EUROPEISKA
KOMMISSIONEN

Bryssel den 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

BILAGA

till

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

Maximalt utnyttjande av it-säkerhetsdirektivet – mot ett effektivt genomförande av direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen

INNEHÅLLSFÖRTECKNING

BILAGA

1. Inledning.

Syftet med denna bilaga är att bidra till effektivare tillämpning, genomförande och kontroll av efterlevnaden av direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen[1] (nedan kallat *direktivet* eller *it-säkerhetsdirektivet*) och att hjälpa medlemsstaterna att säkerställa att EU-lagstiftningen tillämpas på ett effektivt sätt. Närmare bestämt finns har bilagan följande tre specifika syften: a) Att förtydliga för de nationella myndigheterna vilka skyldigheter som de har enligt direktivet. b) Att säkerställa en effektiv kontroll av efterlevnaden av direktivets skyldigheter avseende säkerhetskrav och incidentrapportering. c) Att generellt bidra till rättssäkerhet för alla berörda aktörer.

Därför innehåller denna bilaga vägledning om följande aspekter, som är avgörande för att vi ska uppnå direktivets mål, dvs. en hög gemensam säkerhetsnivå för nät- och informationssystem i EU, som behövs för att vårt samhälle och vår ekonomi ska fungera.

- Medlemsstaternas skyldighet att anta en nationell strategi avseende säkerhet i nät- och informationssystem (avsnitt 2).
- Inrättandet av nationella behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter (*Computer Security Incident Response Teams*) (avsnitt 3).
- De krav avseende säkerhet och incidentrapportering som gäller för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster (avsnitt 4).
- Förhållandet mellan direktivet och annan lagstiftning (avsnitt 5).

Som underlag för denna vägledning har kommissionen använt material och analyser som togs fram i samband med utarbetandet av direktivet samt synpunkter från Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och samarbetsgruppen. Man har också använt sig av erfarenheterna från enskilda medlemsstater. Kommissionen har vid behov beaktat grundprinciperna för tolkning av EU-lagstiftning: direktivets formuleringar, sammanhang och syften. Eftersom direktivet fortfarande inte har införlivats finns det ännu inte några domslut från Europeiska unionens domstol eller nationella domstolar. Därmed är det inte möjligt att använda rättspraxis som vägledning.

I och med att informationen sammanställs i ett enda dokument får medlemsstaterna en god överblick över direktivet och kan beakta denna information när de utarbetar sin nationella lagstiftning. Samtidigt betonar kommissionen att denna bilaga inte är bindande och inte avser att skapa nya regler. Det är domstolen som har den slutliga befogenheten att tolka EU-lagstiftningen.

[1] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. Direktivet trädde i kraft den 8 augusti 2016.

2. Nationell strategi för säkerhet i nät- och informationssystem

Enligt artikel 7 i direktivet ska varje medlemsstat anta en nationell strategi för säkerhet i nät- och informationssystem som kan anses motsvara begreppet nationell it-säkerhetsstrategi (*NCSS*). Den nationella strategins funktion är att fastställa strategiska mål och lämpliga politiska åtgärder och lagstiftningsåtgärder på cybersäkerhetsområdet. NCSS är ett begrepp som använts allmänt internationellt och i Europa, i synnerhet i samband med Enisas samarbete med medlemsstaterna om nationella strategier, som nyligen resulterade i en uppdaterad vägledning för bästa NCSS-praxis[2].

I detta avsnitt specificerar kommissionen hur direktivet förbättrar medlemsstaternas beredskap genom att ålägga dem att ta fram robusta nationella strategier för säkerhet i nät- och informationssystem (artikel 7). Följande aspekter kommer att behandlas: a) Strategins räckvidd. b) Strategins innehåll och förfarandet för antagande.

Såsom förklaras nedan är ett korrekt införlivande av artikel 7 i direktivet grundläggande för att direktivets mål ska kunna uppnås, och därför måste tillräckliga finansiella och mänskliga resurser avsättas för detta.

2.1. Den nationella strategins räckvidd

Enligt formuleringen i artikel 7 gäller skyldigheten att anta en NCSS endast för de sektorer som avses i bilaga II (dvs. energi, transport, bankverksamhet, finansmarknad, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur) och de tjänster som avses i bilaga III (internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster).

I artikel 3 i direktivet fastställs uttryckligen minimiharmonisering som princip, vilket innebär att medlemsstaterna får anta eller behålla bestämmelser som syftar till att uppnå en högre säkerhetsnivå för nät- och informationssystem. När denna princip tillämpas på skyldigheten att anta en NCSS innebär det att medlemsstaterna kan inkludera fler sektorer och tjänster än de som omfattas av bilagorna II och III till direktivet.

Kommissionen förespråkar mot bakgrund av direktivets syfte, som är att uppnå en hög gemensam säkerhetsnivå för nät- och informationssystem i hela unionen[3], att det ska utarbetas en nationell strategi som omfattar alla relevanta dimensioner av samhället och ekonomin, och inte bara de sektorer och digitala tjänster som omfattas av bilagorna II och III till direktivet. Detta överensstämmer med internationell bästa praxis (se ITU:s vägledning och OECD:s analys som det hänvisas till nedan) och med direktivet.

Såsom vidare förklaras nedan gäller detta särskilt för offentliga förvaltningar som ansvarar för andra sektorer och tjänster än de som förtecknas i bilagorna II och III till direktivet. Offentliga förvaltningar kan behandla känsliga uppgifter som behöver täckas av en NCSS och

[2] Enisa, *National Cyber-Security Strategy Good Practice* 2016). Finns på https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
[3] Se artikel 1.1.

förvaltningsplaner som förhindrar läckor och säkerställer ett lämpligt skydd av dessa uppgifter.

2.2. De nationella strategiernas innehåll och förfarandet för antagande.

Enligt artikel 7 i direktivet behöver en NCSS omfatta åtminstone följande:

i) Målen och prioriteringarna i den nationella strategin för säkerhet i nät- och informationssystem.
ii) En styrningsram för att uppnå målen och prioriteringarna i den nationella strategin.
iii) Identifiering av beredskaps-, svars- och återhämtningsåtgärder, inklusive samarbete mellan offentlig och privat sektor.
iv) Uppgift om program för utbildning och åtgärder för ökad medvetenhet.
v) Uppgift om forsknings- och utvecklingsplaner.
vi) En riskbedömningsplan för identifiering av risker.
vii) En förteckning över de olika aktörer som deltar i genomförandet av strategin.

Varken artikel 7 eller skäl 29 specificerar kraven för antagande av en NCSS eller förklarar mer ingående vad en NCSS ska innehålla. När det gäller förfarandet och ytterligare aspekter kopplade till innehållet i NCSS anser kommissionen att det tillvägagångssätt som anges nedan är ett lämpligt sätt att anta en NCSS. Detta baseras på en analys av medlemsstaters och tredjeländers erfarenheter av hur medlemsstater har utarbetat sina egna strategier. En ytterligare informationsresurs är Enisas NCSS-utbildningsverktyg som finns som videoklipp eller kan laddas ned från byråns webbplats[4].

2.3. Förfarande och frågor att behandla

Förfarandet för utarbetande och antagande av en nationell strategi är komplext och mångfacetterat och kräver kontinuerliga kontakter med cybersäkerhetsexperter, det civila samhället och den nationella politiska processen för att det ska vara effektivt och framgångsrikt. En viktig förutsättning är administrativt stöd på hög nivå, åtminstone på statssekreterarnivå eller motsvarande hos det ansvariga departementet, liksom politiskt stöd. För ett framgångsrikt antagande av en NCSS kan man överväga följande femstegsprocess (se figur 1):

Steg ett – **Fastställande av vägledande principer och strategiska mål för strategin.**

För det första bör de nationella behöriga myndigheterna fastställa några nyckelaspekter som ska ingå i NCSS, nämligen de önskade resultaten (eller som det formuleras i artikel 7.1 a i direktivet: *”Målen och prioriteringarna”*), hur dessa resultat kompletterar social och ekonomisk politik på nationell nivå och om de är förenliga med de rättigheter och skyldigheter som följer av landets medlemskap i Europeiska unionen. Målen ska vara specifika, mätbara, uppnåeliga, realistiska och tidsbestämda (*specific, measurable, achievable, realistic and time-bound, Smart*) Ett åskådligt exempel är följande: ”*Vi kommer*

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool.

att se till att denna [tidsbestämda] strategi baseras på en strikt och heltäckande uppsättning indikatorer mot vilka vi kan mäta utvecklingen mot de resultat som vi ska uppnå”[5].

Ovanstående innefattar också en politisk bedömning av om det är möjligt att få en budget som räcker för genomförandet av strategin. Det innefattar också en beskrivning av strategins planerade räckvidd och de olika kategorier av intressenter från offentlig och privat sektor som bör delta när de olika målen och åtgärderna formuleras.

Steg ett bör uppnås genom fokuserade workshoppar med höga departementstjänstemän och politiker under ledning av cyberspecialister med kommunikationskompetens som kan belysa konsekvenserna för en modern digital ekonomi och ett modernt samhälle om cybersäkerhet saknas eller är bristfällig.

Steg två - **Utarbetande av innehållet i strategin.**

Strategin bör innefatta möjliggörande åtgärder, tidsbestämda åtgärder och nyckelindikatorer för den utvärdering, finjustering och förbättring som ska göras efter en definierad genomförandeperiod. Dessa åtgärder bör främja de mål, prioriteringar och resultat som fastställts som vägledande principer. I artikel 7.1 c i direktivet fastställs att möjliggörande åtgärder måste ingå.

Det rekommenderas att man bildar en styrgrupp under ledning av det ansvariga ministeriet för att leda processen med att utarbeta planen och för att underlätta inhämtning av synpunkter. Detta kan göras med hjälp av ett antal grupper av berörda tjänstemän och experter som samlas kring nyckelteman för att utarbeta planen, t.ex. temana riskbedömning, beredskapsplanering, incidenthantering, kompetensutveckling, informationsåtgärder och industriell utveckling. Separat skulle varje enskild sektor (t.ex. energi och transport) också inbjudas att analysera konsekvenserna av att deras sektor tas med, och utsedda leverantörer av samhällsviktiga tjänster och nyckelleverantörer av digitala tjänster skulle delta i fastställandet av prioriteringar och lämna förslag till arbetet. Det är viktigt att intressenter från olika sektorer deltar också med tanke på att direktivet måste genomföras på ett harmoniserat sätt i alla sektorer, samtidigt som hänsyn tas till de olika sektorernas särdrag.

Steg tre - **Utarbetande av en styrningsram.**

För att vara effektiv och ändamålsenlig måste styrningsramen baseras på nyckelaktörer, prioriteringar som identifierats under arbetets gång och på de nationella förvaltningarnas och politiska strukturernas begränsningar och sammanhang. Det är önskvärt att det finns direktrapportering till den politiska nivån och att ramen har en kapacitet för beslutsfattande och resursfördelning, samt att cybersäkerhetsexperter och branschaktörer kan komma med synpunkter. Artikel 7.1 b i direktivet hänvisar till styrningsramen och specificerar att den ska innefatta *”offentliga organs och andra berörda aktörers roller och ansvarsområden”*.

[5] Utdrag ur FN:s nationella cybersäkerhetsstrategi, 2016–2021, s. 67.

Steg fyra - **Sammanställande och granskning av utkastet till strategi.**

I detta steg bör utkastet till strategi sammanställas och granskas med hjälp av en Swot-analys (strategins starka och svaga sidor samt möjligheter och hot). På grundval av denna kan man sedan fastställa om innehållet måste revideras. Efter den interna granskningen bör samråd hållas med intressenterna. Det är viktigt att också genomföra ett offentligt samråd för att förmedla den föreslagna strategins betydelse till allmänheten, få in synpunkter från alla tänkbara källor och söka stöd så att tillräckliga resurser kan avsättas för genomförandet.

Steg fem – **Formellt antagande.**

Detta slutliga steg omfattar det formella antagandet på politisk nivå tillsammans med en tillräcklig budget som återspeglar den betydelse som den berörda medlemsstaten fäster vid cybersäkerheten. För att uppnå direktivets mål uppmanar kommissionen medlemsstaterna att också tillhandahålla uppgifter om budgeten när de sänder sina nationella strategidokument till kommissionen i enlighet med artikel 7.3. Åtaganden avseende budgeten och de nödvändiga personalresurserna är helt avgörande för ett effektivt genomförande av strategin och direktivet. Eftersom cybersäkerhet är ett tämligen nytt och snabbt växande politikområde krävs i de flesta fall nya investeringar även om det allmänna läget i de offentliga finanserna föranleder nedskärningar och besparingar.

Flera offentliga och akademiska källor innehåller råd som kan underlätta arbetsprocessen och fastställandet av innehåll när det gäller de nationella strategierna, t.ex. Enisa[6], ITU[7], OECD[8], Global Forum for Cyber Expertise och University of Oxford[9].

2.4. Konkreta åtgärder som medlemsstaterna måste vidta innan tidsfristen för införlivande löper ut

Innan direktivet antogs hade nästan alla medlemsstater[10] redan offentliggjort dokument som betecknades som NCSS. I avsnitt 6 i denna bilaga förtecknas de strategier som för närvarande gäller i varje medlemsstat[11]. De innehåller vanligtvis strategiska principer, riktlinjer och mål,

---

[6] Enisa, *National Cyber-Security Strategy Good Practice* 2016). Finns påhttps://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[7] ITU, *National Cybersecurity Strategy Guide* (2011). Finns på http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
ITU kommer också att lägga fram en ”verktygslåda” för nationella cybersäkerhetsstrategier under 2017 (se presentation påhttp://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

[8] OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (2012). Finns på: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

[9] Global Cyber Security Capacity Centre och University of Oxford, Global Cyber, *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition* (2016). Finns på: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf.

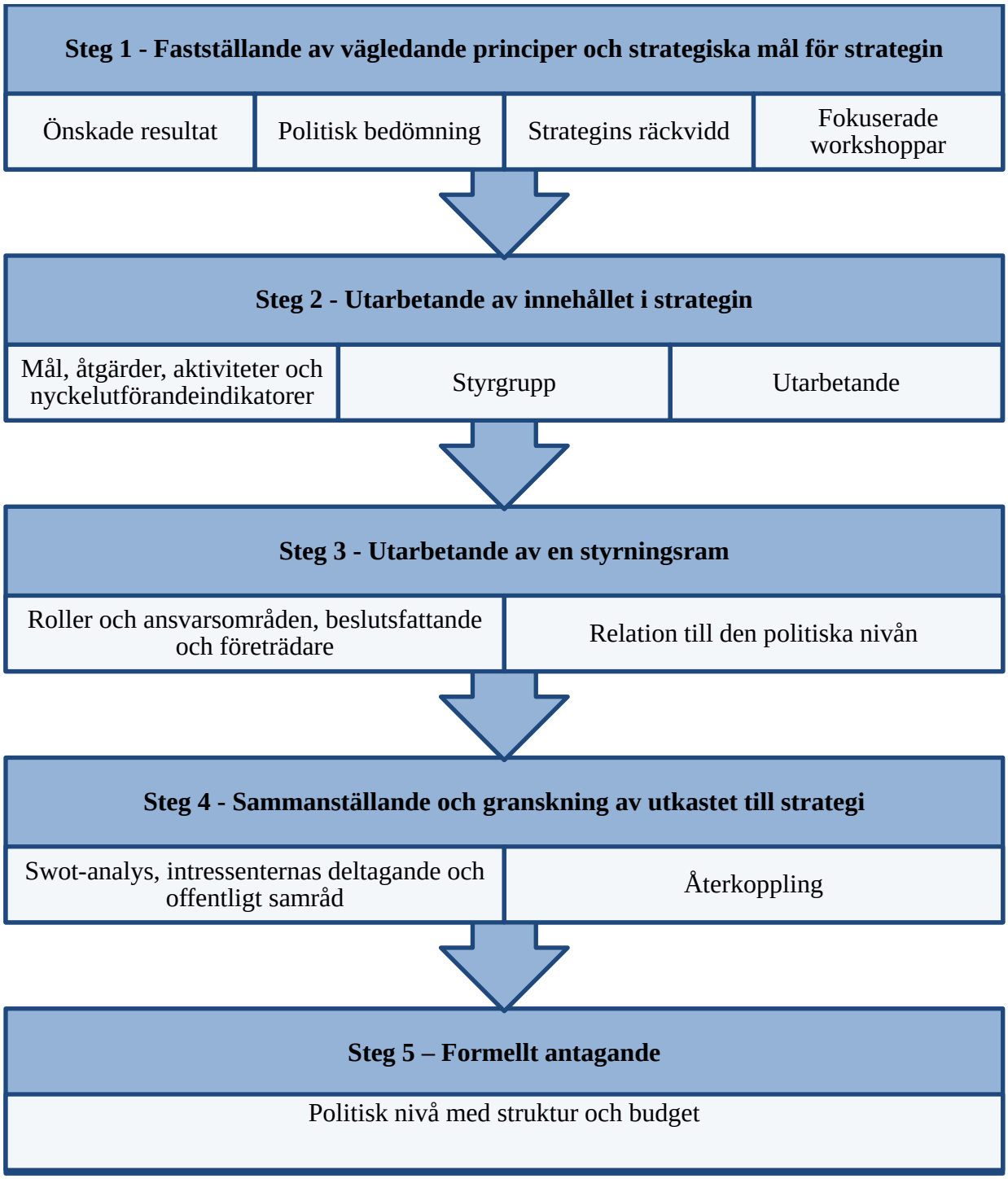
[10] Förutom Grekland, som håller på med utarbetandet av en nationell cyberstrategi sedan 2014 (se på https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Denna information baseras på en NCSS-översikt som tillhandahålls av Enisa påhttps://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

och i en del fall särskilda åtgärder för att begränsa de risker som är förbundna med cybersäkerheten.

I och med att en del av dessa strategier antogs före direktivet omfattar de inte nödvändigtvis alla aspekter som anges i artikel 7. För att säkerställa ett korrekt införlivande kommer medlemsstaterna att behöva göra en gapanalys och analysera innehållet i sin NCSS i förhållande till de sju distinkta krav som anges i artikel 7 inom alla sektorer som anges i bilaga II till direktivet och alla tjänster som anges i bilaga III. Identifierade brister kan sedan åtgärdas genom ändring av medlemsstatens befintliga NCSS eller genom beslut om en komplett översyn av principerna i medlemsstatens nationella strategi för nät- och informationssäkerhet från grunden. Vägledningen ovan avseende förfarandet för antagande av NCSS gäller också för ändring och uppdatering av befintlig NCSS.

Figur 1: Femstegsförfarande för antagande av NCSS



3. Direktiv (EU) 2016/1148: Nationella behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter (*Computer Security Incident Response Teams*).

Enligt artikel 8.1 ska medlemsstaterna utse en eller flera nationella behöriga myndigheter för säkerhet i nät- och informationssystem, som täcker minst de sektorer som avses i bilaga II till direktivet och de tjänster som avses i bilaga III, vilka har till uppgift att övervaka

tillämpningen av direktivet. Medlemsstaterna kan tilldela en eller flera befintliga myndigheter denna roll.

Detta avsnitt fokuserar på hur direktivet förbättrar medlemsstaternas beredskap genom kravet på effektiva nationella behöriga myndigheter och CSIRT-enheter. Närmare bestämt behandlas skyldigheten att utse nationella behöriga myndigheter, inklusive den gemensamma kontaktpunktens roll. Följande tre ämnen diskuteras: a) Tänkbara nationella styrningsstrukturer (centraliserade eller decentraliserade modeller) och andra krav. b) Den gemensamma kontaktpunktens roll. c) CSIRT-enheter.

3.1. Typ av myndigheter

Enligt artikel 8 i direktivet ska medlemsstaterna utse nationella behöriga myndigheter för säkerhet i nät- och informationssystem och det sägs uttryckligen att det är möjligt att utse ”*en eller flera nationella behöriga myndigheter* ”. I skäl 30 i direktivet förklaras varför man gjort detta val: ”*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.”*

Därmed kan medlemsstaterna välja att utse en central myndighet som hanterar alla sektorer och tjänster som omfattas av direktivet eller flera myndigheter, beroende på exempelvis typen av sektor.

När medlemsstaterna beslutar hur de ska göra kan de utnyttja de nationella erfarenheterna från arbetet med den befintliga lagstiftningen om skydd av kritisk infrastruktur. Såsom beskrivs i tabell 1 beslutade medlemsstaterna då att ha antingen ett centraliserat eller ett decentraliserat angreppssätt när de fördelade befogenheterna på nationell nivå. Nationella exempel används här endast som illustration och för att uppmärksamma medlemsstaterna på vilka organisatoriska ramar som finns i dag. Kommissionen menar alltså inte nödvändigtvis att medlemsstaterna måste använda samma modell som för skydd av kritisk infrastruktur när de införlivar direktiv (EU) 2916/1148.

Medlemsstaterna kan också välja att kombinera olika delar av såväl centraliserade som decentraliserade tillvägagångssätt. Deras val kan göras utifrån tidigare nationella förvaltningsarrangemang för de olika sektorer och tjänster som omfattas av direktivet eller helt oberoende av dessa fastställas av de berörda myndigheterna och de intressenter som identifierats som leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. Förekomsten av specialistkunskaper om cybersäkerhet, resurshänsyn, förhållandet mellan intressenterna och nationella intressen (t.ex. ekonomisk utveckling och allmän säkerhet) kan också vara viktiga faktorer som styr medlemsstaternas val.

3.2 Offentlighet och ytterligare relevanta aspekter.

Enligt artikel 8.7 måste medlemsstaterna underrätta kommissionen om utnämningen av nationella behöriga myndigheter och deras uppgifter. Detta måste göras inom tidsfristen för införlivande.

Enligt artiklarna 15 och 17 i direktivet ska medlemsstaterna säkerställa att behöriga myndigheter har de befogenheter och medel de behöver för att utföra de uppgifter som anges i artiklarna.

Utnämningen av specifika enheter till nationella behöriga myndigheter måste också offentliggöras. Direktivet specificerar inte hur offentliggörandet ska ske. Syftet med det här kravet är att uppnå en hög nivå av medvetenhet hos de aktörer som omfattas av direktivet och hos allmänheten, och därför anser kommissionen, baserat på erfarenheter från andra sektorer (telekommunikation, banksektor, läkemedel), att det kan uppnås t.ex. genom en portal som det informeras brett om.

Enligt artikel 8.5 i direktivet ska sådana myndigheter ha ”tillräckliga resurser” för att utföra de uppgifter som de tilldelas enligt direktivet.

Tabell 1: Nationella tillvägagångssätt för att skydda kritisk informationsinfrastruktur

År 2016 offentliggjorde Enisa en studie[12] om medlemsstaternas olika tillvägagångssätt för att skydda sin kritiska informationsinfrastruktur. När det gäller styrelseformerna för skyddet av kritisk informationsinfrastruktur i medlemsstaterna finns det två beskrivna profiler som kan användas i samband med införlivandet av direktivet.

Profil 1: Decentraliserat tillvägagångssätt – med flera sektorsbaserade myndigheter som har behörighet för specifika sektorer och tjänster som anges i bilagorna II och III till direktivet.

Det decentraliserade tillvägagångssättet karakteriseras av följande:

(i) Subsidiaritetsprincipen.
(ii) Starkt samarbete mellan offentliga organ.
(iii)Sektorsspecifik lagstiftning.

Subsidiaritetsprincipen.

I stället för att inrätta eller utse en enda myndighet med övergripande ansvar bygger det decentraliserade tillvägagångssättet på subsidiaritetsprincipen. Det innebär att ansvaret för genomförandet ligger hos en sektorsspecifik myndighet, som har bäst grepp om den lokala sektorn och som redan har etablerade relationer till intressenterna. Enligt subsidiaritetsprincipen fattas beslut av den som är närmast de som påverkas.

Starkt samarbete mellan offentliga organ.

Eftersom en mängd olika myndigheter sysslar med skydd av kritisk informationsinfrastruktur tog många medlemsstater fram samarbetssystem för att samordna de olika myndigheternas arbete och insatser. Dessa samarbetssystem kan ha formen av informella nätverk eller mer institutionaliserade forum eller arrangemang. Samarbetssystemen används dock endast för informationsutbyte och samordning mellan olika offentliga organ, de har inga befogenheter över dem.

Sektorsspecifik lagstiftning.

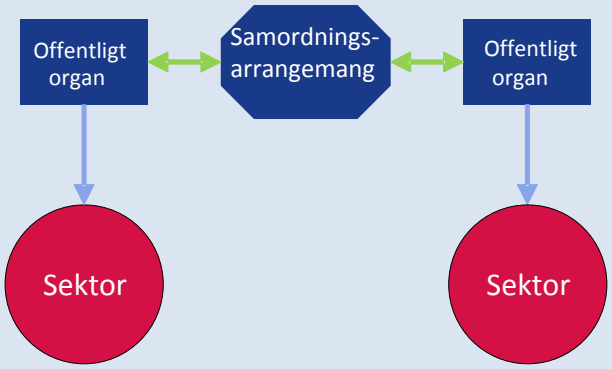
De länder som tillämpar ett decentraliserat tillvägagångssätt på samhällsviktiga sektorer avstår ofta från lagstiftning om skydd av kritisk informationsinfrastruktur. I stället förblir lagar och andra förordningar sektorsspecifika och kan därmed variera mycket mellan olika sektorer. Det har fördelen att åtgärder kopplade till direktivet anpassas till befintlig sektorsbaserad lagstiftning vilket ökar acceptansen hos sektorn och effektiviserar den berörda myndighetens kontroll av efterlevnaden.

Det finns en avsevärd risk för minskad enhetlighet i direktivets tillämpning på olika sektorer och tjänster med ett rent decentraliserat tillvägagångssätt. I sådana fall föreskriver direktivet en

[12] Enisa, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (2016). Finns på: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

gemensam kontaktpunkt för gränsöverskrivande frågor. Den berörda medlemsstaten kan också ge denna enhet i uppdrag att sköta den interna samordningen och samarbetet mellan de olika nationella behöriga myndigheterna, i enlighet med artikel 10 i direktivet.

Figur 2 – Decentraliserat tillvägagångssätt.



Exempel på decentraliserat tillvägagångssätt.

Sverige är ett bra exempel på ett land som hanterar skyddet av kritisk informationsinfrastruktur på ett decentraliserat sätt. Landet tillämpar ett ”systemperspektiv”, vilket innebär att det är olika organ och kommuner som ansvarar för de viktigaste aspekterna av skyddet, t.ex. identifiering av väsentliga tjänster och kritiska infrastrukturer, samordning och stöd till leverantörer, regleringsuppgifter och beredskapsåtgärder. Några av dessa organ är Myndigheten för samhällsskydd och beredskap (MSB), Post- och telestyrelsen (PTS) och flera myndigheter på områdena försvar, militär och brottsbekämpning.

För att samordna åtgärderna mellan olika myndigheter och offentliga enheter har den svenska regeringen utvecklat ett samarbetsnätverk som utgörs av myndigheter med ”särskilt ansvar för samhällsinformationssäkerheten”. Samverkansgruppen för informationssäkerhet (Samfi), som består av företrädare för olika myndigheter, sammanträder flera gånger om året för att diskutera nationella informationssäkerhetsfrågor. Samfi hanterar i första hand politiskt-strategiska områden och sådana ämnen som tekniska frågor och standardisering, nationell och internationell utveckling på informationssäkerhetsområdet och hantering och förebyggande av it-incidenter. (Myndigheten för samhällsskydd och beredskap (MSB) 2015).

Sverige har inte offentliggjort någon central lagstiftning om skydd av kritisk informationsinfrastruktur som är tillämplig på leverantörer av sådan infrastruktur inom alla sektorer. Det är i stället respektive offentlig myndighet som utfärdar lagstiftning med skyldigheter för företag inom enskilda sektorer. MSB har t.ex. rätt att utfärda bestämmelser för statliga myndigheter på informationssäkerhetsområdet, medan PTS kan ålägga operatörer att genomföra vissa tekniska eller organisatoriska säkerhetsåtgärder baserat på sekundärlagstiftning.

Ett annat exempel på ett land som motsvarar delar av den här profilen är Irland. Irland tillämpar en ”subsidiaritetsdoktrin” som innebär att varje ministerium har ansvaret för identifiering av kritisk informationsinfrastruktur och riskbedömning inom sin egen sektor. Man har inte heller antagit någon särskild lagstiftning om detta på nationell nivå. Lagstiftningen är sektorsbaserad och omfattar i första hand energisektorn och telesektorn (2015). Andra exempel är Österrike, Cypern och Finland.

Profil 2: Centraliserat tillvägagångssätt – med en central myndighet vars behörighet omfattar alla sektorer och tjänster som anges i bilagorna II och III till direktivet.

Det centraliserade tillvägagångssättet karakteriseras av följande:

i) En central myndighet för alla sektorer.
ii) Övergripande lagstiftning.

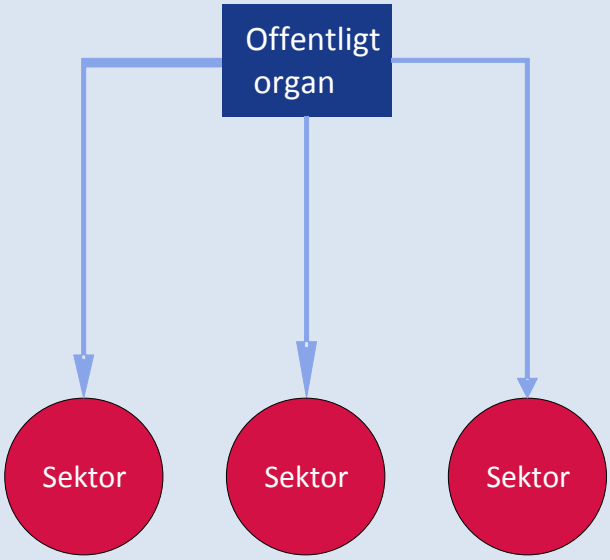
Central myndighet för alla sektorer.

Medlemsstater med ett centraliserat tillvägagångssätt har inrättat myndigheter med ansvarsområden och bred kompetens som omfattar flera eller alla kritiska sektorer, eller har utvidgat befintliga myndigheters befogenheter. Myndigheterna med huvudansvar för skyddet av kritisk informationsinfrastruktur sköter en mängd uppgifter, såsom beredskapsplanering, katastrofhantering, regleringsuppgifter och stöd till privata operatörer. I många fall ingår den nationella eller statliga CSIRT-enheten i denna huvudmyndighet. En central myndighet kommer antagligen att ha en högre koncentration av sakkunskap på cybersäkerhetsområdet än myndigheter för enskilda sektorer, med tanke på det allmänna underskottet av cybersäkerhetskompetens.

Övergripande lagstiftning.

I övergripande lagstiftning fastställs skyldigheter och krav för alla operatörer av kritisk informationsinfrastruktur i alla sektorer. Detta kan uppnås genom ny övergripande lagstiftning eller genom komplettering av sektorsspecifik lagstiftning. Detta främjar en konsekvent tillämpning av direktivet på samtliga sektorer och tjänster som omfattas. Det undanröjer de risker för luckor i genomförandet som skulle kunna uppstå med flera olika myndigheter med specifika ansvarsområden.

Figur 3 – Centraliserat tillvägagångssätt.



Exempel på centraliserat tillvägagångssätt.

Frankrike är ett bra exempel på en EU-medlemsstat med ett centraliserat tillvägagångssätt. Frankrikes Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) utsågs 2011 till nationell huvudmyndighet för försvaret av informationssystem. ANSSI har en stark tillsynsroll för ”operatörer av stor vikt”: Myndigheten kan beordra sådana operatörer att genomföra säkerhetsåtgärder och har befogenhet att göra säkerhetsrevision hos dem. Den fungerar också som gemensam kontaktpunkt för dessa operatörer, som är skyldiga att rapportera säkerhetsincidenter till myndigheten.

Vid säkerhetsincidenter fungerar ANSSI som beredskapsmyndighet när det gäller skyddet av kritisk informationsinfrastruktur och beslutar om de åtgärder som leverantörer måste vidta vid en kris. Statens åtgärder samordnas inom Anssis operativa centrum. På operativ nivå är det CERT-FR, som är en del av Anssi, som ansvarar för att upptäcka hot och reagera på incidenter.

Frankrike har antagit en övergripande rättslig ram för skyddet av kritisk informationsinfrastruktur. År 2006 bestämde premiärministern att det skulle upprättas en förteckning över sektorer med kritisk infrastruktur. Baserat på den här förteckningen, där tolv viktiga sektorer identifierades, har regeringen utsett omkring 250 operatörer av stor vikt. 2013 utfärdades lagen om militär programmering[13]. Där fastställs olika skyldigheter för operatörer av stor vikt, bl.a. rapportering av incidenter och genomförande av säkerhetsåtgärder. Dessa krav är obligatoriska för alla sådana operatörer i alla sektorer (franska senaten 2013).

[13] La loi de programmation militaire.

3.3. Artikel 9 i direktivet: Enheter för hantering av it-säkerhetsincidenter (*CSIRT-enheter*).

Enligt artikel 9 ska varje medlemsstat utse en eller flera CSIRT-enheter som anförtros ansvaret för hantering av risker och incidenter för de sektorer som förtecknas i bilaga II till direktivet och de tjänster som förtecknas i bilaga III. Med beaktande av kravet på minimiharmonisering enligt artikel 3 i direktivet har medlemsstaterna möjlighet att utnyttja CSIRT-enheterna även för sektorer som inte omfattas av direktivet, såsom den offentliga förvaltningen.

Medlemsstaterna kan välja att inrätta en CSIRT-enhet inom den nationella behöriga myndigheten[14].

3.4. Uppgifter och krav

De utsedda CSIRT-enheternas uppgifter, som anges i bilaga I till direktivet, omfattar bl.a. följande:

- Övervakning av incidenter på nationell nivå.
- Tillhandahållande av tidiga varningar, larm, meddelanden och informationsspridning till relevanta aktörer om risker och incidenter.
- Svarsåtgärder vid incidenter.
- Tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet.
- Deltagande i det nätverk av nationella CSIRT-enheter (CSIRT-nätverket) som inrättas enligt artikel 12.

Specifika ytterligare uppgifter anges i artiklarna 14.3, 14.5, 14.6, 16.3, 16.6 och 16.7 i fråga om incidentrapportering i de fall då en medlemsstat bestämmer att CSIRT-enheterna kan ha en sådan roll vid sidan av eller i stället för de nationella behöriga myndigheterna.

Vid införlivandet av direktivet har medlemsstaterna olika alternativ avseende CSIRT-enheternas roll i samband med incidentrapporteringskrav. Obligatorisk direktrapportering till CSIRT-enheter är möjlig och fördelen med det är administrativ effektivitet. Alternativt kan medlemsstaterna välja att ha direktrapportering till nationella behöriga myndigheter och ge CSIRT-enheterna åtkomsträtt till den rapporterade informationen. CSIRT-enheterna är i grund och botten intresserade av problemlösning när det gäller att avskräcka från, upptäcka, vidta åtgärder mot och begränsa konsekvenserna av cyberincidenter (inklusive sådana som inte är kritiska för obligatorisk rapportering) tillsammans med berörda parter, medan kontrollen av efterlevnaden är en fråga för de nationella behöriga myndigheterna.

[14] Se artikel 9.1 sista meningen.

I enlighet med artikel 9.3 i direktivet behöver medlemsstaterna också säkerställa att sådana CSIRT-enheter har tillgång till en säker och motståndskraftig IKT-infrastruktur.

Enligt artikel 9.4 i direktivet ska medlemsstaterna underrätta kommissionen om sina CSIRT-enheters uppgifter samt om huvudinslagen i deras incidenthanteringsförfarande.

De krav som gäller för de CSIRT-enheter som utses av medlemsstaterna anges i bilaga I till direktivet. En CSIRT-enhet måste ge en hög nivå av tillgång till sina kommunikationstjänster. De lokaler och informationssystem som enheten använder ska lokaliseras till säkra platser och kunna säkerställa driftskontinuitet. CSIRT-enheten bör kunna delta i internationella samarbetsnätverk.

3.5. Bistånd för utvecklingen av CSIRT-enheter.

Programmet för infrastruktur för digitala tjänster när det gäller cybersäkerhet (DSI) inom Fonden för ett sammanlänkat Europa (FSE) kan tillhandahålla betydande EU-finansiering för att hjälpa medlemsstaternas CSIRT-enheter att förbättra sin kapacitet och sitt samarbete med varandra genom en samarbetsmekanism för informationsutbyte. Den samarbetsmekanism som håller på att utvecklas inom Smart-projektet 2015/1089 är avsedd att främja ett snabbt och effektivt operativt samarbete på frivillig grund mellan medlemsstaternas CSIRT-enheter, bl.a. till stöd för de uppgifter som nätverket av CSIRT-enheter anförtros enligt artikel 12 i direktivet.

Närmare uppgifter om de berörda ansökningsomgångarna avseende uppbyggnad av kapaciteten för medlemsstaternas CSIRT-enheter finns på webbplatsen för Europeiska kommissionens genomförandeorgan för innovation och nätverk (Inea)[15].

Styrelsen för DSI-programmet ger en informell struktur på policynivå för vägledning och bistånd till medlemsstaternas CSIRT-enheter med sikte på kapacitetsuppbyggnad samt för införandet av den frivilliga samarbetsmekanismen.

En CSIRT-enhet som är nyinrättad eller som utsetts för att utföra uppgifterna i bilaga I till direktivet kan förlita sig på rådgivning och expertis från Enisa för att förbättra sitt arbetssätt och effektivt utföra sina uppgifter[16]. I detta hänseende är det viktigt att påpeka att medlemsstaternas CSIRT-enheter kan använda en del av det arbete som Enisa gjort på senare tid som referens. Såsom anges i avsnitt 7 i denna bilaga har Enisa i synnerhet utfärdat ett antal dokument och studier som beskriver goda arbetsmetoder och tekniska rekommendationer som omfattar bedömning av CSIRT-mognadsgraden, för olika CSIRT-kompetenser och tjänster. Vägledning och goda arbetsmetoder har också utbytts i CSIRT-nätverken på både global (First[17]) och europeisk nivå (Trusted Introducer, TI[18]).

[15] Finns på: https://ec.europa.eu/inea/en/connecting-europe-facility.
[16] Se artikel 9.5 i direktivet.
[17] Forum of Incident Response and Security Teams (https://www.first.org/).
[18] https://www.trusted-introducer.org/.

3.6. Den gemensamma kontaktpunktens roll.

Enligt artikel 8.3 i direktivet måste varje medlemsstat utse en gemensam nationell kontaktpunkt, som ska utöva en sambandsfunktion för att säkerställa gränsöverskridande samarbete med berörda myndigheter i andra medlemsstater, med samarbetsgruppen och med det CSIRT-nätverk[19] som inrättas genom samma direktiv. I skäl 31 och artikel 8.4 förklaras motivet bakom detta krav, dvs. att främja gränsöverskridande samarbete och kommunikation. Det är särskilt viktigt eftersom medlemsstaterna kan besluta att ha mer än en nationell myndighet. En gemensam kontaktpunkt kan alltså göra det lättare att identifiera och samarbeta med myndigheter från olika medlemsstater.

Den gemensamma kontaktpunktens sambandsfunktion innefattar sannolikt samverkan med sekretariaten för samarbetsgruppen och CSIRT-nätverket i de fall då den gemensamma nationella kontaktpunkten varken är en CSIRT-enhet eller en av samarbetsgruppens medlemmar. Medlemsstaterna måste också säkerställa att den gemensamma kontaktpunkten underrättas om de rapporter som inkommer från leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster[20].

I artikel 8.3 föreskrivs att om en medlemsstat bara utser en behörig myndighet, ska denna behöriga myndighet också ha uppgiften att vara gemensam kontaktpunkt. Om en medlemsstat väljer ett decentraliserat upplägg kan den välja att utse en av de olika behöriga myndigheterna till gemensam kontaktpunkt. Oavsett vilken institutionell modell som väljs är medlemsstaterna, om CSIRT-enheten och den gemensamma kontaktpunkten inte är samma enhet, skyldiga att säkerställa ett effektivt samarbete mellan dessa för att uppfylla de skyldigheter som fastställs i direktivet.[21]

Den gemensamma kontaktpunkten ska senast den 9 augusti 2018 och därefter varje år lämna en sammanfattande rapport till samarbetsgruppen om de rapporter som inkommit. Den ska omfatta antalet rapporter, arten av incidenter och de åtgärder som vidtagits av myndigheterna, t.ex. att underrätta andra berörda medlemsstater om incidenten eller informera det rapporterande företaget med tanke på hanteringen av incidenten.[22] På begäran av den behöriga myndigheten eller CSIRT-enheten ska den gemensamma kontaktpunkten vidarebefordra rapporter från leverantörer av samhällsviktiga tjänster till de gemensamma kontaktpunkterna i andra medlemsstater som berörs av incidenten[23].

Medlemsstaterna måste underrätta kommissionen om utnämningen av den gemensamma kontaktpunkten samt om dess uppgifter inom tidsfristen för införlivandet. Utnämningen av en gemensam kontaktpunkt ska tillkännages på samma sätt som utseendet av de nationella behöriga myndigheterna. Kommissionen ska offentliggöra förteckningen över utsedda gemensamma kontaktpunkter.

---

[19] Ett nätverk av nationella CSIRT-enheter för operativt samarbete mellan medlemsstaterna enligt artikel 12.
[20] Se artikel 10.3.
[21] Se artikel 10.1.
[22] Se föregående.
[23] Se artikel 14.5.

3.7. Sanktioner.

Artikel 21 ger medlemsstaterna utrymme att bestämma typen och arten av tillämpliga sanktioner förutsatt att dessa är effektiva, proportionella och avskräckande. Med andra ord är medlemsstaterna i princip fria att besluta om maximibelopp för sanktioner som fastställs i deras nationella lagstiftning, men det belopp eller den procentsats som väljs bör ge de nationella myndigheterna möjlighet att i varje konkret fall fastställa effektiva, proportionella och avskräckande sanktioner, med beaktande av olika faktorer såsom överträdelsens allvarlighetsgrad eller frekvens.

4. Enheter som omfattas av skyldigheter avseende säkerhetskrav och incidentrapportering.

Enheter som har stor betydelse för samhället och ekonomin enligt artikel 4.4 och 4.5 i direktivet, såsom leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, måste vidta ändamålsenliga säkerhetsåtgärder och rapportera allvarliga incidenter till de berörda nationella myndigheterna. Skälet är att säkerhetsincidenter inom sådana tjänster kan ha en inverkan som utgör ett allvarligt hot mot driften av sådana tjänster, vilket kan orsaka allvarliga störningar av ekonomisk verksamhet och samhället som helhet, vilket potentiellt kan undergräva användarnas förtroende och allvarligt skada ekonomin i unionen[24].

Detta avsnitt innehåller en översikt över enheter som omfattas av bilagorna II och III till direktivet och förtecknar deras skyldigheter. Identifieringen av leverantörer av samhällsviktiga tjänster behandlas ingående, med tanke på vilken betydelse denna process har för det harmoniserade genomförandet av direktivet i EU. Avsnittet innehåller ingående förklaringar till definitionerna av digitala infrastrukturer och leverantörer av digitala tjänster. Där granskas också ett eventuellt inkluderande av ytterligare sektorer och förklaras mer ingående det särskilda tillvägagångssättet när det gäller leverantörer av digitala tjänster.

4.1. Leverantörer av samhällsviktiga tjänster.

I direktivet definieras inte uttryckligen vilka specifika enheter som kommer att anses som leverantörer av samhällsviktiga tjänster vilka omfattas av direktivet. I stället anges kriterier som medlemsstaterna ska tillämpa för att genomföra ett identifieringsförfarande där det slutligen fastställs vilka enskilda företag av den typ av enheter som anges i bilaga II som kommer att anses som leverantörer av samhällsviktiga tjänster och som därför omfattas av skyldigheterna enligt direktivet.

4.1.1 Typer av enheter som förtecknas i bilaga II till direktivet.

Enligt artikel 4.4 definieras en leverantör av samhällsviktiga tjänster som en offentlig eller privat enhet av en typ som avses i bilaga II vilken uppfyller kriterierna i artikel 5.2. I bilaga II förtecknas sektorer, delsektorer och typer av enheter för vilka medlemsstaterna måste

[24] Se skäl 2.

genomföra ett identifieringsförfarande enligt artikel 5.2[25]. Sektorerna är bl.a. energi, transport, finansmarknad, infrastruktur, hälso- och sjukvård, vatten och digital infrastruktur.

För de flesta enheter som tillhör ”traditionella sektorer” omfattar EU-lagstiftningen välutvecklade definitioner som det hänvisas till i bilaga II. Detta gäller dock inte för sektorn för digital infrastruktur, som anges i punkt 7 i bilaga II, inklusive internetknutpunkter, domännamnssystem och registerenheter för toppdomäner. För att förtydliga dessa definitioner ge därför en ingående förklaring nedan.

1) Internetknutpunkt (IXP).

Begreppet internetknutpunkt, som definieras i artikel 4.13 och förtydligas i skäl 18, kan beskrivas som en nätfacilitet som möjliggör sammankoppling av mer än två oberoende tekniskt autonoma system, främst i syfte att underlätta utbytet av internettrafik. Internetknutpunkten kan också beskrivas som en fysisk plats där ett antal nät kan utbyta internettrafik med varandra via en växel. Internetknutpunktens huvudsyfte är att göra det möjligt att koppla samman nätverk direkt med varandra, via knutpunkten, i stället för att gå via ett eller flera tredjepartsnät. IXP-leverantören ansvarar normalt inte för dirigeringen av internettrafiken. Det görs av nätleverantörerna. Det finns många fördelar med direkt sammankoppling, men de främsta skälen är kostnad, latens och bandbredd. Trafik som går via en internetknutpunkt faktureras normalt inte till någon part, men så är fallet för trafik till en internetleverantör uppströms. Genom den direkta sammankopplingen, ofta lokaliserad till samma stad som de båda näten, tar man bort behovet för data att transporteras över långa avstånd för att komma från ett nät till ett annat, vilket minskar latensen.

Det bör noteras att definitionen av en IXP inte omfattar fysiska punkter där endast två fysiska nät kopplas samman med varandra (dvs. nätleverantörer som Base och Proximus). När medlemsstaterna införlivar direktivet måste de därför skilja mellan operatörer som underlättar utbytet av aggregerad internettrafik mellan flera nätoperatörer och operatörer av ett enda nät som fysiskt kopplar samman sina nät baserat på ett sammankopplingsavtal. I det senare fallet omfattas nätleverantörerna inte av definitionen i artikel 4.13. Ett klargörande av detta finns i skäl 18, där det fastställs att en IXP inte tillhandahåller tillträde till nätverk och inte fungerar som transitleverantör eller transitförmedlare. Den sista kategorin leverantörer är företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som omfattas av säkerhets- och anmälningskraven enligt artiklarna 13a och 13b i direktiv 2002/21/EG och som därför inte omfattas av direktivet[26].

2) Domännamnssystem (DNS).

Begreppet domännamnssystem definieras i artikel 4.14 som *”ett hierarkiskt, distribuerat namngivningssystem i ett nätverk som hanterar domännamnsförfrågningar”*. Mer exakt kan ett domännamnssystem beskrivas som ett hierarkiskt, distribuerat namngivningssystem för

[25] Se avsnitt 4.1.6 för mer detaljer om identifieringsförfarandet.
[26] Se avsnitt 5.2 för mer detaljer om förhållandet mellan it-säkerhetsdirektivet och direktiv 2002/21/EG.

datorer, tjänster eller varje annan resurs som ansluts till internet och som möjliggör kodning av domännamn till IP-adresser (internetprotokoll). Systemets viktigaste funktion är att översätta de tilldelade domännamnen till IP-adresser. För detta syfte driver ett domännamnssystem en databas och använder namnservrar och resolver för att möjliggöra denna typ av ”översättning” av domännamn till operativa IP-adresser. Även om kodningen av domännamn inte är domännamnssystemets enda uppgift är det en huvuduppgift för systemet. Den rättsliga definitionen i artikel 4.14 fokuserar på systemets huvuduppgift från användarens perspektiv utan att gå in på mer tekniska detaljer, som t.ex. driften av domännamn, namnserver, resolver etc. Slutligen klargör artikel 4.15 vem som ska anses som leverantör av DNS-tjänster.

3) Registerenhet för toppdomäner(TLD-registerenhet).

Registerenhet för toppdomäner definieras i artikel 4.16 som en enhet som administrerar och förvaltar registreringen av internetdomännamn under en specifik toppdomän. Denna administration och förvaltning av domännamn innefattar kodning av TLD-namn till IP-adresser.

Iana (*Internet Assigned Numbers Authority*) ansvarar för den globala samordningen av DNS-rot, IP-adressering och andra IP-resurser. Iana ansvarar framför allt för tilldelningen av generiska toppdomäner (*gTLD*) som t.ex. ”.com” och nationella toppdomäner (*ccTLD*) som t.ex. ”.be” till leverantörer (registerenheter) och underhållet av deras tekniska och administrativa uppgifter. Iana upprätthåller ett globalt register över tilldelade toppdomännamn och har en roll när det gäller spridningen av denna lista till internetanvändare i hela världen liksom när det gäller införandet av nya toppdomäner.

En viktig uppgift för registerenheterna är att tilldela de s.k. registranterna domännam på andra nivån inom deras respektive toppdomän. Dessa registranter kan också på egen hand fördela domännamn på tredje nivån om de så vill. De nationella toppdomänerna utses för att representera ett land eller ett territorium baserat på standarden ISO 3166-1. De ”generiska” toppdomänerna representerar normalt sett inte ett geografiskt område eller ett land.

Det bör noteras att driften av registerenheten för toppdomäner kan innefatta tillhandahållande av domännamnssystem. I enlighet med Ianas bestämmelser om delegering ska den utsedda enhet som hanterar de nationella toppdomänernas behov bl.a. utöva tillsyn över domännamnen och driva det berörda landets domännamnssystem[27]. Sådana omständigheter måste beaktas av medlemsstaterna i samband med deras process för att identifiera leverantörer av samhällsviktiga tjänster enligt artikel 5.2.

4.1.2 Identifiering av leverantörer av samhällsviktiga tjänster

I enlighet med kraven i artikel 5 i direktivet ska varje medlemsstat genomföra ett identifieringsförfarande med avseende på alla enheter av de typer som finns förtecknade i bilaga II vilka har laglig etablering på medlemsstatens territorium. Till följd av denna

[27] Informationen finns på: https://www.icann.org/resources/pages/delegation-2012-02-25-en.

bedömning ska alla enheter som uppfyller kriterierna i artikel 5.2 identifieras som leverantörer av samhällsviktiga tjänster och omfattas av säkerhets- och rapporteringsskyldigheterna enligt artikel 14.

Senast den 9 november 2018 ska medlemsstaterna, för varje sektor och delsektor, identifiera leverantörer av samhällsviktiga tjänster. För att stödja medlemsstaterna i detta förfarande håller samarbetsgruppen för närvarande på att utarbeta en vägledning med relevant information om de nödvändiga stegen och bästa praxis när det gäller identifiering av leverantörer av samhällsviktiga tjänster.

I enlighet med artikel 24.2 ska samarbetsgruppen också diskutera förfarandet för, innehållet i och typen av nationella åtgärder som möjliggör identifiering av leverantörer av samhällsviktiga tjänster inom en särskild sektor. En medlemsstat får, fram till den 9 november 2018, ta upp sitt utkast till nationella åtgärder för att möjliggöra identifiering av leverantörer av samhällsviktiga tjänster till diskussion i samarbetsgruppen.

4.1.3 Inkluderande av ytterligare sektorer.

Med beaktande av kraven på minimiharmonisering enligt artikel 3 kan medlemsstaterna anta eller behålla lagstiftning som säkerställer en högre nivå av säkerhet för nät- och informationssystem. I detta hänseende är medlemsstaterna i allmänhet fria att utvidga säkerhets- och rapporteringsskyldigheterna enligt artikel 14 till att omfatta enheter som hör till andra sektorer och delsektorer än de som förtecknas i bilaga II till direktivet. Olika medlemsstater överväger eller har beslutat att även inkludera några av följande sektorer:

i) Offentliga förvaltningar

Offentliga förvaltningar kan erbjuda samhällsviktiga tjänster enligt direktivets bilaga II som uppfyller kraven i artikel 5.2. I sådana fall skulle offentliga förvaltningar som erbjuder sådana tjänster omfattas av de berörda säkerhetskraven och rapporteringsskyldigheterna. När offentliga förvaltningar erbjuder tjänster som inte faller under ovannämnda tillämpningsområde omfattas dessa däremot inte av de berörda skyldigheterna.

Offentliga förvaltningar är ansvariga för ett korrekt tillhandahållande av offentliga tjänster som tillhandahålls av statliga organ, regionala och lokala myndigheter, byråer och tillhörande företag. Dessa tjänster innefattar ofta skapande och hantering av personuppgifter och företagsuppgifter som rör privatpersoner och organisationer, vilka kan delas och göras tillgängliga för många olika offentliga organ. Generellt sett är det viktigt för samhället och ekonomin i stort att säkerhetsnivån är hög för de nät- och informationssystem som används av offentliga förvaltningar. Kommissionen anser därför att det skulle vara klokt av medlemsstaterna att överväga att låta offentlig förvaltning omfattas av tillämpningsområdet för den nationella lagstiftning som införlivar direktivet, utöver tillhandahållandet av samhällsviktiga tjänster enligt bilaga II och artikel 5.2.

ii) Postsekorn

Postsektorn omfattar tillhandahållande av posttjänster, som t.ex. insamling, sortering, transport och distribution av postförsändelser.

iii) Livsmedelssektorn

Livsmedelsektorn omfattar produktion av jordbruksprodukter och andra livsmedelsprodukter, och den kan omfatta sådana samhällsviktiga tjänster som tillhandahållande av livsmedelstrygghet och säkerställande av livsmedelskvalitet och livsmedelssäkerhet.

iv) Kemisk industri och kärnteknisk industri

Den kemiska industrin och den kärntekniska industrin omfattar i synnerhet lagring, produktion och bearbetning av kemiska och petrokemiska produkter eller kärnämne.

v) Miljösektorn

Miljöverksamhet omfattar tillhandahållande av sådana varor och tjänster som behövs för att skydda miljön och förvalta resurser. Därför syftar verksamheten till att förebygga, minska och undanröja förorening och bevara beståndet av tillgängliga naturresurser. Inom denna sektor kan samhällsviktiga tjänster vara övervakning och kontroll av förorening (dvs. av luft och vatten) och väderfenomen.

vi) Civilskydd

Civilskyddssektorns syfte är förebyggande av, förberedelser inför och insatser efter naturkatastrofer och katastrofer orsakade av människan. Exempel på tjänster som tillhandahålls i detta syfte kan vara aktivering av larmnummer och genomförande av åtgärder för att informera, begränsa verkningarna och vidta svarsåtgärder i samband med nödsituationer.

4.1.4 Behörighet.

Enligt artikel 5.1 ska varje medlemsstat identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium. Bestämmelsen specificerar inte typen av laglig etablering, men i skäl 21 förtydligas att det krävs att leverantören utför en faktisk och reell verksamhet med hjälp av en stabil struktur för att den ska anses vara etablerad i en medlemsstat och att den rättsliga formen för en sådan struktur inte bör vara den avgörande faktorn. Det innebär att en medlemsstat inte bara kan ha jurisdiktion över en leverantör av samhällsviktiga tjänster i de fall då leverantören har sitt huvudkontor på dess territorium, utan även i fall då leverantören har exempelvis en filial eller annan typ av laglig etablering.

Detta har till följd att flera medlemsstater samtidigt kan ha jurisdiktion över samma enhet.

4.1.5 Uppgifter som ska lämnas till kommissionen

För den översyn som kommissionen ska utföra i enlighet med artikel 23.1 i direktivet ska medlemsstaterna senast den 9 november 2018 och därefter vartannat år lämna följande uppgifter till kommissionen:

- Nationella åtgärder som gör det möjligt att identifiera leverantörer av samhällsviktiga tjänster.
- Förteckningen över samhällsviktiga tjänster.
- Antalet identifierade leverantörer av samhällsviktiga tjänster inom varje sektor som avses i bilaga II och dessa leverantörers betydelse för sektorn.

- I förekommande fall, trösklar som används för att fastställa försörjningsnivån med avseende på antalet användare som är beroende av tjänsten i enlighet med artikel 6.1 a och enhetens betydelse i enlighet med artikel 6.1 f.

Den översyn enligt artikel 23.1 som föregår den övergripande översynen av direktivet visar den betydelse som medlagstiftarna fäster vid ett korrekt införlivande av direktivet när det gäller identifiering av leverantörer av samhällsviktiga tjänster, för att undvika marknadsfragmentering.

För att genomföra detta förfarande på bästa möjliga sätt uppmanar kommissionen medlemsstaterna att diskutera frågan och utbyta relevanta erfarenheter i samarbetsgruppen. Kommissionen uppmanar också medlemsstaterna att meddela kommissionen – om nödvändigt på konfidentiell grund – sina förteckningar över identifierade leverantörer av samhällsviktiga tjänster (som slutligen valts ut) utöver alla uppgifter som medlemsstaterna enligt direktivet ska lämna till kommissionen. Tillgång till dessa förteckningar kan underlätta och förbättra kvaliteten på kommissionens bedömning av identifieringsförfarandets enhetlighet och möjliggöra jämförelser av medlemsstaternas olika tillvägagångssätt, vilket gör det möjligt att bättre uppnå direktivets mål.

4.1.6 Hur ska identifieringsprocessen genomföras?

Figur 4 visar att det finns sex nyckelfrågor som en nationell myndighet bör granska i samband med identifieringsprocessen för de enskilda enheterna. I följande stycke motsvarar varje fråga ett steg som ska tas i enlighet med artikel 5 jämförd med artikel 6, och även med beaktande av tillämpligheten av artikel 1.7.

Steg 1 – **Tillhör enheten en sektor/delsektor och motsvarar den en typ som förtecknas i bilaga II till direktivet?**

En nationell myndighet bör bedöma om en enhet som är etablerad på dess territorium tillhör de sektorer och delsektorer som förtecknas i bilaga II till direktivet. Bilaga II omfattar olika ekonomiska sektorer som anses viktiga för att säkerställa den inre marknadens funktion. Bilaga II avser i synnerhet följande sektorer och delsektorer:

- Energi: el, olja och gas.
- Transport: luftfart, järnväg, vattentransporter och vägtransporter.
- Bankverksamhet: kreditinstitut.
- Finansmarknadsinfrastruktur: handelsplatser, centrala motparter.
- Hälso- och sjukvård: hälso- och sjukvårdsleverantörer (inklusive sjukhus och privata kliniker).
- Vatten: leverans och distribution av dricksvatten.
- Digital infrastruktur: internetknutpunkter, leverantörer av domännamnssystem, registerenheter för toppdomäner[28].

[28]Dessa enheter förklaras närmare i avsnitt 4.1.1.

Steg 2 – **Ska *lex specialis* tillämpas?**

I nästa steg måste den nationella myndigheten fastställa om bestämmelsen om *lex specialis* enligt artikel 1.7 ska tillämpas. Där fastställs att om det finns en sektorsspecifik unionsrättsakt som föreskriver säkerhets- och/eller rapporteringskrav för leverantörer av digitala tjänster eller leverantörer av samhällsviktiga tjänster ska den sektorsspecifika unionsrättsakten tillämpas om dess verkan minst motsvarar verkan av skyldigheterna enligt direktivet. I skäl 9 klargörs också att om kraven i artikel 1.7 uppfylls bör medlemsstaterna tillämpa bestämmelserna i den sektorsspecifika unionsrättsakten, inklusive sådana som rör jurisdiktion. Det innebär samtidigt att de berörda bestämmelserna i direktivet inte tillämpas. I sådana fall bör den behöriga myndigheten inte fortsätta identifieringsförfarandet enligt artikel 5.2[29].

Steg 3 – **Tillhandahåller leverantören en samhällsviktig tjänst i direktivets mening?**

Enligt artikel 5.2 ska en enhet som omfattas av identifieringskravet tillhandahålla en tjänst som är viktig för att upprätthålla kritisk samhällelig och/eller ekonomisk verksamhet. När medlemsstaten gör denna bedömning bör den ta hänsyn till att samma enhet kan tillhandahålla både samhällsviktiga tjänster och tjänster som inte är samhällsviktiga. Det betyder att direktivets säkerhets- och rapporteringskrav endast bör tillämpas på en viss leverantör i den utsträckning som leverantören tillhandahåller samhällsviktiga tjänster.

Enligt artikel 5.3 ska varje medlemsstat upprätta en förteckning över alla samhällsviktiga tjänster som tillhandahålls av leverantörer av samhällsviktiga tjänster på dess territorium. Denna förteckning måste lämnas till kommissionen senast senast den 9 november 2018 och därefter vartannat år[30].

Steg 4 – **Är tjänsten beroende av ett nät- och informationssystem?**

Det bör också fastställas om tjänsten uppfyller det andra kriteriet i artikel 5.2 b och i synnerhet om tillhandahållandet av den samhällsviktiga tjänsten är beroende av nät- och informationssystem enligt definitionen i artikel 4.1.

Steg 5 – **Skulle en säkerhetsincident medföra en betydande störning?**

Enligt artikel 5.2 c ska den nationella myndigheten bedöma om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. I artikel 6.1 anges därför ett antal sektorsöverskridande faktorer som måste beaktas i bedömningen. I artikel 6.2 fastställs också att medlemsstaterna i lämpliga fall även bör beakta sektorsspecifika faktorer i samband med bedömningen.

Följande **sektorsöverskridande faktorer** anges i artikel 6.1:

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

[29] Närmare uppgifter om tillämpningen av *lex specialis* finns i avsnitt 5.1.
[30] Se artikel 5.7 b.

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

När det gäller de **sektorspecifika faktorerna** innehåller skäl 28 några exempel (se tabell 4) som kan ge de nationella myndigheterna vägledning.

Tabell 4: Exempel på sektorsspecifika faktorer att beakta när det fastställs om en incident medför betydande störning.

Sektor	Exempel på sektorsspecifika faktorer
Energileverantörer	Producerad volym eller andel av den energi som produceras nationellt
Oljeleverantörer	Volym olja som tillhandahålls per dag
Luftfart (inklusive flygplatser och lufttrafikföretag) **Järnvägstransport** **Hamnar**	Andel av den nationella trafikvolymen Antal passagerare eller fraktrörelser per år
Bank- eller finansmarknadsinfrastruktur	Systemvikt baserat på totala tillgångar Förhållandet mellan totala tillgångar och BNP
Hälso- och sjukvårdssektor	Antal patienter som vårdas av leverantören per år
Produktion, bearbetning och leverans av vatten	Volym, antal, och typ av användare som betjänas (t.ex. sjukhus, offentliga sektorn och privatpersoner) Förekomst av alternativa vattenkällor som omfattar samma geografiska område

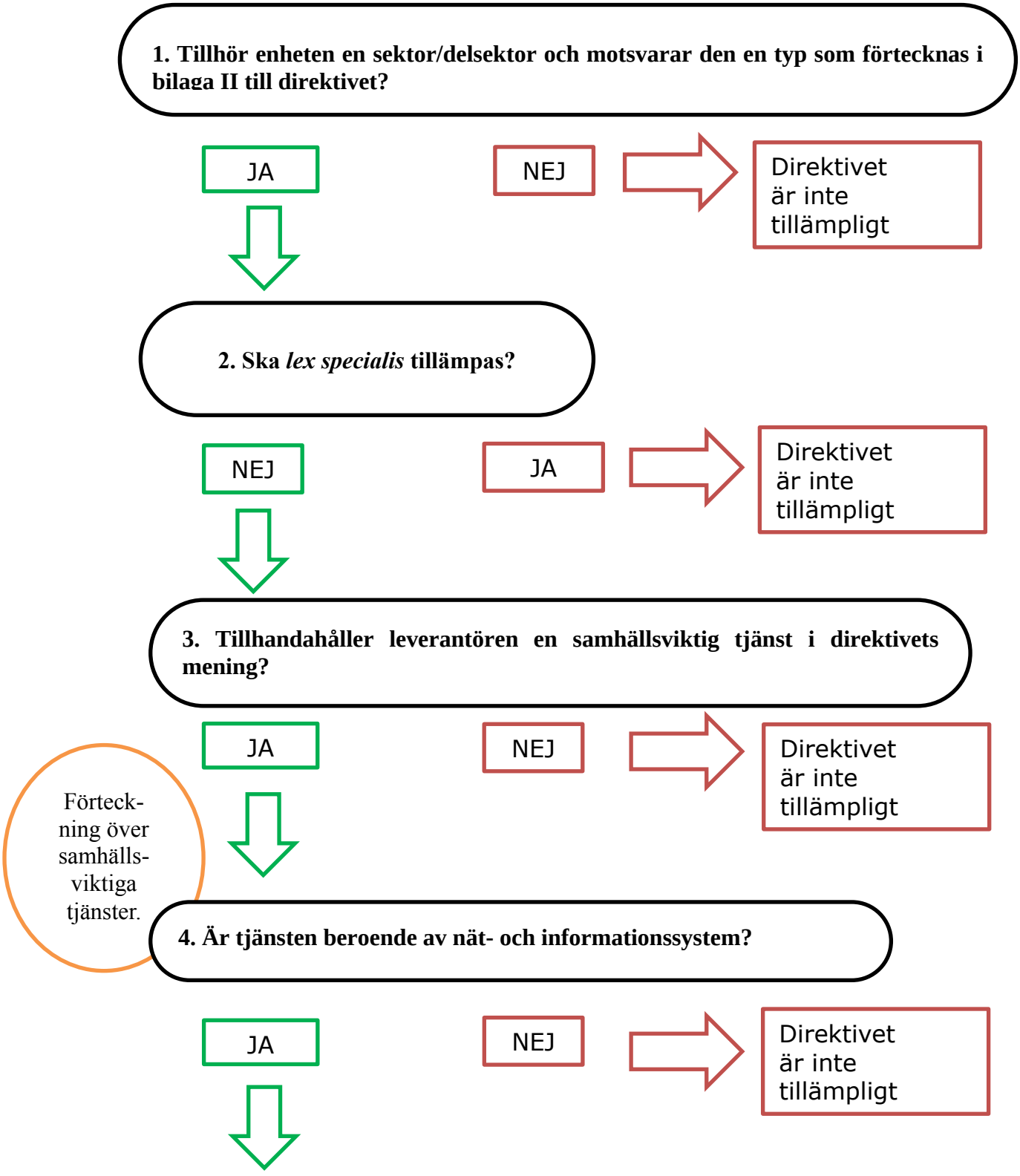
När medlemsstaterna gör sin bedömning enligt artikel 5.2 bör de inte lägga till några kriterier utöver de som förtecknas i bestämmelsen, eftersom det kan begränsa antalet identifierade leverantörer av samhällsviktiga tjänster och undergräva minimiharmoniseringen avseende leverantörer av samhällsviktiga tjänster enligt artikel 3 i direktivet.

Steg 6 – **Tillhandahåller den berörda leverantören samhällsviktiga tjänster i andra medlemsstater?**

Steg 6 avser fall då en leverantör tillhandahåller samhällsviktiga tjänster i två eller fler medlemsstater. Innan identifieringsförfarandet slutförs föreskrivs i artikel 5.4 att den berörda medlemsstaten ska genomföra ett samrådsförfarande[31].

[31] Närmare uppgifter om samrådsförfarandet finns i avsnitt 4.1.7.

Figur 4: Identifieringsförfarandet i sex steg.



5. Skulle en säkerhetsincident medföra en betydande störning?

Sektorsöverskridande faktorer (artikel 6.1)

- **Antal användare** som är beroende av tjänsten
- Andra samhällsviktiga tjänsters **beroende** av tjänsten
- Incidenternas möjliga inverkan på **ekonomisk verksamhet och samhällsverksamhet** eller **allmän säkerhet**
- **Geografiskt område** som kan påverkas
- Enhetens betydelse för upprätthållandet av en tillräcklig **tjänstenivå**

Sektorsspecifika faktorer (exempel som nämns i skäl 28)

- **Energi**: Producerad volym eller andel av den energi som produceras nationellt
- **Transport**: Andel av den nationella trafikvolymen & antal transporter per år
- **Hälso- och sjukvård**: Antal patienter som vårdas av leverantören per år

JA

NEJ → Direktivet är inte tillämpligt

6. Tillhandahåller den berörda leverantören samhällsviktiga tjänster i andra medlemsstater?

JA

NEJ → Direktivet är inte tillämpligt

Obligatoriskt samråd med berörd(a) medlemsstat(er)

Antagande av nationella åtgärder (dvs. förteckning över leverantörer av samhällsviktiga tjänster, politiska och rättsliga åtgärder).

4.1.7 Gränsöverskridande samrådsförfarande

I de fall då en leverantör tillhandahåller samhällsviktiga tjänster i två eller fler medlemsstater föreskriver artikel 5.4 att dessa medlemsstater ska samråda med varandra innan identifieringsförfarandet slutförs. Samrådets syfte är att hjälpa medlemsstaterna att bedöma om leverantören i fråga är av kritisk betydelse när det gäller gränsöverskridande inverkan.

Det önskade utfallet av samrådet är att de nationella myndigheterna utbyter argument och synpunkter och i idealfallet kommer fram till samma resultat när det gäller identifieringen av den berörda leverantören. Direktivet utesluter dock inte att medlemsstaterna kommer fram till olika slutsatser när det ska fastställas om en viss enhet ska identifieras som en leverantör av samhällsviktiga tjänster. I skäl 24 nämns att medlemsstaterna kan begära bistånd från samarbetsgruppen i sådana fall.

Kommissionen anser att medlemsstaterna bör sträva efter att uppnå samförstånd om dessa frågor för att undvika situationer där samma företag har olika rättslig status i olika medlemsstater. Skilda bedömningar bör verkligen utgöra ett undantag, t.ex. när en enhet som identifieras som leverantör av samhällsviktiga tjänster i en medlemsstat har en marginell och obetydlig verksamhet i en annan.

4.2. Säkerhetskrav.

I enlighet med artikel 14.1 ska medlemsstaterna se till att leverantörer av samhällsviktiga tjänster, med beaktande av den senaste tekniska utvecklingen, vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nät- och informationssystem som de använder i sin verksamhet. I enlighet med artikel 14.2 ska lämpliga åtgärder förebygga och minimera verkningarna av incidenter.

Inom en särskild del av samarbetsgruppens verksamhet håller man för när varande på att utarbeta icke-bindande vägledning avseende säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster[32]. Det vägledande dokumentet ska vara färdigt sista kvartalet 2017. Kommissionen uppmuntrar medlemsstaterna att noga följa det vägledande dokument som utarbetas av samarbetsgruppen, så att de nationella bestämmelserna om säkerhetskrav ligger så nära varandra som möjligt. En harmonisering av sådana krav skulle avsevärt förenkla efterlevanden för sådana leverantörer av samhällsviktiga tjänster som tillhandahåller samhällsviktiga tjänster i mer än en medlemsstat och även avsevärt underlätta de nationella behöriga myndigheternas och CSIRT-enheternas tillsynsuppgifter.

4.3 Rapporteringskrav.

Enligt artikel 14.3 måste medlemsstaterna säkerställa att leverantörer av samhällsviktiga tjänster rapporterar ”*incidenter som har en betydande inverkan på kontinuiteten i de*

[32] I samband med utarbetandet av vägledningen har man tittat på förteckningar över internationella standarder, goda arbetsmetoder och metoder för riskbedömning/riskhantering för alla sektorer som omfattas av direktivet, och detta användes sedan som underlag för förslag till säkerhetsdomäner och säkerhetsåtgärder.

samhällsviktiga tjänster som de tillhandahåller". Följaktligen ska leverantörerna inte rapportera varje liten incident utan endast allvarliga incidenter som påverkar den samhällsviktiga tjänstens kontinuitet. I artikel 4.7 definieras en incident som "*en händelse med en faktisk negativ inverkan på säkerheten i nätverks- och informationssystem*". Begreppet *säkerhet i nät- och informationssystem* definieras vidare i artikel 4.2 som "*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."* Följaktligen kan varje händelse som har negativ inverkan inte bara på tillgängligheten utan även på riktigheten, integriteten eller konfidentialiteten hos data eller tillhörande tjänster potentiellt utlösa rapporteringsskyldigheten. Tjänsternas kontinuitet enligt artikel 14.3 kan undergrävas inte bara i de fall då den fysiska tillgängligheten berörs utan även av andra säkerhetsincidenter som påverkar tillhandahållandet av tjänsten[33].

Samarbetsgruppen håller också på att utarbeta en icke-bindande rapporteringsvägledning för omständigheter då leverantörer av samhällsviktiga tjänster är skyldiga att rapportera incidenter i enlighet med artikel 14.7 samt formatet och förfarandet för den nationella rapporteringen. Denna vägledning ska vara färdig sista kvartalet 2017.

Olika nationella rapporteringskrav kan leda till rättsosäkerhet, mer komplicerade och betungande förfaranden och betydande administrativa kostnader för leverantörer med gränsöverskridande verksamhet. Kommissionen välkomnar därför samarbetsgruppens arbete. Precis som när det gäller säkerhetskraven uppmuntrar kommissionen medlemsstaterna att noga följa det vägledande dokument som utarbetas av samarbetsgruppen, så att de nationella bestämmelserna om rapportering av incidenter ligger så nära varandra som möjligt.

4.4. Bilaga III i direktivet: Leverantörer av digitala tjänster.

Leverantörer av digitala tjänster är den andra kategori av enheter som omfattas av direktivet. Dessa enheter anses vara viktiga ekonomiska aktörer eftersom många företag använder dem för tillhandahållandet av sina egna tjänster, och störningar av den digitala tjänsten kan påverka viktig ekonomisk och samhällelig verksamhet.

4.4.1 Kategorier av leverantörer av digitala tjänster.

Artikel 4.5, där digital tjänst definieras, hänvisar till den rättsliga definitionen i artikel 1.1 b i direktiv (EU) 2015/1535 genom att begränsa tillämpningsområdet till de typer av tjänster som förtecknas i bilaga III. I artikel 1.1 b i direktiv (EU) 2015/1535 definieras dessa tjänster som "*tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare*", och i bilaga III till direktivet förtecknas tre specifika typer av tjänster: internetbaserad marknadsplats, internetbaserad sökmotor och molntjänster. Till skillnad från när det gäller leverantörer av samhällsviktiga tjänster kräver direktivet dock inte att medlemsstaterna ska identifiera leverantörer av digitala tjänster, vilka sedan skulle

[33] Samma sak gäller för leverantörer av digitala tjänster.

omfattas av de tillämpliga skyldigheterna. Därmed kommer de tillämpliga skyldigheterna i direktivet, nämligen säkerhets- och rapporteringskraven enligt artikel 16, att gälla för alla leverantörer av digitala tjänster som omfattas av direktivet.

Följande avsnitt innehåller ytterligare förklaringar avseende de tre typer av digitala tjänster som omfattas av direktivet.

1. Leverantör av internetbaserad marknadsplats

Internetbaserade marknadsplatser ger ett stort antal företag av många olika slag möjlighet att bedriva handel gentemot kunder och ingå förbindelser med andra företag. De ger företag den basinfrastruktur de behöver för att bedriva handel över gränser. De har i synnerhet en viktig roll i ekonomin genom att ge små och medelstora företag tillgång till EU:s bredare digitala inre marknad. Tillhandahållandet av fjärrbearbetningstjänster online som underlättar kundernas ekonomiska verksamhet, inbegripet behandling av transaktioner och aggregering av uppgifter om köpare, leverantörer och produkter, kan också ingå i verksamheten hos leverantörer av internetbaserade marknadsplatser, liksom underlättande av sökning efter lämpliga produkter, tillhandahållande av produkter, transaktionsexpertis och matchande av köpare och säljare.

Begreppet internetbaserad marknadsplats definieras i artikel 4.17 och förklaras närmare i skäl 15. Den beskrivs som en tjänst som gör det möjligt för konsumenter och näringsidkare att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare, och den är slutdestinationen för ingåendet av sådana avtal. Exempelvis kan en leverantör som *E-bay* anses som en internetbaserad marknadsplats, eftersom den utgörs av en plattform där andra kan inrätta butiker för att göra sina produkter och tjänster tillgängliga online för konsumenter eller företag. Appbutiker på nätet, som distribuerar tillämpningar och datorprogram, anses också falla under definitionen av interbaserad marknadsplats eftersom de gör det möjligt för apputvecklare att sälja eller distribuera sina tjänster till konsumenter eller andra företag. Mellanhänder för tredjeparters tjänster, som *Skyscanner* och prisjämförelsetjänster, som skickar användaren vidare till webbplatsen för den näringsidkare med vilken det faktiska avtalet om tjänsten eller produkten ingås, omfattas emellertid inte av definitionen i artikel 4.17.

2. Leverantörer av internetbaserade sökmotorer

Begreppet internetbaserad sökmotor definieras i artikel 4.18 och förklaras närmare i skäl 16. Det beskrivs som 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. Sökfunktioner som är begränsade till sökningar på en webbplats och prisjämförelsewebbplatser omfattas inte. En sökmotor som den som tillhandahålls av EUR LEX[34] kan t.ex. inte anses som en sökmotor i direktivets mening eftersom sökfunktionen är begränsad till den enskilda webbplatsens innehåll.

[34] Finns på: http://eur-lex.europa.eu/homepage.html.

3. Leverantörer av molntjänster

I artikel 4.19 definieras molntjänst som ”en digital tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser” och i skäl 17 förtydligas närmare begreppen dataresurser, skalbar och elastisk pool.

Molntjänster kan kortfattat beskrivas som en viss typ av datatjänst som använder delade resurser för att behandla data på begäran, där de gemensamma resurserna avser varje typ av hårdvaru- eller mjukvarukomponenter (dvs. nät, servrar eller annan infrastruktur, lagring, tillämpning och tjänst) som på begäran tillhandahålls åt användare för bearbetning av data. Begreppet delbar avser dataresurser där många användare utnyttjar samma fysiska infrastruktur för databehandling. Dataresursen kan definieras som delbar om den pool av resurser som används av leverantören när som helst kan utökas eller minskas beroende på användarens behov. Datacenter eller enskilda komponenter inom ett datacenter kan eventuellt läggas till eller tas bort om den totala mängden datakapacitet eller lagringskapacitet behöver uppdateras. Begreppet elastisk pool kan beskrivas som att man ändrar arbetsbelastningen genom att de tillgängliga resurserna automatiskt utökas eller minskas så att de vid varje tidpunkt ligger så nära den aktuella efterfrågan som möjligt[35].

Det finns i dagsläget tre typer av molntjänstmodeller som en leverantör kan tillhandahålla:

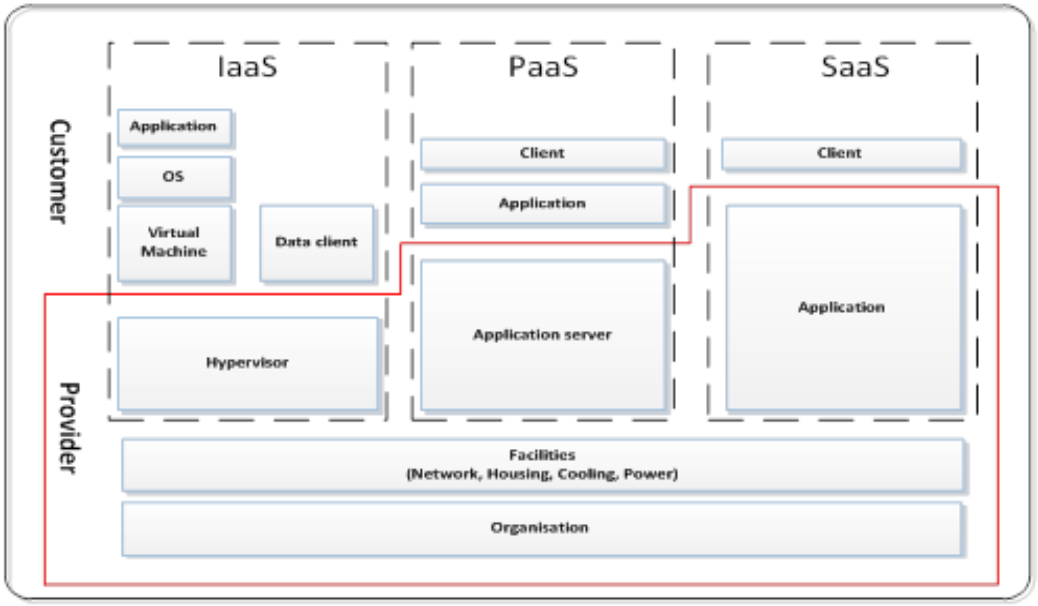
- Infrastruktur som en tjänst (*Infrastructure as a Service, IaaS*): En molntjänstkategori där den molnkapacitetstyp som tillhandahålls åt kunden är en infrastruktur. Tjänsten omfattar virtuellt tillhandahållande av dataresurser i form av hårdvara och nät- och lagringstjänster. Den används för servrar, lagring, nät och operativsystem. Den tillhandahåller företagsinfrastrukur där ett företag kan lagra sina data och driva de tillämpningar som behövs för den dagliga verksamheten.

- Plattform som en tjänst (*Platform as a Service, PaaS*): En molntjänstkategori där den molnkapacitetstyp som tillhandahålls åt kunden är en plattform. Den omfattar dataplattformar online som gör det möjligt för företag att använda befintliga tillämpningar eller att utveckla och testa nya sådana.

- Mjukvara som en tjänst (*Software as a service, SaaS*): En molntjänstkategori där den molnkapacitetstyp som tillhandahålls åt kunden är en tillämpning eller mjukvara som används via internet. Den här typen av molntjänst gör att användaren inte behöver köpa, installera och hantera mjukvara och har fördelen att mjukvaran blir tillgänglig för alla som har en internetuppkoppling.

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, *Elasticity in Cloud Computing: What It Is, and What It Is Not*, finns på: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Se även s. 2–5 i COM(2012) 529.

Figur 5: Tjänstemodeller och resurser i molnbaserade datortjänster



Övergripande riktlinjer om särskilda molnrelaterade frågor[36] och ett vägledande dokument med grundläggande information om molnbaserade datortjänster[37] har tillhandahållits av Enisa.

4.4.2 Säkerhetskrav

Enligt artikel 16.1 ska medlemsstaterna säkerställa att leverantörer av digitala tjänster vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som företag använder när de tillhandahåller sina tjänster. Dessa säkerhetsåtgärder bör ta hänsyn till den senaste tekniska utvecklingen och följande fem faktorer: i) Säkerheten i system och anläggningar. ii) Incidenthantering. iii) Hantering av driftskontinuitet. iv) Övervakning, revision och testning. v) Efterlevnad av internationella standarder.

För detta ändamål har kommissionen enligt artikel 16.8 befogenhet att anta genomförandeakter för att ytterligare specificera dessa element och säkerställa en hög grad av harmonisering för de berörda tjänsteleverantörerna. Genomförandeakten förväntas bli antagen av kommissionen under hösten 2017. Dessutom ska medlemsstaterna se till att leverantörer av digitala tjänster vidtar nödvändiga åtgärder för att förebygga och minimera verkningarna av incidenter i syfte att säkerställa kontinuiteten i dessa tjänster.

4.4.3 Rapporteringskrav

Leverantörer av digitala tjänster bör vara skyldiga att rapportera allvarliga incidenter till behöriga myndigheter eller till CSIRT-enheterna. I enlighet med artikel 16.3 i it-säkerhetsdirektivet utlöses denna rapporteringskyldighet i sådana fall där säkerhetsincidenten

[36] Available at: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Cloud Security Guide for SMEs* (2015). Available at: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

i fråga har en avsevärd inverkan på tillhandahållandet av tjänsten. För att fastställa graden av inverkan anges i artikel 16.4 fem faktorer som ska beaktas av leverantörer av digitala tjänster. Kommissionen har enligt artikel 16.8 befogenhet att anta genomförandeakter för att ytterligare specificera dessa faktorer. Den ytterligare specificeringen av dessa faktorer kommer att ingå i den genomförandeakt som specificerar de säkerhetsaspekter som avses i punkt 4.4.2 och som kommissionen planerar att anta under hösten.

4.4.4 Riskbaserad regleringsstrategi.

I artikel 17 anges att leverantörer av digitala tjänster är underkastade tillsynsåtgärder i efterhand från de nationella behöriga myndigheternas sida. Medlemsstaterna måste se till att de behöriga myndigheterna vidtar åtgärder när de har mottagit bevis på att en leverantör av digitala tjänster inte uppfyller kraven i artikel 16 i direktivet.

Enligt artikel 16.8 och 16.9 har kommissionen befogenhet att anta genomförandeakter med avseende på rapporterings- och säkerhetskrav som ökar graden av harmonisering för leverantörer av digitala tjänster. Enligt artikel 16.10 får medlemsstaterna inte införa några ytterligare säkerhets- eller rapporteringskrav för leverantörer av digitala tjänster än de som föreskrivs i direktivet, utom i fall där sådana åtgärder är nödvändiga för att de ska kunna skydda sina väsentliga statliga funktioner, särskilt för att skydda den nationella säkerheten och för att möjliggöra utredning, upptäckt och lagföring av brott.

Slutligen, och med hänsyn till den gränsöverskridande karaktären hos leverantörer av digitala tjänster, följer direktivet inte modellen med flera parallella jurisdiktioner, utan en strategi som grundar sig på kriteriet om företagets huvudsakliga verksamhetsställe inom EU[38]. Denna strategi möjliggör en enda uppsättning regler som ska gälla för leverantörer av digitala tjänster, med en behörig myndighet med ansvar för tillsyn. Detta är särskilt viktigt eftersom många leverantörer av digitala tjänster erbjuder sina tjänster i många medlemsstater samtidigt. Tillämpningen av denna strategi minimerar den administrativa bördan på leverantörerna och säkerställer en väl fungerande digital inre marknad.

4.4.5 Behörighet.

Som förklaras ovan följer det av artikel 18.1 i it-säkerhetsdirektivet att det är den medlemsstat där leverantören har sitt huvudsakliga etableringsställe som har jurisdiktion med avseende på företaget. I sådana fall då en specifik leverantör erbjuder tjänster i EU utan att vara etablerad på EU:s territorium, är denna leverantör enligt artikel 18.2 skyldig att utse en företrädare i unionen. I sådana fall är det den medlemsstat där företrädaren är etablerad som har jurisdiktion med avseende på företaget. I fall där en leverantör tillhandahåller tjänster i en medlemsstat, men inte har utsett någon företrädare i EU, kan medlemsstaten i fråga i princip vidta åtgärder mot leverantören eftersom denne underlåter att fullgöra sina skyldigheter enligt direktivet.

[38] Se särskilt artikel 17 i direktivet.

4.4.6 Undantag från säkerhets- och rapporteringskraven för mindre leverantörer av digitala tjänster.

Enligt artikel 16.11 ska leverantörer av digitala tjänster som är mikroföretag eller små företag enligt definitionen i kommissionens rekommendation 2003/361/EG39 undantas från tillämpningen av bestämmelserna om säkerhetskrav och rapportering i artikel 16. Det innebär att företag som sysselsätter färre än 50 personer och har en årsomsättning och/eller en årlig balansomslutning på högst 10 miljoner euro inte omfattas av dessa krav. Vid fastställandet av storleken på företaget är det inte relevant om det berörda företaget endast tillhandahåller digitala tjänster i den mening som avses i it-säkerhetsdirektivet eller om det även erbjuder andra tjänster.

5. Förhållandet mellan it-säkerhetsdirektivet och annan lagstiftning.

Detta avsnitt fokuserar på *lex specialis*-bestämmelserna i it-säkerhetsdirektivets artikel 1.7, och beskriver de tre exempel på *lex specialis* som kommissionen hittills har bedömt samt förtydligar de säkerhets- och rapporteringskrav som tillämpas på leverantörer av telekommunikation och betrodda tjänster.

5.1 It-säkerhetsdirektivet, artikel 1.7: *Lex specialis*-bestämmelsen.

I enlighet med artikel 1.7 i it-säkerhetsdirektivet är bestämmelserna om säkerhets- och/eller rapporteringskrav för leverantörer av digitala tjänster eller leverantörer av samhällsviktiga tjänster enligt direktivet inte tillämpliga om en sektorsspecifik EU-lagstiftning föreskriver säkerhets- och/eller rapporteringskrav som minst motsvarar verkan av motsvarande skyldigheter i direktivet. Medlemsstaterna behöver beakta artikel 1.7 vid införlivandet av direktivet överlag och informera kommissionen om tillämpningen av *lex specialis*-bestämmelser.

Metod.

Vid bedömningen av huruvida en sektorsspecifik EU-lagstiftning överensstämmer med de relevanta bestämmelserna i direktivet bör särskild vikt läggas vid frågan om huruvida bestämmelserna om säkerhetsrelaterade skyldigheter i den sektorsspecifika lagstiftningen inbegriper åtgärder som garanterar säkerheten i nät- och informationssystem i enlighet med artikel 4.2 i direktivet.

När det gäller rapporteringsplikten föreskrivs i artiklarna 14.3 och 16.3 i direktivet att leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster utan onödigt dröjsmål ska rapportera alla incidenter som har en betydande/avsevärd inverkan på tillhandahållandet av tjänsten i fråga till den behöriga myndigheten eller till CSIRT-enheten. Här är det särskilt viktigt att uppmärksamma leverantörens skyldighet att i rapporten ta med information som gör det möjligt för den behöriga myndigheten eller CSIRT-enheten att fastställa eventuella gränsöverskridande konsekvenser av en säkerhetsincident.

[39] EUT L 24, 20.5.2003, s. 36.

För närvarande finns det ingen sektorspecifik lagstiftning för leverantörer av digitala tjänster med säkerhets- och rapporteringskrav som är jämförbara med dem som fastställs i artikel 16 i it-säkerhetsdirektivet och som kan beaktas vid tillämpningen av artikel 1.7 i direktivet[40].

När det gäller leverantörer av samhällsviktiga tjänster omfattas för närvarande den finansiella sektorn och särskilt sektorerna banktjänster och finansmarknadsinfrastruktur (jfr punkt 3 och 4 i bilaga II) av säkerhets- och/eller rapporteringskrav på grundval av sektorsspecifik EU-lagstiftning. Detta beror på att frågan om säkerhet och sundhet i it- och nät- och informationssystem som används av finansinstitut är en väsentlig del av de krav med avseende på operativa risker som ställs på finansinstitut med stöd av EU-lagstiftning.

Exempel.

i) Betaltjänstdirektivet 2.

Beträffande banksektorn, och särskilt vad gäller tillhandahållande av betaltjänster som tillhandahålls av kreditinstitut enligt definitionen i artikel 4.1 i förordning (EU) nr 575/2013, innehåller det så kallade betaltjänstdirektivet 2[41] säkerhets- och rapporteringskrav (jfr artiklarna 95 och 96 i det direktivet).

I artikel 95.1 föreskrivs närmare bestämt att betaltjänstleverantörer ska anta lämpliga begränsningsåtgärder och kontrollmekanismer för att hantera operativa risker och säkerhetsrisker med anknytning till de betaltjänster som de tillhandahåller. Dessa åtgärder bör inbegripa fastställande och upprätthållande av effektiva incidenthanteringsförfaranden, däribland förfaranden för upptäckt och klassificering av allvarliga operativa incidenter och säkerhetsincidenter. I skäl 95 och 96 i betaltjänstdirektivet 2 klargörs ytterligare vilket slags säkerhetsåtgärder det rör sig om. Av dessa bestämmelser framgår tydligt att de föreskrivna åtgärderna syftar till att hantera säkerhetsrisker med anknytning till de nät- och informationssystem som används vid tillhandahållandet av betaltjänster. Dessa säkerhetskrav kan därför anses minst motsvara verkan av motsvarande bestämmelse i artikel 14.1 och 14.2 i it-säkerhetsdirektivet.

Vad gäller anmälningsskyldigheten fastställs i artikel 96.1 i betalningstjänstdirektivet 2 en skyldighet för betaltjänstleverantörer att utan onödigt dröjsmål underrätta den behöriga myndigheten om allvarliga säkerhetsincidenter. På ett sätt som kan jämföras med artikel 14.5 i it-säkerhetsdirektivet åläggs den behöriga myndigheten genom artikel 96.2 i betalningstjänstdirektivet 2 att informera de behöriga myndigheterna i andra medlemsstater, om incidenten är av relevant för dem. Denna skyldighet innebär samtidigt att rapporteringen av säkerhetsincidenter måste omfatta information som gör det möjligt för myndigheterna att bedöma de gränsöverskridande verkningarna av en incident. Genom artikel 96.3 a i

[40] Detta påverkar inte sådan anmälan av en personuppgiftsincident till tillsynsmyndigheten som omfattas av artikel 33 i den allmänna dataskyddsförordningen.
[41] Direktiv (EU) 2015/2366, EUT L 337, 23.12.2015, s. 35.

betalningstjänstdirektivet 2 bemyndigas EBA att, i samarbete med ECB, utarbeta riktlinjer om underrättelsens exakta innehåll och format.

Följaktligen kan det konstateras att enligt artikel 1.7 i it-säkerhetsdirektivet bör både säkerhetskraven och rapporteringskraven som föreskrivs i artikel 95 respektive artikel 96 i betalningstjänstdirektivet 2 tillämpas i stället för motsvarande bestämmelser i artikel 14 i it-säkerhetsdirektivet när det handlar om betalningstjänster som tillhandahålls av kreditinstitut.

ii) Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister.

När det gäller finansmarknadens infrastruktur innehåller förordning (EU) nr 648/2012, jämförd med kommissionens delegerade förordning (EU) nr 153/2013, bestämmelser om säkerhetskrav för centrala motparter. Dessa bestämmelser kan betraktas som *lex specialis.* Rättsakterna innehåller särskilt bestämmelser om tekniska och organisatoriska åtgärder med anknytning till säkerheten i nätverks- och informationssystem. Dessa bestämmelser är till och med mer detaljerade än kraven i artikel 14.1 och 14.2 i it-säkerhetsdirektivet och kan därför anses överensstämma med artikel 1.7 i det direktivet när det gäller säkerhetskraven.

I artikel 26.1 i förordning (EU) nr 648/2012 anges att enheten ska ha ”*stabila styrformer, som omfattar en tydlig organisationsstruktur med en väldefinierad, transparent och konsekvent ansvarsfördelning, effektiva metoder för att identifiera, hantera, övervaka och rapportera de risker som denna motpart är eller kan bli utsatt för samt ha tillfredsställande rutiner för intern kontroll, däribland sunda förfaranden för administration och redovisning*.” Artikel 26.3 föreskriver att organisationsstrukturen måste säkerställa väl fungerande tjänster och verksamhet genom användning av lämpliga och proportionella system, resurser och förfaranden.

I artikel 26.6 klargörs att en central motpart ska ha ”*tillräckliga IT-system som kan hantera dess tjänsters och verksamhets komplexitet, mångfald och inriktning, så att den tryggar hög säkerhetsstandard och att dess uppgifter är säkra och konfidentiella*”. Dessutom föreskrivs i artikel 34.1 att en central motpart ska etablera, genomföra och upprätthålla lämpliga riktlinjer för kontinuerlig verksamhet och en lämplig katastrofplan som säkerställer ett snabbt återupptagande av verksamheten.

Dessa skyldigheter specificeras närmare i kommissionens delegerade förordning (EU) nr 153/2013 av den 19 december 2012 om komplettering av Europaparlamentets och rådets förordning (EU) nr 648/2012 med avseende på tekniska tillsynsstandarder för krav på centrala motparter[42]. Genom artikel 4 i denna förordning åläggs centrala motparter en skyldighet att utarbeta lämpliga riskhanteringsverktyg som gör det möjligt att hantera och rapportera alla relevanta risker och som närmare anger vilka typer av åtgärder (t.ex. användning av stabila informations- och riskkontrollsystem, tillgång till resurser, sakkunskap och all nödvändig information för riskhanteringsfunktionen, tillgång till adekvata interna kontrollmekanismer såsom goda administrativa rutiner och redovisningsrutiner som hjälper den centrala

[42] EUT L 52, 23.2.2013, s. 41.

motpartens styrelse att kontrollera och bedöma om dess riktlinjer, förfaranden och system för riskhantering är tillräckliga och effektiva).

Artikel 9 tar dessutom uttryckligen upp frågan om säkerhet i it-system och föreskriver konkreta tekniska och organisatoriska åtgärder av betydelse för upprätthållandet av ett stabilt system för informationssäkerhet som på lämpligt sätt hanterar it-säkerhetsrisken. Sådana åtgärder bör omfatta mekanismer och förfaranden för att trygga tillgången till tjänster och skydda uppgifternas autenticitet, integritet och konfidentialitet.

(iii) 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[43].

När det gäller handelsplatser uppställs i artikel 48.1 i direktiv 2014/65/EU kravet att operatörerna ska kunna säkerställa kontinuitet i sin verksamhet även vid eventuella driftsavbrott i sina handelssystem. Denna allmänna skyldighet har nyligen preciserats och kompletterats genom kommissionens delegerade förordning (EU) 2017/584[44] av den 14 juli 2016 om komplettering av Europaparlamentets och rådets direktiv 2014/65/EU avseende tekniska tillsynsstandarder som specificerar organisatoriska krav för handelsplatser[45]. I artikel 23.1 i denna förordning anges att handelsplatser ska ha inrättat förfaranden och arrangemang för fysisk och elektronisk säkerhet för att skydda sina system från missbruk eller obehörig tillgång och för att säkerställa skydd av uppgifter. Dessa åtgärder bör göra det möjligt att förebygga eller minimera risken för angrepp mot informationssystem.

I artikel 23.2 föreskrivs vidare att de åtgärder och arrangemang som operatörerna vidtar bör göra det möjligt att snabbt identifiera och hantera risker med avseende på obehörigt tillträde, systemstörningar som allvarligt hindrar eller avbryter driften av ett informationssystem och störningar som äventyrar uppgifternas tillgänglighet, integritet eller autenticitet. I artikel 15 i förordningen föreskrivs vidare att handelsplatser ska ha inrättat effektiva arrangemang för driftskontinuitet för att säkerställa tillräcklig stabilitet i systemet och hantera störande incidenter. Dessa åtgärder bör göra det möjligt för operatören att återuppta handeln inom eller nära två timmar efter incidenten och samtidigt se till att volymen förlorade uppgifter ligger nära noll.

Artikel 16 anger vidare att identifierade åtgärder för att möta och hantera incidenter som orsakar störningar bör ingå i handelsplatsernas kontinuitetsplan och tar upp vissa element som operatören behöver ta hänsyn till när kontinuitetsplanen antas (t.ex. inrätta en särskild grupp för säkerhetspersonal, utföra och regelbundet se över en konsekvensbedömning som identifierar risker).

Sett till innehållet i dessa säkerhetsåtgärder tycks de vara avsedda att hantera risker med anknytning till tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos

[43] EUT L 173, 12.6.2014, s. 349.
[44] EUT L 87, 31.3.2017, s. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

uppgifter eller levererade tjänster, och följaktligen kan man sluta sig till att ovannämnda sektorsspecifika EU-lagstiftning uppställer säkerhetskrav som till sin verkan åtminstone motsvarar kraven i artikel 14.1 och 14.2 it-säkerhetsdirektivet.

5.2 It-säkerhetsdirektivet, artikel 1.3: Leverantörer av telekommunikation och betrodda tjänster.

Enligt artikel 1.3 är de säkerhets- och rapporteringskrav som föreskrivs i direktivet inte tillämpliga på leverantörer som omfattas av kraven i artikel 13a och 13b i direktiv 2002/21/EG. Artikel 13a och 13b i direktiv 2002/21/EG tillämpas på företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster. När det gäller tillhandahållande av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster måste företaget således uppfylla säkerhets- och anmälningskraven i direktiv 2002/21/EG.

Om samma företag emellertid tillhandahåller även andra tjänster, såsom digitala tjänster (t.ex. datormoln eller marknadsplatser online) som förtecknas i bilaga III till it-säkerhetsdirektivet, eller tjänster av typen DNS-tjänster eller internetknutpunkter (IXP) enligt punkt 7 i bilaga II till it-säkerhetsdirektivet, kommer företaget att omfattas av it-säkerhetsdirektivets säkerhets- och anmälningskrav när det gäller tillhandahållandet av dessa särskilda tjänster. Det bör noteras att i och med att leverantörerna av sådana tjänster som anges i punkt 7 i bilaga II tillhör kategorin leverantörer av samhällsviktiga tjänster, är medlemsstaterna skyldiga att genomföra ett identifieringsförfarande enligt artikel 5.2 och fastställa vilka enskilda leverantörer av DNS-, IXP- eller toppdomäntjänster (TLD) som behöver uppfylla it-säkerhetsdirektivets krav. Detta innebär att efter en sådan bedömning kommer endast de DNS-, IXP- eller TLD-leverantörer som motsvarar kriterierna i artikel 5.2 i it-säkerhetsdirektivet att vara skyldiga att uppfylla kraven i detta direktiv.

I artikel 1.3 anges det vidare att direktivets säkerhets- och rapporteringskrav inte heller ska tillämpas på leverantörer av betrodda tjänster som omfattas av liknande krav enligt artikel 19 i förordning (EU) nr 910/2014.

6. Offentliggjorda nationella dokument om cybersäkerhet.

	Medlemsstat	Strategins namn och tillgängliga länkar
1	Österrike	*Austrian Cybersecurity Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgien	*Securing Cyberspace* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulgarien	*Cyber Resilient Bulgaria 2020* (2016) http://www.cyberbg.eu/ (BG)
4	Kroatien	*The national cyber security strategy of the republic of Croatia* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Republiken Tjeckien	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Cypern	*Cybersecurity Strategy of the Republic of Cyprus* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Danmark	*The Danish Cyber and Information Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Estland	*Cyber Security Strategy* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Finland	*Finland´s Cyber security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Frankrike	*French national digital security strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Irland	*National Cyber Security Strategy 2015-2017* (2015)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Italien	*National Strategic Framework for Cyberspace Security* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Tyskland	*Cyber-security Strategy for Germany* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Ungern	*National Cyber Security Strategy of Hungary* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Lettland	*Cyber Security Strategy of Latvia 2014–2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Litauen	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luxemburg	*National Cybersecurity Strategy II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*National Cyber Security Strategy Green Paper* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Nederländerna	*National Cyber Security Strategy 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Polen	*Cyberspace Protection Policy of the Republic of Poland* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Rumänien	*Cybersecurity Strategy of Romania* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Portugal	*National Cyberspace Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view

		(EN)
23	Slovakien	*Cyber Security Concept of the Slovak Republic for 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Slovenien	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Spanien	*National Cyber Security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Sverige	*The Swedish National Cybersecurity Strategy* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Storbritannien	*National Cyber Security Strategy (2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Förteckning över god praxis och rekommendationer från Enisa.

För åtgärder vid incidenter

- ✓ Strategier för hantering av incidenter och samarbete vid cyberkriser[46]

För incidenthantering

- ✓ Projekt för automatisering i samband med incidenthantering[47]
- ✓ Vägledning för god praxis vi incidenthantering[48]

För incidentklassificering och taxonomi

- ✓ Översikt över befintliga taxonomier[49]
- ✓ Vägledning med god praxis för användning av taxonomier i samband med upptäckt och förebyggande av incidenter[50]

För CSIRT-mognadsgraden

- ✓ Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity[51]
- ✓ Study on CSIRT Maturity – Evaluation Process[52]
- ✓ Guidelines for national and governmental CSIRTs on how to assess maturity[53]

För kapacitetsuppbyggnad och utbildning för CSIRT

- ✓ Good Practice Guide on Training Methodologies[54]

För information om befintliga CSIRT-enheter i Europa – Översikt över CSIRT-enheter fördelade efter land[55]

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016). Tillgänglig på:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
[47] Mer information finns på: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[48] ENISA, *Good Practice Guide for Incident Management* (2010). Tillgänglig på:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[49] Mer information finns på: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies
[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Tillgänglig på:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). Tillgänglig på:https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). Tillgänglig på:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
[53] ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). Tillgänglig på: https://www.enisa.europa.eu/publications/csirt-capabilities
[54] ENISA, *Good Practice Guide on Training Methodologies* (2014). Tillgänglig på:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies
[55] Mer information finns på: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map