om denne sköter underhållet av sina nätverk och informationssystem internt eller lägger ut uppgifterna på entreprenad.

Syftet med säkerhetsåtgärderna ska vara att säkerställa en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till risken. Vid bedömningen av vad som är en lämplig nivå i förhållande till risken ska bl.a. den tekniska utvecklingen beaktas, dvs. de 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. För att säkerställa en lämplig nivå på säkerheten behöver leverantörer av samhällsviktiga tjänster regelbundet och vid behov se över vilka säkerhetsåtgärder som ska vidtas.

Paragrafen behandlas i avsnitt 7.1.4.

14 §

Paragrafen genomför artikel 14.2 i NIS-direktivet.

Enligt paragrafen ska leverantörer av samhällsviktiga tjänster vidta lämpliga åtgärder för att förebygga och minimera incidenters verkningar.

Det innefattar åtgärder som stöder upptäckt och analys av incidenter samt åtgärder för att hantera en inträffad incident. Åtgärderna ska ha till syfte att säkerställa kontinuiteten i den samhällsviktiga tjänst som leverantören tillhandahåller. Om en incident inträffar finns det som regel anledning att se över säkerhetsåtgärderna.

Paragrafen behandlas i avsnitt 7.1.5.

Skyldigheter för leverantörer av digitala tjänster

15 §

Paragrafen genomför artikel 16.1 i NIS-direktivet.

Paragrafen ålägger leverantörer av digitala tjänster att vidta vissa tekniska och organisatoriska åtgärder. Begreppen tekniska och organisatoriska åtgärder behandlas i kommentaren till 13 §.

Det är leverantören av digitala tjänster som avgör vilka konkreta åtgärder som ska vidtas. Åtgärderna ska dock hantera risker som hotar säkerheten i nätverk och informationssystem som de använder när de tillhandahåller digitala tjänster inom EU och säkerställa en nivå på säkerheten som är lämplig i förhållande till risken. Uttrycken säkerhet i nätverk och informationssystem respektive risk definieras i 2 § 2 och 10.

Vid bedömningen av vad som är en lämplig nivå i förhållande till risken ska bl.a. den tekniska utvecklingen beaktas, dvs. de tekniska lösningar som vid var tid finns tillgängliga på marknaden. För att säkerställa en lämplig nivå på säkerheten behöver leverantörer av digitala tjänster regelbundet och vid behov se över vilka säkerhetsåtgärder som ska vidtas.

Paragrafen behandlas i avsnitt 8.1.

16 §

Paragrafen genomför artikel 16.2 i NIS-direktivet.

Paragrafen innebär att leverantörer av digitala tjänster bl.a. ska vidta åtgärder som stöder upptäckt av incidenter och åtgärder för att hantera en inträffad incident. Skyldigheten avser endast incidenter som påverkar nätverk och informationssystem som leverantören använder och som har verkningar på digitala tjänster som leverantören erbjuder inom EU. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

Paragrafen behandlas i avsnitt 8.1.

Bemyndigande

17 §

I paragrafen finns ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om vad som krävs av en leverantör för att uppfylla kraven på säkerhetsåtgärder som följer av lagen. Föreskrifter som kan meddelas med stöd av detta bemyndigande är t.ex. sådana som beskriver vad ett systematiskt och riskbaserat informationssäkerhetsarbete enligt 11 § innebär och vilka faktorer som ska beaktas vid bedömningen av vad som utgör en lämplig nivå på säkerheten i nätverken och informationssystemen enligt 15 §.

Paragrafen behandlas i avsnitt 7.1.6 och 8.1.

Incidentrapportering

Rapporteringsskyldighet för leverantörer av samhällsviktiga tjänster

18 §

Paragrafen genomför artiklarna 14.3 och 16.5 i NIS-direktivet.

Enligt paragrafen är leverantörer av samhällsviktiga tjänster skyldiga att rapportera vissa incidenter. Endast incidenter med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem och som har orsakat en betydande inverkan på den samhällsviktiga tjänstens kontinuitet ska rapporteras. Incidenter som endast påverkar den samhällsviktiga tjänsten på andra sätt behöver inte rapporteras enligt denna bestämmelse. När det gäller sådana incidenter kan det dock finnas rapporteringskrav i andra regelverk. Rapporteringskravet gäller oavsett var incidenten har skett. Leverantörer av samhällsviktiga tjänster har därför en skyldighet att rapportera incidenter hos exempelvis en tredjepartsleverantör och följdincidenter på grund av en sådan incident, under förutsättning att incidenten har en betydande inverkan på den samhällsviktiga tjänst som leverantören tillhandahåller.

I paragrafen anges också att rapporteringen ska ske utan onödigt dröjsmål. Det innebär att rapporteringen som regel ska ske så snart de första kritiska åtgärderna har vidtagits för att avhjälpa incidenten och de uppgifter som ska lämnas finns tillgängliga. I de fall incidenten påverkar flera leverantörer eller är gränsöverskridande kan det krävas att rapporteringen sker snarast möjligt med följd att rapporten kan behöva kompletteras när incidenten har avhjälpts och de fullständiga uppgifter som ska lämnas finns tillgängliga.

För att incidentrapporteringen ska vara ändamålsenlig bör en rapport innehålla en beskrivning av incidenten, de åtgärder som har vidtagits för att hantera incidenten och incidentens gränsöverskridande verkningar.

Paragrafen behandlas i avsnitt 7.2.

Rapporteringsskyldighet för leverantörer av digitala tjänster

19 §

Paragrafen genomför artikel 16.3 i NIS-direktivet.

Enligt paragrafen är leverantörer av digitala tjänster skyldiga att rapportera vissa incidenter. Skyldigheten gäller endast incidenter med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem och som orsakat en avsevärd inverkan på tillhandahållandet av en digital tjänst som leverantören erbjuder inom EU.

Angående vad det innebär att incidentrapporteringen ska ske utan onödigt dröjsmål och vilken information en rapport ska innehålla, se kommentaren till 18 §.

Paragrafen behandlas i avsnitt 8.2.

Bemyndigande

20 §

I paragrafen finns ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om vad som krävs av leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster för att uppfylla kraven på incidentrapportering i lagen. Föreskrifter som kan meddelas med stöd av detta bemyndigande är t.ex. sådana som anger vilka faktorer som ska beaktas vid bedömningen av om en incident har en sådan inverkan på kontinuiteten i en samhällsviktig tjänst att den medför krav på rapportering enligt 18 §.

Paragrafen behandlas i avsnitt 7.2.7 och 8.2.

Tillsyn

Tillsynsmyndighetens uppdrag

21 §

Paragrafen genomför artikel 8.1 och 8.2 i NIS-direktivet.

Av paragrafen framgår att regeringen i förordning utser vilken eller vilka myndigheter som ska vara tillsynsmyndighet. Vidare regleras att tillsynsmyndighetens uppgift är att utöva tillsyn över lagen och de föreskrifter som har meddelats i anslutning till den. Det innebär att huvudsyftet med tillsynen är att bedöma hur leverantörerna uppfyller kraven på säkerhetsåtgärder och incidentrapportering.

Paragrafen behandlas i avsnitt 9.1 och 9.2.

22 §

Paragrafen genomför artikel 17.1 i NIS-direktivet.

Paragrafen begränsar tillsynsmyndighetens uppdrag i fråga om leverantörer av digitala tjänster. Till skillnad mot vad som gäller för leverantörer av samhällsviktiga tjänster ska tillsynsåtgärder beträffande leverantörer av digitala tjänster vidtas bara när tillsynsmyndigheten har befogad anledning att anta att leverantören inte uppfyller lagens krav. Det innebär att tillsynsmyndigheten måste ha uppgifter som ger stöd för en överträdelse. Sådana uppgifter kan tillsynsmyndigheten få t.ex. av leverantören av digitala tjänster själv, en annan tillsynsmyndighet eller en tjänsteanvändare. Även incidentrapporteringen kan innehålla information som gör att tillsynsmyndigheten har befogad anledning att anta att lagen inte följs.

Paragrafen behandlas i avsnitt 9.2.

Anmälningsskyldighet för leverantörer av samhällsviktiga tjänster

23 §

Av paragrafen framgår att leverantörer av samhällsviktiga tjänster har en skyldighet att utan dröjsmål anmäla sig till tillsynsmyndigheten. Av anmälan ska det framgå om de tillhandahåller samhällsviktiga tjänster i två eller flera medlemsstater inom EU.

Paragrafen behandlas i avsnitt 6.3.

Tillsynsmyndighetens undersökningsbefogenheter

24 §

Paragrafen genomför artiklarna 15.2 och 17.2 a i NIS-direktivet.

I paragrafen behandlas den skyldighet som leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster har att vid tillsyn tillhandahålla tillsynsmyndigheten information. Skyldigheten gäller sådan information som behövs för tillsynen. Det kan t.ex. vara fråga om risk- och säkerhetsanalyser, åtgärdsplaner, styrande dokument och genomförda säkerhetsrevisioner.

Paragrafen behandlas i avsnitt 9.3.1.

25 §

Paragrafen genomför artiklarna 15.1, 15.2 och 17.2 a i NIS-direktivet.

Paragrafen reglerar tillsynsmyndighetens rätt att få tillträde till områden, lokaler och andra utrymmen i den utsträckning det krävs för att kunna utöva tillsyn. Tillträdesrätten omfattar inte bostäder. Rätten motsvaras av en skyldighet för den som står under tillsyn att tillhandahålla begärt tillträde. Det intrång som tillträdet innebär måste stå i proportion till behovet av tillsynsåtgärden. Tillträdesrätten ger inte tillsynsmyndigheten rätt att bereda sig tillträde med tvång. Om den som står under tillsyn inte samarbetar kan dock tillsynsmyndigheten förelägga leverantören att ge tillträde vid äventyr av vite och i sista hand begära handräckning av Kronofogdemyndigheten, se 26 och 27 §§.

Paragrafen behandlas i avsnitt 9.3.2.

26 §

Paragrafen genomför artiklarna 15.1, 15.2 och 17.2 i NIS-direktivet.

Första stycket reglerar vilka förelägganden som tillsynsmyndigheten får meddela vid tillsyn. Som utgångspunkt ska dock tillsynsmyndigheten i första hand försöka få till stånd frivillig rättelse. Om det inte lyckas får tillsynsmyndigheten förelägga en leverantör att tillhandahålla information och ge tillträde enligt 24 och 25 §§.

Ett beslut om föreläggande får enligt *andra stycket* förenas med vite. När vite föreläggs är lagen (1985:206) om viten tillämplig.

Paragrafen behandlas i avsnitt 9.3.3.

27 §

Paragrafen genomför artiklarna 15.1, 15.2 och 17.2 i NIS-direktivet.

Paragrafen reglerar tillsynsmyndighetens möjlighet att begära handräckning av Kronofogdemyndigheten för att genomföra tillsynsåtgärder.

Paragrafen behandlas i avsnitt 9.3.3.

Ingripanden och sanktioner

Åtgärdsförelägganden

28 §

Paragrafen genomför artiklarna 15.3, 17.2 b och 21 i NIS-direktivet.

Enligt *första stycket* får tillsynsmyndigheten utfärda de förelägganden som behövs för att leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster ska uppfylla de krav på riskanalys, tekniska och organisatoriska åtgärder, incidenthantering och incidentrapportering som följer av lagen och av föreskrifter som har meddelats i anslutning till den. Tillsynsmyndigheten får även utfärda förelägganden när det gäller skyldigheten att utse företrädare enligt 10 §.

Ett föreläggande får enligt *andra stycket* förenas med vite. När vite föreläggs är lagen om viten tillämplig.

Paragrafen behandlas i avsnitt 10.2.

Sanktionsavgift

29 §

Paragrafen genomför artikel 21 i NIS-direktivet.

Paragrafen reglerar vid vilka överträdelser som tillsynsmyndigheten kan besluta om sanktionsavgift. Avgiftsskyldigheten bygger på strikt ansvar. Det krävs alltså varken uppsåt eller oaktsamhet för att en sanktionsavgift ska kunna tas ut. Det är tillräckligt att en överträdelse har ägt rum. Även statliga myndigheter, kommuner och landsting kan påföras sanktionsavgift.

Paragrafen behandlas i avsnitt 10.3.1.

30 §

Paragrafen genomför artikel 21 i NIS-direktivet och fastställer minimi- och maxbelopp för sanktionsavgift. Hur avgiften ska bestämmas i det enskilda fallet regleras i 31 §.

Paragrafen behandlas i avsnitt 10.3.2.

31 §

Paragrafen genomför artikel 21 i NIS-direktivet.

I paragrafen anges de omständigheter som särskilt ska beaktas när tillsynsmyndigheten bestämmer sanktionsavgiftens storlek. Uppräkningen är inte uttömmande. Utöver de i paragrafen angivna omständigheterna kan hänsyn behöva tas till hur länge överträdelsen har pågått. Det kan också vara relevant att beakta bestämmelsens betydelse för tillsynsområdet. I mildrande riktning kan det vara aktuellt att beakta om leverantören har samarbetat med tillsynsmyndigheten för att komma till rätta med överträdelsen.

Paragrafen behandlas i avsnitt 10.3.3.

32 §

Paragrafen genomför artikel 21 i NIS-direktivet.

Paragrafen ger tillsynsmyndigheten möjlighet att sätta ned sanktionsavgiften, helt eller delvis, om överträdelsen är ringa, ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut sanktionsavgift. Det kan exempelvis vara oskäligt att ta ut en avgift om den avgiftsskyldige redan har drabbats av en sanktionsavgift enligt något annat regelverk för i princip samma brist. Att regelverket har överträtts på ett sådant sätt att det varit närmast omöjligt för den avgiftsskyldige att upptäcka överträdelsen eller överträdelsen på annat sätt varit utom den avgiftsskyldiges kontroll, kan i undantagsfall göra överträdelsen ursäktlig och därför utgöra grund för jämkning. Det är däremot inte oskäligt att ta ut en sanktionsavgift när överträdelsen exempelvis berott på att en leverantör inte känt till reglerna eller överträdelsen berott på dålig ekonomi, tidsbrist eller bristande rutiner.

Paragrafen behandlas i avsnitt 10.3.3.

33 §

Paragrafen genomför artikel 21 i NIS-direktivet.

Paragrafen syftar till att förhindra att samma överträdelse blir föremål för dubbla prövningar och sanktioner. Om ett vitesföreläggande har meddelats och föreläggandet inte följs, kan tillsynsmyndigheten välja att ansöka om utdömande av vitet eller att besluta om sanktionsavgift om förutsättningarna för det är uppfyllda. När en domstolsprocess inleds om utdömande av vitet är dock tillsynsmyndigheten enligt bestämmelsen förhindrad att besluta om sanktionsavgift för samma överträdelse.

Paragrafen behandlas i avsnitt 10.3.4.

34 §

Paragrafen genomför artikel 21 i NIS-direktivet.

Paragrafen reglerar bl.a. den bortre tidsgränsen för när en sanktionsavgift får beslutas.

Första stycket innebär att om kommunikation enligt förvaltningslagen (2017:900) med den som avgiften ska tas ut av inte har skett inom två år från överträdelsen, får en sanktionsavgift inte tas ut. Bevisbördan för att kommunikation har skett ligger på tillsynsmyndigheten. Tidsfristen räknas från när överträdelsen ägde rum.

Av *andra stycket* framgår att ett beslut om sanktionsavgift ska delges den avgiftsskyldige. Det innebär att myndigheten ska använda sig av de metoder för delgivning som regleras i delgivningslagen (2010:1932) för att säkerställa att den som beslutet gäller får del av underrättelsen.

Paragrafen behandlas i avsnitt 10.3.5.

35 och 36 § §

Paragraferna genomför artikel 21 i NIS-direktivet och reglerar betalning och indrivning av sanktionsavgifter.

Paragraferna behandlas i avsnitt 10.3.5.

Föreskrifter om verkställighet

37 §

Paragrafen upplyser om att det finns en möjlighet för regeringen eller den myndighet som regeringen bestämmer att meddela verkställighetsföreskrifter. Exempelvis kan närmare föreskrifter meddelas om formerna för anmälningsskyldigheten enligt 23 § och när i tiden en sådan anmälan ska ske, formerna för incidentrapportering enligt 18 och 19 §§ och vilken information som den som står under tillsyn är skyldig att tillhandahålla tillsynsmyndigheten enligt 24 §.

Paragrafen behandlas i avsnitt 6.2.

Förordnande om att beslut ska gälla omedelbart

38 §

Paragrafen innebär en möjlighet för tillsynsmyndigheten att i enskilda fall bestämma att ett beslut om föreläggande ska gälla omedelbart. Den som beslutet gäller har vid ett överklagande av ett sådant beslut möjlighet att begära att beslutet tills vidare inte ska gälla, s.k. inhibition. Bestämmelser om inhibition finns i 28 § förvaltningsprocesslagen (1971:291).

Paragrafen behandlas i avsnitt 10.4.

Överklagande

39 §

Paragrafen reglerar rätten att överklaga beslut enligt lagen och behandlas i avsnitt 10.5.

15.2 Förslaget till lag om ändring i lagen (2018:000) om informationssäkerhet för samhällsviktiga och digitala tjänster

8 §

Paragrafen innehåller undantag från lagens tillämpningsområde. Hänvisningen i paragrafen ändras till följd av att säkerhetsskyddslagen (1996:627) ersätts av en ny säkerhetsskyddslag.

Ändringen behandlas i avsnitt 5.4.2.

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.

Sammanfattning av betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2015:36)

Bakgrund

I juli 2016 antog Europaparlamentet och rådet NIS-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.

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 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.

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 utformningen 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 förelägganden, 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 (CSIRTenheter)*. 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 CSIRTenhet 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 tillsynsmyndigheternas 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.

Förslag till lag om informationssäkerhetför vissa tillhandahållare av samhällsviktiga 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 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.

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerheten i nätverks- och informationssystem i hela unionen i den ursprungliga lydelsen.

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 DNStjänster 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.

Förteckning över remissinstanserna

Remissinstanser som har gett in yttrande

Affärsverket Svenska kraftnät, Attunda tingsrätt, Bodens kommun, Datainspektionen, Datskydd.net, Eon AB, E-hälsomyndigheteten, E-legitimationsnämnden, Energiföretagen Sverige, Energigas Sverige, Energimarknadsinspektionen, Finansinspektionen, Fortifikationsverket, Försvarets materielverk, Försvarets radioanstalt, Försvarshögskolan, Försvarsmakten, Förvaltningsrätten i Stockholm, Göteborgs kommun, Halmstads kommun, Helsingborgs kommun, Inspektionen för vård och omsorg, It- och telekomföretagen, Journalistförbundet, Justitiekanslern, Jönköpings läns landsting, Kalmar läns landsting, Kammarrätten i Stockholm, Kiruna kommun, Kungl. Tekniska Högskolan, Kustbevakningen, Lantmäteriet, Linköpings kommun, Livsmedelsverket, Luftfartsverket, Luleå kommun, Läkemedelsverket, Länsstyrelsen i Blekinge län, Länsstyrelsen i Stockholms län, Länsstyrelsen i Skåne län, Länsstyrelsen i Västra Götalands län, Malmö kommun, Myndigheten för samhällsskydd och beredskap, Nasdaq Stockholm AB, Netnod, Norrköpings kommun, Polismyndigheten, Post- och telestyrelsen, Riksgäldskontoret, Riksrevisionen, , Statistiska centralbyrån, SJ AB, Sjöfartsverket, Skåne läns landsting, SME-D, Södermanlands läns landsting, Socialstyrelsen, Statens servicecenter, Statens veterinärmedicinska anstalt, Statens energimyndighet, Statskontoret, Stiftelsen för internetinfrastruktur, Stockholms läns landsting, Stockholms kommun, Stockholms universitet, Strålsäkerhetsmyndigheten, Sveriges advokatsamfund, Svea hovrätt, Swedegas AB, Svenska bankföreningen, Svenska Petroleum och Biodrivmedel Institutet, Svenskt Näringsliv, Svenskt vatten, Sveriges Hamnar, Sveriges Kommuner och Landsting, Säkerhets- och försvarsföretagen, Säkerhetspolisen, Totalförsvarets forskningsinstitut, Trafikverket, Transportstyrelsen, Tågoperatörerna, Vänersborgs kommun, Västra Götalands läns landsting och Östhammars kommun.

Övriga som har yttrat sig

Advenica, Frobbit AB, Föreningen Swedish Network Users Society, Swedish Association och Civil Security, Svenska Stadsnätsföreningen, och Utgivarna.

Remissinstanser som uttryckligen har avstått från att yttra sig

Riksdagens ombudsmän, Karlstads kommun och Regelrådet.

Remissinstanser som inte har gett in något yttrande

Uppsala universitet, Kronobergs läns landsting, Norrbottens läns landsting, Östergötlands läns landsting, Eskilstuna kommun, Flens kommun, Gotlands kommun, Gävle kommun, Karlsborgs kommun, Karlskrona kommun, Leksands kommun, Nynäshamn kommun, Sigtuna kommun, Svedala kommun, Västerås kommun, Älvsbyns kommun, ACR Aviation Capacity Resourses AB, COWI AB, IP-only, Preem AB, Svensk handel, Swedavia, Transportföretagen och Vårdföretagarna.