I

(Lagstiftningsakter)

DIREKTIV

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/1148

av den 6 juli 2016

om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([1]),

i enlighet med det ordinarie lagstiftningsförfarandet ([2]), och

av följande skäl:

(1) Nätverks- och informationssystem och nätverks- och informationstjänster spelar en viktig roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och i synnerhet för den inre marknadens funktion.

(2) Säkerhetsincidenter, som blir allt mer omfattande och vanliga och får allt större inverkan, utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Dessa system kan också bli mål för avsiktligt sabotage i syfte att skada dem eller förorsaka driftsavbrott. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande ekonomiska förluster, undergräva användarnas förtroende och medföra allvarliga konsekvenser för unionens ekonomi.

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

(4) På grundval av de betydande framstegen inom det europeiska forumet för medlemsstaterna vad gäller att främja diskussioner och utbyten av bästa praxis, inbegripet utarbetandet av principer för ett europeiskt samarbete vid it-relaterade kriser, bör en samarbetsgrupp inrättas, bestående av företrädare för medlemsstaterna, kommissionen och Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), som ska stödja och underlätta strategiskt

([1]) EUT C 271, 19.9.2013, s. 133.
([2]) Europaparlamentets ståndpunkt av den 13 mars 2014 (ännu ej offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 17 maj 2016 (ännu ej offentliggjord i EUT). Europaparlamentets ståndpunkt av den 6 juli 2016 (ännu ej offentliggjord i EUT).

samarbete mellan medlemsstaterna vad gäller säkerhet i nätverks- och informationssystem. För att denna grupp ska vara effektiv och inkluderande är det viktigt att alla medlemsstater har en minimikapacitet och en strategi som säkerställer en hög nivå på säkerheten i nätverks- och informationssystem på det egna territoriet. Dessutom bör säkerhets- och rapporteringskrav gälla för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, för att främja en riskhanteringskultur och säkerställa att de allvarligaste incidenterna rapporteras.

(5) Den befintliga kapaciteten räcker inte för att säkerställa en hög nivå på säkerheten i nätverks- och informationssystem i unionen. Medlemsstaterna har mycket olika beredskapsnivåer, vilket har lett till skilda tillvägagångssätt i unionen. Resultatet blir olika skyddsnivåer för konsumenter och företag, vilket undergräver den allmänna nivån på säkerheten i nätverks- och informationssystem i unionen. Avsaknaden av gemensamma krav för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster gör det i sin tur omöjligt att inrätta en övergripande och effektiv mekanism för samarbete på unionsnivå. Universitet och forskningscentrum har en avgörande roll att spela när det gäller att främja forskning, utveckling och innovation på dessa områden.

(6) Effektiva åtgärder för att lösa problemen vad gäller säkerhet i nätverks- och informationssystem förutsätter därför ett övergripande angreppssätt på unionsnivå, som omfattar en gemensam miniminivå för kapacitetsuppbyggnad och planering, utbyte av information, samarbete och gemensamma säkerhetskrav för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. Leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster är emellertid inte förhindrade att genomföra striktare säkerhetsåtgärder än de som föreskrivs i detta direktiv.

(7) Detta direktiv bör tillämpas på både leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, så att alla relevanta incidenter och risker täcks. De skyldigheter som införs för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster bör dock inte tillämpas på företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster i den mening som avses i Europaparlamentets och rådets direktiv 2002/21/EG ([1]), vilka omfattas av de specifika krav på säkerhet och integritet som föreskrivs i det direktivet, och inte heller på leverantörer av betrodda tjänster i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 910/2014 ([2]), vilka omfattas av de säkerhetskrav som föreskrivs i den förordningen.

(8) Detta direktiv bör inte påverka varje enskild medlemsstats möjlighet att vidta de åtgärder som är nödvändiga för att skydda dess väsentliga säkerhetsintressen, för att upprätthålla allmän ordning och säkerhet och för att möjliggöra utredning, upptäckt och lagföring av brott. Enligt artikel 346 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) ska ingen medlemsstat vara förpliktad att lämna information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen. Rådets beslut 2013/488/EU ([3]) och sekretessavtal, eller informella sekretessavtal såsom *Traffic Light Protocol*, är relevanta i detta sammanhang.

(9) Vissa ekonomiska sektorer regleras redan eller kan komma att regleras av sektorsspecifika unionsrättsakter som inbegriper regler med anknytning till säkerheten i nätverks- och informationssystem. När dessa unionsrättsakter innehåller bestämmelser med krav på säkerhet i nätverks- och informationssystem eller rapportering av incidenter, bör de bestämmelserna tillämpas, om de innehåller krav vilkas verkan minst motsvarar verkan av skyldigheterna i detta direktiv. Medlemsstaterna bör då tillämpa bestämmelserna i sådana sektorsspecifika unionsrättsakter, inklusive sådana som rör jurisdiktion, och bör inte genomföra identifieringsförfarandet för leverantörer av samhällsviktiga tjänster enligt definitionen i detta direktiv. Medlemsstaterna bör i detta sammanhang informera kommissionen om tillämpningen av sådana *lex specialis*-bestämmelser. Vid fastställandet av huruvida kraven på säkerhet i nätverks- och informationssystem och rapportering av incidenter som ingår i sektorsspecifika unionsrättsakter motsvarar kraven i detta direktiv, bör endast bestämmelserna i relevanta unionsrättsakter och deras tillämpning i medlemsstaterna beaktas.

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

([1]) Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv) (EGT L 108, 24.4.2002, s. 33).

([2]) Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

([3]) Rådets beslut 2013/488/EU av den 23 september 2013 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 274, 15.10.2013, s. 1).

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

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

(13) Operativ risk utgör en viktig del av reglering och tillsyn inom banksektorn och sektorn för finansmarknadsinfrastrukturer. Den omfattar all verksamhet, inbegripet nätverks- och informationssystems säkerhet, integritet och motståndskraft. Kraven på dessa system, som ofta är mer långtgående än de som föreskrivs i detta direktiv, fastställs i ett antal unionsrättsakter, som inbegriper bestämmelser om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag och bestämmelser om tillsynskrav för kreditinstitut och värdepappersföretag, vilka inbegriper krav avseende operativ risk, bestämmelser om marknader för finansiella instrument, vilka inbegriper krav avseende riskbedömning för värdepappersföretag och för reglerade marknader, bestämmelser om OTC-derivat, centrala motparter och transaktionsregister, vilka inbegriper krav avseende operativ risk för centrala motparter och transaktionsregister, och bestämmelser om förbättrad värdepappersavveckling i unionen och om värdepapperscentraler, vilka inbegriper krav avseende operativ risk. Dessutom utgör krav på rapportering av incidenter en del av normal tillsynspraxis inom finanssektorn och ingår ofta i tillsynshandböcker. Medlemsstaterna bör beakta dessa bestämmelser och krav vid tillämpningen av *lex specialis*.

(14) Såsom Europeiska centralbanken konstaterade i sitt yttrande av den 25 juli 2014 ([1]) påverkar detta direktiv inte den ordning för Eurosystemets tillsyn över betalnings- och avvecklingssystem som fastställs i unionsrätten. Det skulle vara lämpligt att de myndigheter som ansvarar för denna övervakning utbytte erfarenheter om frågor som rör säkerhet i nätverks- och informationssystem med de behöriga myndigheterna enligt detta direktiv. Detsamma gäller för medlemmar i Europeiska centralbankssystemet som står utanför euroområdet och som utövar sådan tillsyn över betalnings- och avvecklingssystem på grundval av nationella lagar och andra författningar.

(15) En internetbaserad marknadsplats ger konsumenter och näringsidkare möjlighet att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare och är slutdestinationen för ingåendet av sådana avtal. Den bör inte omfatta onlinetjänster som endast fungerar som mellanhand för tredjepartstjänster genom vilka ett avtal slutligen kan ingås. Den bör därför inte omfatta onlinetjänster som jämför priset på vissa varor eller tjänster från olika näringsidkare och sedan leder användaren vidare till den näringsidkare som valts för köp av varan. Datatjänster som tillhandahålls av den internetbaserade marknadsplatsen kan inbegripa behandling av transaktioner, sammanställning av data eller profilering av användare. Applikationsbutiker, som fungerar som onlinebutiker och möjliggör digital distribution av applikationer eller programvara från tredje part, ska betraktas som en typ av internetbaserad marknadsplats.

(16) En internetbaserad sökmotor gör det möjligt för användaren att göra sökningar på i princip alla webbplatser på grundval av en sökning inom vilket ämnesområde som helst. Den kan också vara inriktad på webbplatser på ett visst språk. Definitionen av internetbaserad sökmotor enligt detta direktiv bör inte omfatta sökfunktioner som begränsas till innehållet på en särskild webbplats, oberoende av om sökfunktionen tillhandahålls av en extern sökmotor. Den bör inte heller omfatta onlinetjänster som jämför priset på vissa varor eller tjänster från olika näringsidkare och sedan leder användaren vidare till den näringsidkare som valts för köp av varan.

(17) Molntjänster omfattar många olika verksamheter, som kan levereras enligt olika modeller. Vid tillämpningen av detta direktiv omfattar termen *molntjänster* tjänster som medger åtkomst till en skalbar och elastisk pool av delbara dataresurser. Sådana dataresurser omfattar resurser såsom nätverk, servrar eller annan infrastruktur, lagring, applikationer och tjänster. Termen *skalbar* avser dataresurser som leverantören av molntjänster fördelar på ett flexibelt sätt, oberoende av resursernas geografiska läge, för att hantera fluktuationer i efterfrågan. Termen *elastisk pool* används för att beskriva dataresurser som avsätts och utnyttjas beroende på efterfrågan för att

([1]) EUT C 352, 7.10.2014, s. 4.

tillgängliga resurser snabbt ska kunna utökas och minskas i takt med arbetsbördan. Termen *delbar* används för att beskriva dataresurser som tillhandahålls flera användare som delar en gemensam åtkomst till tjänsten där behandlingen genomförs separat för varje användare, även om tjänsten tillhandahålls från samma elektroniska utrustning.

(18) En internetknutpunkts (IXP) uppgift är att koppla samman nätverk. En IXP tillhandahåller inte tillträde till nätverk och fungerar inte som transitleverantör eller transitförmedlare. En IXP tillhandahåller inte heller andra tjänster utan samband med sammankoppling, även om detta inte hindrar en IXP-leverantör från att tillhandahålla andra tjänster. En IXP är till för att sammankoppla nätverk som är tekniskt och organisatoriskt separata. Termen *autonomt system* används för att beskriva ett tekniskt fristående nätverk.

(19) Medlemsstaterna bör ansvara för att fastställa vilka enheter som uppfyller kriterierna för definitionen av leverantör av samhällsviktiga tjänster. I syfte att säkerställa ett enhetligt tillvägagångssätt bör definitionen av leverantör av samhällsviktiga tjänster tillämpas konsekvent i alla medlemsstater. I detta syfte föreskriver detta direktiv en bedömning av de enheter som är verksamma i specifika sektorer och delsektorer, upprättandet av en förteckning över samhällsviktiga tjänster, beaktandet av en gemensam förteckning över sektorsöverskridande faktorer för fastställande av om en eventuell incident skulle medföra en betydande störning, en samrådsprocess med de berörda medlemsstaterna i de fall där enheter tillhandahåller tjänster i mer än en medlemsstat, och samarbetsgruppens stöd vid identifieringsförfarandet. I syfte att säkerställa att eventuella förändringar på marknaden återspeglas på ett korrekt sätt bör förteckningen över identifierade leverantörer regelbundet ses över av medlemsstaterna och vid behov uppdateras. Medlemsstaterna bör slutligen till kommissionen överlämna den information som är nödvändig för att bedöma i vilken utsträckning denna gemensamma metod har gjort det möjligt för medlemsstaterna att tillämpa definitionen konsekvent.

(20) Vid förfarandet för identifiering av leverantörer av samhällsviktiga tjänster bör medlemsstaterna, åtminstone för varje delsektor som avses i detta direktiv, bedöma vilka tjänster som måste betraktas som viktiga för att upprätthålla kritisk samhällelig och ekonomisk verksamhet samt huruvida de enheter som är förtecknade i de sektorer och delsektorer som avses i detta direktiv och tillhandahåller dessa tjänster uppfyller kriterierna för identifiering av leverantörer. Vid bedömning av huruvida en enhet tillhandahåller en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, är det tillräckligt att undersöka om enheten tillhandahåller en tjänst som finns upptagen i förteckningen över samhällsviktiga tjänster. Det bör dessutom påvisas att tillhandahållandet av den samhällsviktiga tjänsten är beroende av nätverks- och informationssystem. Slutligen bör medlemsstaterna, vid bedömning av huruvida en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten, beakta ett antal sektorsöverskridande faktorer samt, i lämpliga fall, sektorsspecifika faktorer.

(21) Vid identifiering av leverantörer av samhällsviktiga tjänster krävs det att leverantören utför en faktisk och reell verksamhet med hjälp av en stabil struktur för att den ska anses vara etablerad i en medlemsstat. Den rättsliga formen för en sådan struktur bör här, oavsett om det är en filial eller ett dotterbolag med juridisk personlighet, inte vara den avgörande faktorn.

(22) Det är möjligt att enheter verksamma inom de sektorer och delsektorer som avses i detta direktiv tillhandahåller både samhällsviktiga och icke samhällsviktiga tjänster. Inom luftfartssektorn tillhandahåller t.ex. flygplatser tjänster som en medlemsstat kan anse vara samhällsviktiga, såsom skötseln av start- och landningsbanorna, men också ett antal tjänster som kan betraktas som icke samhällsviktiga, såsom tillhandahållande av butiksområden. Leverantörer av samhällsviktiga tjänster bör omfattas av de specifika säkerhetskraven endast när det gäller tjänster som anses vara samhällsviktiga. I syfte att identifiera leverantörer bör medlemsstaterna därför upprätta en förteckning över de tjänster som betraktas som samhällsviktiga.

(23) Förteckningen över tjänster bör omfatta alla de tjänster som tillhandahålls på en viss medlemsstats territorium och som uppfyller kraven enligt detta direktiv. Medlemsstaterna bör kunna lägga till nya tjänster i den befintliga förteckningen. Förteckningen över tjänster bör fungera som referenspunkt för medlemsstaterna och möjliggöra identifiering av leverantörer av samhällsviktiga tjänster. Syftet med förteckningen är att identifiera de typer av samhällsviktiga tjänster inom en viss sektor som det hänvisas till i detta direktiv och därmed skilja dem från de icke samhällsviktiga tjänster som en enhet med verksamhet inom en viss sektor kan ansvara för. Den förteckning över tjänster som varje medlemsstat upprättar skulle utgöra ett ytterligare bidrag till bedömningen av lagstiftningspraxis inom varje medlemsstat med syftet att säkerställa en övergripande enhetlighet mellan medlemsstaternas identifieringsförfaranden.

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

(25) Till följd av identifieringsförfarandet bör medlemsstaterna vidta nationella åtgärder för att fastställa vilka enheter som omfattas av skyldigheter när det gäller säkerhet i nätverks- och informationssystem. Detta skulle kunna uppnås genom upprättande av en förteckning över alla leverantörer av samhällsviktiga tjänster eller genom antagande av nationella bestämmelser, inbegripet objektivt mätbara kriterier, såsom leverantörens produktion eller antalet användare, som gör det möjligt att fastställa vilka enheter som omfattas av skyldigheter när det gäller säkerhet i nätverks- och informationssystem. De nationella åtgärderna, oavsett om de redan har vidtagits eller om de vidtas mot bakgrund av detta direktiv, bör omfatta alla rättsliga åtgärder, administrativa åtgärder och strategier som möjliggör identifiering av leverantörer av samhällsviktiga tjänster enligt detta direktiv.

(26) För att ge en indikation om betydelsen i förhållande till den berörda sektorn av de identifierade leverantörerna av samhällsviktiga tjänster, bör medlemsstaterna beakta dessa leverantörers antal och storlek, till exempel i form av marknadsandelar eller den mängd som produceras eller levereras, utan att vara förpliktade att lämna ut uppgifter som skulle avslöja vilka leverantörer som har identifierats.

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

(28) Utöver de sektorsöverskridande faktorerna bör också sektorsspecifika faktorer beaktas vid fastställelsen av huruvida en incident skulle medföra en betydande störning vid tillhandahållandet av en samhällsviktig tjänst. När det gäller energileverantörer kan sådana faktorer omfatta mängden eller andelen producerad nationell el, för oljeleverantörer mängden olja per dag, för lufttransport, inbegripet flygplatser och lufttrafikföretag, järnvägstransport och kusthamnar andelen nationell trafikmängd och antalet passagerare eller lastningar per år, för bankverksamhet eller finansmarknadsinfrastrukturer deras betydelse för systemet på grundval av samlade tillgångar eller förhållandet mellan dessa tillgångar och BNP, för hälso- och sjukvårdssektorn antalet patienter som leverantören vårdar per år, för produktion, bearbetning och leverans av vatten, volym, antal och typer av användare, inbegripet t.ex. sjukhus, offentlig sektor, organisationer och personer) samt förekomsten av alternativa vattenkällor för samma geografiska område.

(29) För att uppnå och bibehålla en hög nivå på säkerheten i nätverks- och informationssystem bör alla medlemsstater ha en nationell strategi för säkerhet i nätverks- och informationssystem genom vilken fastställs de strategiska mål och konkreta politiska åtgärder som ska genomföras.

(30) Mot bakgrund av skillnaderna i nationella förvaltningsstrukturer och för att skydda befintliga sektorsspecifika arrangemang eller unionens tillsyns- och regleringsmyndigheter och undvika överlappning, bör medlemsstaterna kunna utse mer än en nationell behörig myndighet med ansvar för att utföra uppgifter som rör säkerheten i de nätverks- och informationssystem som används av leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster enligt detta direktiv.

(31) För att underlätta gränsöverskridande samarbete och kommunikation och för att göra det möjligt att genomföra detta direktiv på ett effektivt sätt måste varje medlemsstat, utan att det påverkar sektorsspecifika regleringsarrangemang, utse en nationell gemensam kontaktpunkt med ansvar för samordningen av frågor angående säkerhet i nätverks- och informationssystem och gränsöverskridande samarbete på unionsnivå. Behöriga myndigheter och gemensamma kontaktpunkter bör förses med de tekniska och finansiella resurser och personalresurser som de behöver för att på ett effektivt sätt kunna utföra de uppgifter som de tilldelas och därmed uppnå målen med detta direktiv. Eftersom syftet med detta direktiv är att förbättra den inre marknadens funktion genom att skapa tillit och förtroende, måste medlemsstaternas organ kunna samarbeta effektivt med ekonomiska aktörer och ha en struktur som är förenlig med detta.

(32) Behöriga myndigheter eller enheter för hantering av it-säkerhetsincidenter (*Computer Security Incident Response Teams*, nedan kallade *CSIRT-enheter*) bör ta emot rapporter om incidenter. De gemensamma kontaktpunkterna bör inte direkt ta emot några rapporter om incidenter, såvida de inte också fungerar som behörig myndighet eller som en CSIRT-enhet. En behörig myndighet eller en CSIRT-enhet bör dock kunna ge den gemensamma kontaktpunkten i uppgift att vidarebefordra incidentrapporter till de gemensamma kontaktpunkterna i andra berörda medlemsstater.

(33) För att säkerställa att medlemsstaterna och kommissionen får information på ett ändamålsenligt sätt bör den gemensamma kontaktpunkten lämna en sammanfattande rapport till samarbetsgruppen som bör vara anonymiserad för att bevara rapporternas konfidentialitet och identiteten på leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, eftersom information om de rapporterande enheternas identitet inte krävs för utbyte av bästa praxis inom samarbetsgruppen. Den sammanfattande rapporten bör innehålla uppgifter om antalet mottagna incidentrapporter samt information om de rapporterade incidenternas art, såsom vilka typer av säkerhetsöverträdelser det rör sig om eller hur allvarliga eller långvariga de varit.

(34) Medlemsstaterna bör ha både den tekniska och organisatoriska kapacitet som krävs för att förebygga, upptäcka, vidta åtgärder mot och begränsa effekterna av incidenter och risker vad gäller nätverks- och informationssystem. Medlemsstater bör därför säkerställa att de har väl fungerande CSIRT-enheter, även kallade *incidenthanteringsorganisationer* (*Computer Emergency Response Teams*, Cert), som uppfyller grundläggande krav för att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå. För att alla typer av leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster ska kunna dra nytta av sådan kapacitet och sådant samarbete bör medlemsstaterna säkerställa att alla typer omfattas av en utsedd CSIRT-enhet. Med tanke på vikten av internationellt samarbete på området cybersäkerhet, bör CSIRT-enheterna kunna delta i internationella samarbetsnätverk utöver det CSIRT-nätverk som inrättas genom detta direktiv.

(35) Eftersom de flesta nätverks- och informationssystem drivs privat, är det mycket viktigt med samarbete mellan offentlig och privat sektor. Leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster bör uppmuntras att upprätta egna informella samarbetsmekanismer för att säkerställa säkerheten i nätverks- och informationssystem. Samarbetsgruppen bör vid behov kunna bjuda in berörda parter till diskussionerna. För att effektivt uppmuntra utbyte av information och bästa praxis är det mycket viktigt att säkerställa att samarbetet inte leder till nackdelar för de leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster som deltar i sådana utbyten.

(36) Enisa bör bistå medlemsstaterna och kommissionen genom att tillhandahålla expertis och rådgivning och underlätta utbytet av bästa praxis. Kommissionen bör samråda med Enisa vid tillämpningen av detta direktiv, och medlemsstaterna bör ha möjlighet att göra detta. För att bygga upp kapacitet och kunskap bland medlemsstaterna bör samarbetsgruppen också fungera som ett instrument för utbyte av bästa praxis, diskussioner om medlemsstaternas kapacitet och beredskap och, på frivillig grund, bistå medlemmarna vid utvärdering av nationella strategier för säkerhet i nätverks- och informationssystem, vid kapacitetsuppbyggnad och utvärderingar av övningar som avser säkerheten i nätverks- och informationssystem.

(37) Medlemsstaterna bör vid behov kunna använda eller anpassa befintliga organisationsstrukturer eller strategier vid tillämpningen av detta direktiv.

(38) Samarbetsgruppens och Enisas respektive uppgifter är beroende av och kompletterar varandra. Enisa bör generellt bistå samarbetsgruppen i utförandet av dess uppgifter i enlighet med Enisas mål enligt Europaparlamentets och rådets förordning (EU) nr 526/2013 [1], nämligen att bistå unionens institutioner, organ och byråer samt medlemsstaterna med att genomföra de strategier som krävs för att uppfylla rättsliga och regleringsmässiga krav på säkerhet i nätverks- och informationssystem i befintliga och framtida unionsrättsakter. Enisa bör särskilt tillhandahålla bistånd på de områden som motsvarar dess egna uppgifter enligt förordning (EU) nr 526/2013, nämligen att analysera strategier för säkerhet i nätverks- och informationssystem, stödja anordnandet och genomförandet av övningar på unionsnivå som avser säkerhet i nätverks- och informationssystem samt utbyta information och bästa praxis vad gäller åtgärder för ökad medvetenhet och utbildning. Enisa bör också delta i utarbetandet av riktlinjer för sektorsspecifika kriterier för fastställande av hur betydande en incidents inverkan är.

[1] Europaparlamentets och rådets förordning (EU) nr 526/2013 av den 21 maj 2013 om Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och om upphävande av förordning (EG) nr 460/2004 (EUT L 165, 18.6.2013, s. 41).

(39) I syfte att främja avancerad säkerhet i nätverks- och informationssystem bör samarbetsgruppen vid behov samarbeta med berörda unionsinstitutioner, -organ, och -byråer för att utbyta sakkunskap och bästa praxis samt ge råd om säkerhetsaspekter på nätverks- och informationssystem som kan påverka deras arbete, samtidigt som befintliga arrangemang för utbyte av konfidentiell information respekteras. Vid samarbete med rättsvårdande myndigheter om säkerhetsaspekter på nätverks- och informationssystem som kan påverka deras arbete bör samarbetsgruppen respektera befintliga informationskanaler och etablerade nätverk.

(40) Information om incidenter blir allt mer värdefull för allmänheten och företag, särskilt små och medelstora företag. I vissa fall tillhandahålls sådan information redan via webbplatser på nationell nivå, på ett specifikt lands språk, och är främst inriktad på incidenter och händelser med en nationell dimension. Eftersom företag i allt större utsträckning bedriver gränsöverskridande verksamhet och medborgare använder onlinetjänster, bör information om incidenter tillhandahållas i samlad form på unionsnivå. CSIRT-nätverkets sekretariat uppmuntras att upprätta en webbplats eller upplåta utrymme åt en särskild sida på en befintlig webbplats, där allmän information om allvarliga incidenter i unionen görs tillgänglig för allmänheten. Informationen ska vara särskilt inriktad på företags intressen och behov. CSIRT-enheter som deltar i CSIRT-nätverket uppmanas att på frivillig grund tillhandahålla den information som ska offentliggöras på denna webbplats, utan att därvid inkludera konfidentiell eller känslig information.

(41) I fall då information anses vara konfidentiell enligt unionsbestämmelser och nationella bestämmelser om affärshemligheter, bör konfidentiell behandling säkerställas vid genomförande av verksamhet och uppfyllande av mål enligt detta direktiv.

(42) Övningar där incidentscenarier simuleras i realtid är viktiga för att testa medlemsstaternas beredskap och samarbete när det gäller säkerhet i nätverks- och informationssystem. Övningsserien CyberEurope, som samordnas av Enisa med deltagande av medlemsstaterna är ett användbart verktyg för att testa och utarbeta rekommendationer för hur incidenthanteringen på unionsnivå bör förbättras med tiden. Med tanke på att medlemsstaterna för närvarande inte har någon skyldighet att vare sig planera eller delta i övningar, bör inrättandet av CSIRT-nätverket enligt detta direktiv göra det möjligt för medlemsstaterna att delta i övningar på grundval av noggrann planering och strategiska val. Den samarbetsgrupp som inrättas enligt detta direktiv bör diskutera de strategiska besluten om övningar, särskilt men inte enbart när det gäller övningarnas regelbundenhet och utformningen av scenarierna. Enisa bör i enlighet med sitt mandat stödja anordnandet och genomförandet av unionsomfattande övningar genom att tillhandahålla expertis och rådgivning till samarbetsgruppen och CSIRT-nätverket.

(43) I och med att säkerhetsproblem som påverkar nätverks- och informationssystem är globala till sin natur behövs ett närmare internationellt samarbete för att förbättra säkerhetsstandarder och informationsutbyte och för att främja ett gemensamt sätt att hantera säkerhetsfrågor.

(44) Ansvaret för att säkerställa säkerheten i nätverks- och informationssystemen vilar i hög grad på leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. En riskhanteringskultur, som inbegriper riskbedömning och genomförande av säkerhetsåtgärder som är anpassade till riskerna, bör främjas och utvecklas genom ändamålsenliga krav i lagstiftning och frivillig branschpraxis. Att skapa trovärdiga och lika konkurrensvillkor är också avgörande för att samarbetsgruppen och CSIRT-nätverket ska fungera effektivt och för att säkerställa ett effektivt samarbete från alla medlemsstater.

(45) Detta direktiv är tillämpligt endast på offentliga förvaltningar vilka identifieras som leverantörer av samhällsviktiga tjänster. Det är därför medlemsstaternas ansvar att säkerställa säkerheten i nätverks- och informationssystem som används av offentliga förvaltningar som inte omfattas av detta direktiv.

(46) Åtgärder för riskhantering omfattar åtgärder för att identifiera alla incidentrisker, för att förebygga, upptäcka och hantera incidenter och för att begränsa deras inverkan. Säkerheten i nätverks- och informationssystem omfattar lagrade, överförda och behandlade uppgifters säkerhet.

(47) Behöriga myndigheter bör behålla rätten att anta nationella riktlinjer angående de omständigheter under vilka leverantörer av samhällsviktiga tjänster är skyldiga att rapportera incidenter.

(48) Många företag i unionen är beroende av leverantörer av digitala tjänster för att tillhandahålla sina tjänster. Eftersom vissa digitala tjänster skulle kunna utgöra en viktig resurs för sina användare, inklusive leverantörer av samhällsviktiga tjänster, och dessa användare inte alltid har alternativ tillgängliga, bör detta direktiv också gälla för leverantörer av sådana tjänster. För många företag är säkerheten, kontinuiteten och tillförlitligheten hos den typ av digitala tjänster som avses i detta direktiv av avgörande betydelse för att företaget ska fungera väl. En störning i en sådan digital tjänst kan hindra tillhandahållandet av andra tjänster som är beroende av den och därmed påverka viktig ekonomisk och samhällelig verksamhet i unionen. Sådana digitala tjänster skulle därför kunna vara av avgörande betydelse för att företag som är beroende av dem ska fungera väl och för dessa företags deltagande i den inre marknaden och den gränsöverskridande handeln inom unionen. Leverantörer av digitala tjänster som omfattas av detta direktiv är sådana som anses erbjuda digitala tjänster som många företag i unionen i allt högre grad är beroende av.

(49) Leverantörer av digitala tjänster bör säkerställa en säkerhetsnivå som är anpassad till graden av risk för de digitala tjänster som de tillhandahåller, med beaktande av den betydelse som deras tjänster har för verksamhet som bedrivs av andra företag inom unionen. Graden av risk för leverantörer av samhällsviktiga tjänster, som ofta är viktiga för att upprätthålla kritisk samhällelig och ekonomisk verksamhet, är i praktiken högre än för leverantörer av digitala tjänster. Säkerhetskraven för leverantörer av digitala tjänster bör därför vara lindrigare. Leverantörer av digitala tjänster bör fritt kunna vidta de åtgärder som de anser lämpliga för att hantera risker för säkerheten i deras nätverks- och informationssystem. Leverantörer av digitala tjänster bör, på grund av den gränsöverskridande arten, omfattas av ett mer harmoniserat tillvägagångssätt på unionsnivå. Genomförandeakter bör underlätta fastställandet och genomförandet av sådana åtgärder.

(50) Trots att hårdvarutillverkare och mjukvaruutvecklare varken är leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster, ökar deras produkter säkerheten i nätverks- och informationssystem. De spelar därför en viktig roll när det gäller att göra det möjligt för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster att skydda sina nätverks- och informationssystem. Sådana hårdvaru- och mjukvaruprodukter omfattas redan av befintliga bestämmelser om produktansvar.

(51) De tekniska och organisatoriska åtgärder som leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster åläggs bör inte innebära krav på att någon särskild kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt.

(52) Leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster bör säkerställa säkerheten i de nätverks- och informationssystem som de använder. Det rör sig framför allt om privata nätverks- och informationssystem som antingen förvaltas av deras interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Säkerhets- och rapporteringskraven bör gälla för relevanta leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, oavsett om de sköter underhållet av sina nätverks- och informationssystem internt eller lägger ut uppgifterna på entreprenad.

(53) För att undvika oproportionella finansiella och administrativa bördor för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster bör kraven stå i proportion till den risk som det berörda nätverks- och informationssystemet utgör, med beaktande av den senaste tekniska utvecklingen. När det gäller leverantörer av digitala tjänster, bör dessa krav inte gälla för mikroföretag och små företag.

(54) När offentliga förvaltningar i medlemsstaterna använder tjänster som erbjuds av leverantörer av digitala tjänster, särskilt molntjänster, är det möjligt att de från leverantörerna av dessa tjänster vill kräva ytterligare säkerhetsåtgärder utöver dem som leverantörer av digitala tjänster vanligtvis skulle erbjuda i överensstämmelse med kraven i detta direktiv. De bör kunna göra detta genom avtalsförpliktelser.

(55) Definitionerna av internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster i detta direktiv är specifika för det här direktivet och påverkar inte andra instrument.

(56) Detta direktiv bör inte hindra medlemsstaterna från att anta nationella åtgärder som innebär krav på offentliga organ att säkerställa särskilda säkerhetskrav när de sluter avtal om molntjänster. Alla sådana nationella åtgärder bör tillämpas på det berörda offentliga organet och inte på leverantören av molntjänster.

(57) Med tanke på de avgörande skillnaderna mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, särskilt de förstnämndas direkta koppling till fysisk infrastruktur och de senares gränsöverskridande art, bör harmoniseringsnivån för dessa två grupper av enheter i detta direktiv differentieras. Medlemsstaterna bör kunna identifiera de relevanta leverantörerna av samhällsviktiga tjänster och införa strängare krav än de som fastställs i detta direktiv. Medlemsstaterna bör inte identifiera leverantörer av digitala tjänster, eftersom detta direktiv bör gälla för alla leverantörer av digitala tjänster som omfattas av dess tillämpningsområde. Dessutom bör detta direktiv och de genomförandeakter som antas enligt detsamma säkerställa en hög harmoniseringsnivå för leverantörer av digitala tjänster med avseende på säkerhets- och rapporteringskrav. Detta bör möjliggöra en enhetlig behandling av leverantörer av digitala tjänster i hela unionen, på ett sätt som står i proportion till leverantörernas art och den grad av risk de kan utsättas för.

(58) Utan att det påverkar medlemsstaternas skyldigheter enligt unionsrätten bör detta direktiv inte hindra medlemsstaterna från att införa säkerhets- och rapporteringskrav för enheter som inte är leverantörer av digitala tjänster inom ramen för detta direktivs tillämpningsområde.

(59) Behöriga myndigheter bör säkerställa att de upprätthåller informella och tillförlitliga kanaler för informationsutbyte. Vid offentliggörande av incidenter som rapporteras till de behöriga myndigheterna bör allmänhetens intresse av att få information om hot vägas mot eventuell renomméskada och kommersiell skada för de leverantörer av samhällsviktiga tjänster och de leverantörer av digitala tjänster som rapporterar incidenter. Vid genomförandet av rapporteringsskyldigheterna bör behöriga myndigheter och CSIRT-enheterna särskilt ta hänsyn till behovet av att hålla uppgifter om produkters sårbara aspekter strikt konfidentiella till dess att lämpliga säkerhetslösningar släpps.

(60) Leverantörer av digitala tjänster bör omfattas av mindre ingripande, reaktiv efterhandstillsyn som är anpassad till deras tjänsters och verksamheters art. Den berörda behöriga myndigheten bör därför endast vidta åtgärder när den har mottagit bevis – till exempel från leverantören av digitala tjänster själv, från en annan behörig myndighet, inbegripet en behörig myndighet i en annan medlemsstat, eller från en tjänsteanvändare – för att en leverantör av digitala tjänster inte uppfyller kraven i detta direktiv, särskilt efter en incident. Den behöriga myndigheten bör därför inte ha någon allmän skyldighet att utöva tillsyn av leverantörer av digitala tjänster.

(61) Behöriga myndigheter bör ha de medel som de behöver för att kunna fullgöra sina förpliktelser, inbegripet befogenhet att inhämta tillräckligt med information för att bedöma nivån på säkerheten i nätverks- och informationssystem.

(62) Incidenter kan vara en följd av brottslig verksamhet, vars förebyggande, utredning och lagföring stöds av samordning och samarbete mellan leverantörer av samhällsviktiga tjänster, leverantörer av digitala tjänster, behöriga myndigheter och rättsvårdande myndigheter. Om en incident misstänks ha samband med allvarlig brottslig verksamhet enligt unionsrätt eller nationell rätt, bör medlemsstaterna uppmuntra leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster att rapportera incidenter som misstänks vara av allvarlig brottslig art till de relevanta rättsvårdande myndigheterna. När så är lämpligt är det önskvärt att samordningen mellan behöriga myndigheter och rättsvårdande myndigheter i olika medlemsstater underlättas av Europeiska it-brottscentrumet (EC3) och Enisa.

(63) Säkerheten för personuppgifter undergrävs ofta till följd av incidenter. I detta sammanhang bör behöriga myndigheter och dataskyddsmyndigheter samarbeta och utbyta information om alla relevanta frågor för att hantera personuppgiftsincidenter till följd av incidenter.

(64) Jurisdiktion över leverantörer av digitala tjänster bör tillkomma den medlemsstat där den berörda leverantören av digitala tjänster har sitt huvudsakliga etableringsställe i unionen, vilket i princip motsvarar den plats där leverantören har sitt huvudkontor i unionen. Det krävs att leverantören utför en faktisk och reell verksamhet med hjälp av en stabil struktur för att den ska anses vara etablerad. Den rättsliga formen för en sådan struktur bör här, oavsett om det är en filial eller ett dotterbolag med juridisk personlighet, inte vara den avgörande faktorn. Detta

kriterium bör inte vara avhängigt av om nätverks- och informationssystemen är fysiskt belägna på en viss plats; att sådana system finns och används innebär inte i sig att det rör sig om ett huvudsakligt etableringsställe och utgör därför inte ett kriterium för att fastställa det huvudsakliga etableringsstället.

(65) En leverantör av digitala tjänster som inte är etablerad i unionen men erbjuder tjänster inom unionen bör utse en företrädare. I syfte att fastställa om en sådan leverantör av digitala tjänster erbjuder tjänster inom unionen bör det kontrolleras om det är uppenbart att leverantören av digitala tjänster planerar att erbjuda tjänster till personer i en eller flera medlemsstater. Enbart den omständigheten att en webbplats tillhörande leverantören av digitala tjänster eller en mellanhand, eller en e-postadress och andra kontaktuppgifter, är tillgängliga i unionen, eller att ett språk används som allmänt används i det tredjeland där leverantören av digitala tjänster är etablerad, är inte tillräcklig för att fastställa en sådan avsikt. Emellertid kan faktorer som att det används ett visst språk eller en viss valuta som allmänt används i en eller flera medlemsstater med möjligheten att beställa tjänster på detta andra språk, eller att kunder eller användare i unionen omnämns, göra det uppenbart att leverantören av digitala tjänster planerar att erbjuda tjänster inom unionen. Företrädaren bör agera på leverantören av digitala tjänsters vägnar och det bör vara möjligt för behöriga myndigheter eller CSIRT-enheterna att kontakta företrädaren. Företrädaren bör utses uttryckligen genom en skriftlig fullmakt från leverantören av digitala tjänster att agera på dess vägnar med avseende på leverantörens skyldigheter enligt detta direktiv, inklusive incidentrapportering.

(66) Standardisering av säkerhetskrav är en marknadsdriven process. För att säkerställa en enhetlig tillämpning av säkerhetsstandarder bör medlemsstaterna främja efterlevnad eller överensstämmelse med specificerade standarder för att garantera en hög nivå på säkerheten i nätverks- och informationssystem på unionsnivå. Enisa bör bistå medlemsstaterna genom rådgivning och riktlinjer. Därför kan det vara lämpligt att utarbeta harmoniserade standarder, i enlighet med Europaparlamentets och rådets förordning (EU) nr 1025/2012 ([1]).

(67) Enheter som inte omfattas av detta direktivs tillämpningsområde kan drabbas av incidenter med en betydande inverkan på de tjänster som de tillhandahåller. Om dessa enheter anser att det ligger i allmänhetens intresse att rapportera förekomsten av sådana incidenter till de berörda myndigheterna i medlemsstaterna, bör de kunna göra det på frivillig grund. Sådana rapporter bör behandlas av den behöriga myndigheten eller CSIRT-enheten förutsatt att behandlingen inte utgör en oproportionell eller orimlig börda för de berörda medlemsstaterna.

(68) För att säkerställa enhetliga villkor för genomförandet av detta direktiv bör kommissionen tilldelas genomförandebefogenheter för att fastställa de förfaranden som krävs för samarbetsgruppens verksamhet och de säkerhets- och rapporteringskrav som är tillämpliga på leverantörer av digitala tjänster. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([2]). När kommissionen antar genomförandeakter om de förfaranden som krävs för samarbetsgruppens verksamhet bör den ta största hänsyn till yttrandet från Enisa.

(69) När kommissionen antar genomförandeakter om säkerhetskraven för leverantörer av digitala tjänster bör den ta största hänsyn till yttrandet från Enisa och samråda med berörda parter. Kommissionen uppmuntras dessutom att beakta följande exempel: när det gäller systems och anläggningars säkerhet: fysisk säkerhet och miljösäkerhet, funktionssäkerhet, kontroll av åtkomst till nätverks- och informationssystem samt nätverks- och informationssystemens integritet; när det gäller incidenthantering: incidenthanteringsförfaranden, kapacitet att upptäcka incidenter, incidentrapportering och kommunikation; när det gäller driftskontinuitetshantering: strategier för tjänstekontinuitet samt beredskapsplaner, kapacitet för katastrofberedskap; när det gäller övervakning, revision och testning: strategier för övervakning och loggning, beredskapsövningar, testning av nätverks- och informationssystem, säkerhetsbedömningar och övervakning av efterlevnaden.

(70) Vid genomförandet av detta direktiv bör kommissionen på lämpligt sätt samarbeta med relevanta sektorskommittéer och organ som inrättas på unionsnivå inom de områden som omfattas av detta direktiv.

([1]) Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

([2]) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

(71) Detta direktiv bör med jämna mellanrum ses över av kommissionen i samråd med berörda parter, främst i syfte att avgöra behovet av ändringar med hänsyn till samhällsutvecklingen, den politiska utvecklingen, den tekniska utvecklingen eller ändrade marknadsvillkor.

(72) Utbytet av information om risker och incidenter inom samarbetsgruppen och CSIRT-nätverket och uppfyllandet av kravet att rapportera incidenter till de behöriga nationella myndigheterna eller CSIRT-enheterna kan kräva behandling av personuppgifter. Sådan behandling bör ske i enlighet med Europaparlamentets och rådets direktiv 95/46/EG ([1]) och Europaparlamentets och rådets förordning (EG) nr 45/2001 ([2]). Vid tillämpningen av detta direktiv bör Europaparlamentets och rådets förordning (EG) nr 1049/2001 ([3]) tillämpas där så är lämpligt.

(73) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den 14 juni 2013 ([4]).

(74) Eftersom målet för detta direktiv, nämligen att uppnå en hög gemensam nivå på säkerheten i nätverks- och informationssystem i unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå detta mål.

(75) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna, i synnerhet rätten till respekt för privatliv och kommunikationer, skydd av personuppgifter, näringsfriheten, rätten till egendom, rätten till ett effektivt rättsmedel och rätten att yttra sig. Detta direktiv bör genomföras i enlighet med dessa rättigheter och principer.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte och tillämpningsområde

1. I detta direktiv fastställs åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverks- och informationssystem inom unionen, i syfte att förbättra den inre marknadens funktion.

2. Direktivet omfattar i detta syfte följande:

a) Det fastställer skyldigheter för alla medlemsstater att anta en nationell strategi för säkerhet i nätverks- och informationssystem.

b) Det inrättar en samarbetsgrupp i syfte att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna och att utveckla förtroende och tillit mellan dem.

c) Det inrättar ett nätverk för enheter för hantering av it-säkerhetsincidenter (nedan kallat *CSIRT-nätverket*) i syfte att bidra till utvecklingen av förtroende och tillit mellan medlemsstaterna och främja ett snabbt och effektivt operativt samarbete.

([1]) Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).
([2]) Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).
([3]) Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).
([4]) EUT C 32, 4.2.2014, s. 19.

d) Det fastställer säkerhets- och rapporteringskrav för leverantörer av samhällsviktiga tjänster och för leverantörer av digitala tjänster.

e) Det fastställer skyldigheter för medlemsstaterna att utse nationella behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter med uppgifter som har anknytning till säkerheten i nätverks- och informationssystem.

3. Säkerhets- och rapporteringskraven enligt detta direktiv ska inte tillämpas på företag som omfattas av kraven i artiklarna 13a och 13b i direktiv 2002/21/EG eller på leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 i förordning (EU) nr 910/2014.

4. Detta direktiv påverkar inte tillämpningen av rådets direktiv 2008/114/EG ([1]) eller Europaparlamentets och rådets direktiv 2011/93/EU ([2]) och 2013/40/EU ([3]).

5. Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget får information som är konfidentiell enligt unionsbestämmelser och nationella bestämmelser, såsom bestämmelser om affärshemligheter, utbytas med kommissionen och andra relevanta myndigheter endast när sådant utbyte är nödvändigt för att tillämpa detta direktiv. Den information som utbyts ska begränsas till vad som är relevant och proportionellt för ändamålet med utbytet. Vid sådant utbyte ska informationens konfidentialitet bevaras och säkerhetsintressen och kommersiella intressen hos leverantörer av såväl samhällsviktiga tjänster som digitala tjänster skyddas.

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

7. Om det i en sektorsspecifik unionsrättsakt föreskrivs krav på att leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster antingen ska säkerställa säkerheten i sina nätverks- och informationssystem eller rapportera incidenter, ska bestämmelserna i den sektorsspecifika unionsrättsakten tillämpas, förutsatt att verkan av kraven i fråga minst motsvarar verkan av skyldigheterna i detta direktiv.

Artikel 2

Behandling av personuppgifter

1. Behandling av personuppgifter enligt detta direktiv ska ske i enlighet med direktiv 95/46/EG.

2. Behandling av personuppgifter som utförs av unionens institutioner och organ enligt detta direktiv ska ske i enlighet med förordning (EG) nr 45/2001.

Artikel 3

Minimiharmonisering

Utan att det påverkar tillämpningen av artikel 16.10 eller medlemsstaternas skyldigheter enligt unionsrätten får medlemsstaterna anta eller behålla bestämmelser som syftar till att uppnå en högre nivå på säkerheten i nätverks- och informationssystem.

([1]) Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (EUT L 345, 23.12.2008, s. 75).

([2]) Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF (EUT L 335, 17.12.2011, s. 1).

([3]) Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF (EUT L 218, 14.8.2013, s. 8).

Artikel 4

Definitioner

I detta direktiv avses med

1. *nätverks- och informationssystem*:

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

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

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

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

3. *nationell strategi för säkerheten i nätverks- och informationssystem*: en ram med strategiska mål och prioriteringar för säkerhet i nätverks- och informationssystem på nationell nivå,

4. *leverantör av samhällsviktiga tjänster*: en offentlig eller privat enhet av en typ som avses i bilaga II vilken uppfyller kriterierna i artikel 5.2,

5. *digital tjänst*: en tjänst i den mening som avses i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ([1]) av en typ som anges i bilaga III,

6. *leverantör av digitala tjänster*: en juridisk person som tillhandahåller en digital tjänst,

7. *incident*: en händelse med en faktisk negativ inverkan på säkerheten i nätverks- och informationssystem,

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

9. *risk*: en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i nätverks- och informationssystem,

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

11. *standard*: en standard i den mening som avses i artikel 2.1 i förordning (EU) nr 1025/2012,

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

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

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

([1]) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

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

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

17. *internetbaserad marknadsplats*: en digital tjänst som gör det möjligt för konsumenter och/eller näringsidkare enligt definitionen i artikel 4.1 a respektive 4.1 b i Europaparlamentets och rådets direktiv 2013/11/EU ([1]) att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare antingen på webbplatsen för den internetbaserade marknadsplatsen eller på en webbplats tillhörande en näringsidkare där datatjänster som tillhandahålls av en internetbaserad marknadsplats används,

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

19. *molntjänster*: en digital tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser.

Artikel 5

Identifiering av leverantörer av samhällsviktiga tjänster

1. Senast den 9 november 2018 ska medlemsstaterna, för varje sektor och delsektor som avses i bilaga II, identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium.

2. Kriterierna för identifiering av leverantörer av samhällsviktiga tjänster enligt artikel 4.4 ska vara följande:

a) En enhet tillhandahåller en tjänst som är viktig för att upprätthålla kritisk samhällelig och/eller ekonomisk verksamhet,

b) tillhandahållandet av denna tjänst är beroende av nätverks- och informationssystem, och

c) en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

3. Med avseende på tillämpningen av punkt 1 ska varje medlemsstat upprätta en förteckning över de tjänster som avses i punkt 2 a.

4. Med avseende på tillämpningen av punkt 1 gäller att om en enhet tillhandahåller en tjänst som avses i punkt 2 a i två eller flera medlemsstater, ska dessa medlemsstater samråda med varandra. Detta samråd ska äga rum innan ett beslut om identifiering fattas.

5. Medlemsstaterna ska regelbundet och minst vartannat år efter den 9 maj 2018 se över och vid behov uppdatera förteckningen över identifierade leverantörer av samhällsviktiga tjänster.

6. Samarbetsgruppens roll ska, i överensstämmelse med de uppgifter som anges i artikel 11, vara att hjälpa medlemsstaterna att tillämpa ett enhetligt tillvägagångssätt i förfarandet för identifiering av leverantörer av samhällsviktiga tjänster.

7. Med avseende på den översyn som avses i artikel 23 ska medlemsstaterna, senast den 9 november 2018 och därefter vartannat år, tillhandahålla kommissionen den information som är nödvändig för att kommissionen ska kunna bedöma genomförandet av detta direktiv, särskilt enhetligheten i medlemsstaternas tillvägagångssätt för identifiering av leverantörer av samhällsviktiga tjänster. Denna information ska omfatta åtminstone

a) nationella åtgärder som gör det möjligt att identifiera leverantörer av samhällsviktiga tjänster,

([1]) Europaparlamentets och rådets direktiv 2013/11/EU av den 21 maj 2013 om alternativ tvistlösning vid konsumenttvister och om ändring av förordning (EG) nr 2006/2004 och direktiv 2009/22/EG (direktivet om alternativ tvistlösning) (EUT L 165, 18.6.2013, s. 63).

b) den förteckning över tjänster som avses i punkt 3,

c) det antal leverantörer av samhällsviktiga tjänster som har identifierats för varje sektor som avses i bilaga II samt en uppgift om deras betydelse för den sektorn,

d) tröskelvärden, om sådana finns, för att fastställa den relevanta leveransnivån med hänvisning till det antal användare som är beroende av tjänsten i enlighet med artikel 6.1 a eller till betydelsen av den specifika leverantören av samhällsviktiga tjänster i enlighet med artikel 6.1 f.

I syfte att bidra till tillhandahållandet av jämförbar information får kommissionen, med största hänsyn till yttrandet från Enisa, anta lämpliga tekniska riktlinjer om parametrar för den information som avses i denna punkt.

Artikel 6

Betydande störning

1. När medlemsstaterna fastställer om en störning är betydande enligt artikel 5.2 c, ska de beakta åtminstone följande sektorsöverskridande faktorer:

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

b) Hur beroende andra sektorer enligt bilaga II är av den tjänst som enheten tillhandahåller.

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

d) Enhetens marknadsandel.

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

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

2. För att fastställa huruvida en incident skulle medföra en betydande störning ska medlemsstaterna även, i lämpliga fall, beakta sektorsspecifika faktorer.

KAPITEL II

NATIONELLA RAMAR FÖR SÄKERHETEN I NÄTVERKS- OCH INFORMATIONSSYSTEM

Artikel 7

Nationell strategi för säkerhet i nätverks- och informationssystem

1. Varje medlemsstat ska anta en nationell strategi för säkerhet i nätverks- och informationssystem som fastställer strategiska mål och lämpliga politiska åtgärder och lagstiftningsåtgärder för att uppnå och bibehålla en hög nivå på säkerheten i nätverks- och informationssystem och som täcker åtminstone de sektorer som avses i bilaga II och de tjänster som avses i bilaga III. Den nationella strategin för säkerhet i nätverks- och informationssystem ska i synnerhet omfatta följande:

a) Målen och prioriteringarna i den nationella strategin för säkerhet i nätverks- och informationssystem.

b) En styrningsram för att uppnå målen och prioriteringarna i den nationella strategin för säkerhet i nätverks- och informationssystem, inklusive offentliga organs och andra berörda aktörers roller och ansvarsområden.

c) Identifiering av beredskaps-, svars- och återhämtningsåtgärder, inklusive samarbete mellan offentlig och privat sektor.

d) Uppgift om program för utbildning och åtgärder för ökad medvetenhet rörande den nationella strategin för säkerhet i nätverks- och informationssystem.

e) Uppgift om forsknings- och utvecklingsplaner rörande den nationella strategin för säkerhet i nätverks- och informationssystem.

f) En riskbedömningsplan för identifiering av risker.

g) En förteckning över de olika aktörer som deltar i genomförandet av den nationella strategin för säkerhet i nätverks- och informationssystem.

2. Medlemsstaterna får begära Enisas bistånd vid utarbetandet av nationella strategier för säkerhet i nätverks- och informationssystem.

3. Medlemsstaterna ska underrätta kommissionen om sina nationella strategier för säkerhet i nätverks- och informationssystem inom tre månader från deras antagande. Härvid får medlemstaterna utesluta delar av strategin som rör nationell säkerhet.

Artikel 8

Nationella behöriga myndigheter och gemensam kontaktpunkt

1. Varje medlemsstat ska utse en eller flera nationella behöriga myndigheter för säkerhet i nätverks- och informationssystem (nedan kallad *den behöriga myndigheten*), åtminstone för de sektorer som avses i bilaga II och de tjänster som avses i bilaga III. Medlemsstaterna får tilldela en eller flera befintliga myndigheter denna roll.

2. De behöriga myndigheterna ska övervaka tillämpningen av detta direktiv på nationell nivå.

3. Varje medlemsstat ska utse en gemensam nationell kontaktpunkt för säkerhet i nätverks- och informationssystem (nedan kallad *den gemensamma kontaktpunkten*). Medlemsstaterna får tilldela en befintlig myndighet denna roll. Om en medlemsstat bara utser en behörig myndighet, ska denna behöriga myndighet också vara den gemensamma kontaktpunkten.

4. Den gemensamma kontaktpunkten ska utöva en sambandsfunktion för att säkerställa gränsöverskridande samarbete mellan medlemsstaternas myndigheter och med de berörda myndigheterna i andra medlemsstater samt med den samarbetsgrupp som avses i artikel 11 och det CSIRT-nätverk som avses i artikel 12.

5. Medlemsstaterna ska säkerställa att de behöriga myndigheterna och de gemensamma kontaktpunkterna har tillräckliga resurser för att på ett effektivt sätt kunna utföra de uppgifter de tilldelas och därigenom uppnå målen med detta direktiv. Medlemsstaterna ska säkerställa att de utsedda företrädarna samarbetar på ett effektivt och säkert sätt i samarbetsgruppen.

6. De behöriga myndigheterna och den gemensamma kontaktpunkten ska, när så är lämpligt och i överensstämmelse med nationell rätt, samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna och de nationella dataskyddsmyndigheterna.

7. Varje medlemsstat ska utan dröjsmål underrätta kommissionen om utnämningen av den behöriga myndigheten och den gemensamma kontaktpunkten och deras uppgifter samt alla senare ändringar. Varje medlemsstat ska offentliggöra utnämningen av den behöriga myndigheten och den gemensamma kontaktpunkten. Kommissionen ska offentliggöra förteckningen över utsedda gemensamma kontaktpunkter.

Artikel 9

Enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter)

1. Varje medlemsstat ska utse en eller flera CSIRT-enheter som ska uppfylla kraven i punkt 1 i bilaga I, som täcker åtminstone de sektorer som avses i bilaga II och de tjänster som avses i bilaga III och som ansvarar för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande. En CSIRT-enhet får inrättas inom en behörig myndighet.

2. Medlemsstaterna ska säkerställa att CSIRT-enheterna har de resurser som de behöver för att effektivt utföra sina uppgifter enligt punkt 2 i bilaga I.

Medlemsstaterna ska säkerställa att deras CSIRT-enheter samarbetar på ett ändamålsenligt, effektivt och säkert sätt i det CSIRT-nätverk som avses i artikel 12.

3. Medlemsstaterna ska säkerställa att deras CSIRT-enheter har tillgång till lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur på nationell nivå.

4. Medlemsstaterna ska underrätta kommissionen om sina CSIRT-enheters uppgifter samt om huvudinslagen i deras incidenthanteringsförfarande.

5. Medlemsstaterna får begära Enisas bistånd vid inrättandet av nationella CSIRT-enheter.

Artikel 10

Samarbete på nationell nivå

1. Om den behöriga myndigheten, den gemensamma kontaktpunkten och CSIRT-enheten i en och samma medlemsstat är separata, ska de samarbeta när det gäller fullgörandet av skyldigheterna enligt detta direktiv.

2. Medlemsstaterna ska säkerställa att antingen de behöriga myndigheterna eller CSIRT-enheterna mottar incidentrapporter som lämnas in i enlighet med detta direktiv. Om en medlemsstat beslutar att CSIRT-enheterna inte ska motta rapporter ska CSIRT-enheterna, i den mån det är nödvändigt för att de ska kunna utföra sina uppgifter, beviljas tillgång till uppgifter om incidenter som rapporterats av leverantörer av samhällsviktiga tjänster enligt artikel 14.3 och 14.5, eller av leverantörer av digitala tjänster enligt artikel 16.3 och 16.6.

3. Medlemsstaterna ska säkerställa att de behöriga myndigheterna eller CSIRT-enheterna informerar de gemensamma kontaktpunkterna om incidentrapporter som lämnats in i enlighet med detta direktiv.

Den gemensamma kontaktpunkten ska senast den 9 augusti 2018, och därefter en gång om året, lämna en sammanfattande rapport till samarbetsgruppen om de rapporter som mottagits, inklusive antalet rapporter och de rapporterade incidenternas art, samt om vilka åtgärder som vidtagits i enlighet med artiklarna 14.3, 14.5, 16.3 och 16.6.

KAPITEL III

SAMARBETE

Artikel 11

Samarbetsgrupp

1. För att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna och skapa förtroende och tillit, och i syfte att uppnå en hög gemensam nivå på säkerheten i nätverks- och informationssystem i unionen, inrättas härmed en samarbetsgrupp.

Samarbetsgruppen ska utföra sina uppgifter på grundval av tvååriga arbetsprogram enligt punkt 3 andra stycket.

2. Samarbetsgruppen ska bestå av företrädare för medlemsstaterna, kommissionen och Enisa.

När så är lämpligt får samarbetsgruppen bjuda in företrädare för de berörda parterna att delta i arbetet.

Kommissionen ska tillhandahålla sekretariatet.

3. Samordningsgruppen ska ha följande uppgifter:

a) Tillhandahålla strategisk vägledning för verksamheten i det CSIRT-nätverk som inrättas enligt artikel 12.

b) Utbyta bästa praxis om informationsutbyte angående incidentrapportering enligt artiklarna 14.3, 14.5, 16.3 och 16.6.

c) Utbyta bästa praxis mellan medlemsstaterna och, i samarbete med Enisa, bistå medlemsstaterna med kapacitetsuppbyggnad för att säkerställa säkerheten i nätverks- och informationssystem.

d) Diskutera medlemsstaternas förmåga och beredskap samt utvärdera, på frivillig grund, nationella strategier för säkerhet i nätverks- och informationssystem och CSIRT-enheternas effektivitet och identifiera bästa praxis.

e) Utbyta information och bästa praxis vad gäller åtgärder för ökad medvetenhet och utbildning.

f) Utbyta information och bästa praxis om forskning och utveckling vad gäller säkerhet i nätverks- och informationssystem.

g) Vid behov utbyta erfarenheter om frågor som rör säkerhet i nätverks- och informationssystem med unionens berörda institutioner, organ och byråer.

h) Diskutera de standarder och specifikationer som avses i artikel 19 med företrädare för de relevanta europeiska standardiseringsorganen.

i) Samla in information om bästa praxis vad gäller risker och incidenter.

j) Årligen studera de sammanfattande rapporter som avses i artikel 10.3 andra stycket.

k) Diskutera arbetet med övningar som avser säkerhet i nätverks- och informationssystem och utbildning, inklusive det arbete som utförs av Enisa.

l) Med Enisas bistånd utbyta bästa praxis för medlemsstaternas identifiering av leverantörer av samhällsviktiga tjänster, inklusive i samband med beroende, vad gäller risker och incidenter, som sträcker sig över gränser.

m) Diskutera metoder för rapportering av incidentrapporter enligt artiklarna 14 och 16.

Samarbetsgruppen ska, senast den 9 februari 2018 och därefter vartannat år, utarbeta ett arbetsprogram med åtgärder som ska vidtas för att genomföra dess mål och uppgifter, som ska överensstämma med målen för detta direktiv.

4. Med avseende på den översyn som avses i artikel 23 ska samarbetsgruppen, senast den 9 augusti 2018 och därefter med 1,5 års mellanrum, utarbeta en rapport med en bedömning av erfarenheterna av det strategiska samarbetet enligt den här artikeln.

5. Kommissionen ska anta genomförandeakter i vilka fastställs de förfaranden som krävs för samarbetsgruppens verksamhet. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 22.2.

Vid tillämpningen av första stycket ska kommissionen senast den 9 februari 2017 förelägga den kommitté som avses i artikel 22.1 det första utkastet till genomförandeakt.

Artikel 12

CSIRT-nätverk

1. För att bidra till utvecklingen av förtroende och tillit mellan medlemsstaterna och för att främja snabbt och effektivt operativt samarbete inrättas härmed ett nätverk för nationella CSIRT-enheter.

2. CSIRT-nätverket ska bestå av företrädare för medlemsstaternas CSIRT-enheter och Cert-EU. Kommissionen ska delta i CSIRT-nätverket som observatör. Enisa ska tillhandahålla sekretariatet och aktivt stödja samarbetet mellan CSIRT-enheterna.

3. CSIRT-nätverket ska ha följande uppgifter:

a) Utbyta information om CSIRT-enheternas tjänster, verksamhet och samarbetskapacitet.

b) På begäran av en företrädare för en CSIRT-enhet från en medlemsstat som kan komma att påverkas av en incident, utbyta och diskutera ej kommersiellt känsliga uppgifter rörande incidenten och dithörande risker; en CSIRT-enhet från en medlemsstat kan dock neka att bidra till diskussionen om det finns en risk för att det skulle skada utredningen av incidenten.

c) På frivillig grund utbyta och tillgängliggöra icke-konfidentiella uppgifter om enskilda incidenter.

d) På begäran av en företrädare för en medlemsstats CSIRT-enhet, diskutera och om möjligt utarbeta en samordnad åtgärd till följd av en incident som har upptäckts inom den medlemsstatens jurisdiktion.

e) Stödja medlemsstaterna i hanteringen av gränsöverskridande incidenter på grundval av deras frivilliga ömsesidiga bistånd.

f) Diskutera, utforska och identifiera ytterligare former av operativt samarbete, inklusive med avseende på

   i) kategorier av risker och incidenter,

   ii) tidiga varningar,

   iii) ömsesidigt bistånd,

   iv) principer och metoder för samordning, när medlemsstaterna vidtar åtgärder mot gränsöverskridande risker och incidenter.

g) Informera samarbetsgruppen om sin verksamhet och om ytterligare former av operativt samarbete som diskuterats enligt led f samt begära vägledning i sistnämnda avseende.

h) Diskutera lärdomar från övningar som avser säkerhet i nätverks- och informationssystem, inklusive från sådana som organiserats av Enisa.

i) På begäran av en enskild CSIRT-enhet, diskutera den enhetens kapacitet och beredskap.

j) Utfärda riktlinjer för att underlätta konvergens mellan operativ praxis med avseende på tillämpningen av bestämmelserna i denna artikel om operativt samarbete.

4. Med avseende på den översyn som avses i artikel 23 ska CSIRT-nätverket, senast den 9 augusti 2018 och därefter med 1,5 års mellanrum, utarbeta en rapport med en bedömning av erfarenheterna av det operativa samarbetet enligt denna artikel, inklusive slutsatser och rekommendationer. Rapporten ska även föreläggas samarbetsgruppen.

5. CSIRT-nätverket ska fastställa sin arbetsordning.

Artikel 13

Internationellt samarbete

Unionen får i enlighet med artikel 218 i EUF-fördraget ingå internationella avtal med tredjeländer eller internationella organisationer, och därvid tillåta och organisera deras deltagande i vissa av samarbetsgruppens verksamheter. Sådana avtal ska beakta behovet av att säkerställa ändamålsenligt skydd av uppgifter.

KAPITEL IV

SÄKERHET I NÄTVERKS- OCH INFORMATIONSSYSTEM SOM ANVÄNDS AV LEVERANTÖRER AV SAMHÄLLSVIKTIGA TJÄNSTER

Artikel 14

Säkerhetskrav och incidentrapportering

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

2. Medlemsstaterna ska säkerställa att leverantörer av samhällsviktiga tjänster vidtar lämpliga åtgärder för att förebygga och minimera verkningarna av incidenter som påverkar säkerheten i nätverks- och informationssystem som används för att tillhandahålla sådana samhällsviktiga tjänster, i syfte att säkerställa kontinuiteten i dessa tjänster.

3. Medlemsstaterna ska säkerställa att leverantörer av samhällsviktiga tjänster utan onödigt dröjsmål till den behöriga myndigheten eller CSIRT-enheten rapporterar incidenter som har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänster som de tillhandahåller. Rapporterna ska innehålla information som gör det möjligt för den behöriga myndigheten eller CSIRT-enheten att fastställa incidentens eventuella gränsöverskridande verkningar. Rapportering ska inte medföra ökat ansvar för den rapporterande parten.

4. För att avgöra om en incident har en betydande inverkan ska hänsyn framför allt tas till följande faktorer:

a) Det antal användare som påverkas av störningen av den samhällsviktiga tjänsten.

b) Hur länge incidenten varar.

c) Hur stort geografiskt område som påverkas av incidenten.

5. Mot bakgrund av informationen i rapporten från leverantören av den samhällsviktiga tjänsten ska den behöriga myndigheten eller CSIRT-enheten informera den eller de andra berörda medlemsstaterna, om incidenten har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i den medlemsstaten. Därvid ska den behöriga myndigheten eller CSIRT-enheten, i enlighet med unionsrätten eller med nationell lagstiftning som är förenlig med unionsrätten, bevara nämnda leverantörs säkerhetsintressen och kommersiella intressen samt konfidentialiteten hos informationen i leverantörens rapport.

När omständigheterna tillåter ska den behöriga myndigheten eller CSIRT-enheten förse den rapporterande leverantören av samhällsviktiga tjänster med relevant information om uppföljningen av rapporten, såsom information som skulle kunna bidra till effektiv hantering av incidenten.

På begäran av den behöriga myndigheten eller CSIRT-enheten ska den gemensamma kontaktpunkten vidarebefordra rapporter enligt första stycket till gemensamma kontaktpunkter i andra medlemsstater som påverkats av incidenten.

6. Efter samråd med den rapporterande leverantören av samhällsviktiga tjänster får den behöriga myndigheten eller CSIRT-enheten informera allmänheten om enskilda incidenter, om allmänheten behöver känna till dem för att det ska vara möjligt att förhindra en incident eller åtgärda en pågående incident.

7. Behöriga myndigheter som agerar tillsammans inom samarbetsgruppen får utarbeta och anta riktlinjer för under vilka omständigheter leverantörer av samhällsviktiga tjänster är skyldiga att rapportera incidenter, inklusive riktlinjer om vilka faktorer som ska användas för att fastställa om en incident har betydande inverkan enligt punkt 4.

Artikel 15

Genomförande och efterlevnad

1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har de befogenheter och medel de behöver för att bedöma huruvida leverantörer av samhällsviktiga tjänster uppfyller sina skyldigheter enligt artikel 14 och effekterna därav på säkerheten i nätverks- och informationssystem.

2. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har de befogenheter och medel som krävs för att ålägga leverantörer av samhällsviktiga tjänster att tillhandahålla

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

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

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

3. Efter att ha bedömt information eller resultat av säkerhetsrevisioner enligt punkt 2, får den behöriga myndigheten utfärda bindande anvisningar till leverantörerna av samhällsviktiga tjänster om hur de ska avhjälpa de identifierade bristerna.

4. Den behöriga myndigheten ska ha ett nära samarbete med dataskyddsmyndigheter när den åtgärdar incidenter som medför personuppgiftsincidenter.

KAPITEL V

SÄKERHET I NÄTVERKS- OCH INFORMATIONSSYSTEM SOM ANVÄNDS AV LEVERANTÖRER AV DIGITALA TJÄNSTER

Artikel 16

Säkerhetskrav och incidentrapportering

1. Medlemsstaterna ska säkerställa att leverantörer av digitala tjänster utarbetar och vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder när de tillhandahåller sådana tjänster som avses i bilaga III inom unionen. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken, varvid hänsyn ska tas till

a) säkerheten i system och anläggningar,

b) incidenthantering,

c) hantering av driftskontinuitet,

d) övervakning, revision och testning,

e) efterlevnad av internationella standarder.

2. Medlemsstaterna ska säkerställa att leverantörer av digitala tjänster vidtar åtgärder för att förebygga och minimera den inverkan som incidenter som påverkar säkerheten i deras nätverks- och informationssystem har på de tjänster som avses i bilaga III och som erbjuds inom unionen, i syfte att säkerställa kontinuiteten i dessa tjänster.

3. Medlemsstaterna ska säkerställa att leverantörer av digitala tjänster utan onödigt dröjsmål till den behöriga myndigheten eller CSIRT-enheten rapporterar alla incidenter som har en avsevärd inverkan på tillhandahållandet av en tjänst som avses i bilaga III och som de erbjuder inom unionen. Rapporterna ska innehålla information som gör det möjligt för den behöriga myndigheten eller CSIRT-enheten att fastställa vilken betydelse eventuell gränsöverskridande inverkan har. Rapportering ska inte medföra ökat ansvar för den rapporterande parten.

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

a) Det antal användare som påverkas av incidenten, framför allt användare som är beroende av tjänsten för att kunna tillhandahålla sina egna tjänster.

b) Hur länge incidenten varar.

c) Hur stort geografiskt område som påverkas av incidenten.

d) I vilken utsträckning incidenten stör tjänstens funktion.

e) I vilken utsträckning incidenten inverkar på den ekonomiska och samhälleliga verksamheten.

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

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

6. Om så är lämpligt, och särskilt om den incident som avses i punkt 3 berör två eller flera medlemsstater, ska den behöriga myndigheten eller CSIRT-enheten informera andra medlemsstater som påverkats. Därvid ska de behöriga myndigheterna, CSIRT-enheter och gemensamma kontaktpunkter, i enlighet med unionsrätten eller nationell lagstiftning som är förenlig med unionsrätten, bevara leverantören av digitala tjänsters säkerhetsintressen och kommersiella intressen samt den tillhandahållna informationens konfidentialitet.

7. Efter samråd med den berörda leverantören av digitala tjänster får den behöriga myndigheten eller CSIRT-enheten och, om så är lämpligt, myndigheterna eller CSIRT-enheterna i andra berörda medlemsstater, informera allmänheten om enskilda incidenter eller kräva att leverantören av digitala tjänster gör det, om allmänheten behöver känna till dem för att det ska vara möjligt att förhindra en incident eller åtgärda en pågående incident eller om incidentens avslöjande på annat sätt omfattas av allmänintresset.

8. Kommissionen ska anta genomförandeakter för att ytterligare specificera de element som avses i punkt 1 och de faktorer som anges i punkt 4 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 22.2 senast den 9 augusti 2017.

9. Kommissionen får anta genomförandeakter som fastställer format och förfaranden tillämpliga på rapporteringskrav. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 22.2.

10. Utan att det påverkar tillämpningen av artikel 1.6 får medlemsstaterna inte införa ytterligare säkerhets- eller rapporteringskrav för leverantörer av digitala tjänster.

11. Kapitel V ska inte tillämpas på mikroföretag och små företag enligt definitionen i kommissionens rekommendation 2003/361/EG ([1]).

([1]) Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

Artikel 17

Genomförande och efterlevnad

1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna vid behov vidtar åtgärder genom tillsynsåtgärder i efterhand, när de har mottagit bevis på att en leverantör av digitala tjänster inte uppfyller kraven i artikel 16. Sådana bevis får läggas fram av en behörig myndighet i en annan medlemsstat där tjänsten tillhandahålls.

2. Vid tillämpning av punkt 1 ska de behöriga myndigheterna ha de befogenheter och medel som krävs för att ålägga leverantörer av digitala tjänster att

a) tillhandahålla den information som behövs för en bedömning av säkerheten i deras nätverks- och informationssystem, inbegripet dokumenterade säkerhetsprinciper, och

b) åtgärda varje underlåtenhet att uppfylla kraven i artikel 16.

3. Om en leverantör av digitala tjänster har sitt huvudsakliga etableringsställe eller en företrädare i en medlemsstat, men dess nätverks- och informationssystem är belägna i en eller flera andra medlemsstater, ska den behöriga myndigheten i den medlemsstat där det huvudsakliga etableringsstället eller företrädaren finns och de behöriga myndigheterna i dessa andra medlemsstater samarbeta och vid behov bistå varandra. Detta bistånd och samarbete får omfatta informationsutbyte mellan de berörda behöriga myndigheterna och begäranden om att de tillsynsåtgärder som avses i punkt 2 ska vidtas.

Artikel 18

Jurisdiktion och territorialitet

1. Vid tillämpningen av detta direktiv ska en leverantör av digitala tjänster anses omfattas av jurisdiktionen i den medlemsstat där leverantören har sitt huvudsakliga etableringsställe. En leverantör av digitala tjänster ska anses ha sitt huvudsakliga etableringsställe i en medlemsstat om den har sitt huvudkontor i denna medlemsstat.

2. En leverantör av digitala tjänster som inte är etablerad i unionen men som erbjuder sådana tjänster som avses i bilaga III inom unionen ska utse en företrädare i unionen. Företrädaren ska vara etablerad i en av de medlemsstater där tjänsterna erbjuds. Leverantören av digitala tjänster ska anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad.

3. Att leverantören av digitala tjänster utser en företrädare ska inte påverka eventuella rättsliga åtgärder mot leverantören av digitala tjänster själv.

KAPITEL VI

STANDARDISERING OCH FRIVILLIG RAPPORTERING

Artikel 19

Standardisering

1. För att främja en enhetlig tillämpning av artiklarna 14.1, 14.2, 16.1 och 16.2 ska medlemsstaterna, utan att föreskriva eller gynna användning av en viss typ av teknik, uppmuntra användningen av europeiska eller internationellt accepterade standarder och specifikationer av relevans för säkerheten i nätverks- och informationssystem.

2. Enisa ska i samarbete med medlemsstaterna utarbeta råd och riktlinjer för de tekniska områden som ska beaktas när det gäller punkt 1 samt för redan befintliga standarder, inklusive medlemsstaternas nationella standarder, som skulle kunna täcka dessa områden.

Artikel 20

Frivillig rapportering

1. Utan att det påverkar tillämpningen av artikel 3 får enheter som inte har identifierats som leverantörer av samhällsviktiga tjänster och som inte är leverantörer av digitala tjänster, på frivillig grund, rapportera incidenter som har en betydande inverkan på kontinuiteten i de tjänster som de tillhandahåller.

2. Vid behandlingen av rapporter ska medlemsstaterna agera i enlighet med det förfarande som fastställs i artikel 14. Medlemsstaterna får ge behandling av obligatoriska rapporter företräde framför behandling av frivilliga rapporter. Frivilliga rapporter ska endast behandlas om behandlingen inte utgör en oproportionell eller orimlig börda för de berörda medlemsstaterna.

En frivillig rapport får inte leda till att den rapporterande enheten åläggs skyldigheter som den inte skulle ha varit föremål för om den inte hade gett in rapporten.

KAPITEL VII

SLUTBESTÄMMELSER

Artikel 21

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella bestämmelser som har antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast den 9 maj 2018 samt utan dröjsmål eventuella ändringar som berör dem.

Artikel 22

Kommittéförfarande

1. Kommissionen ska biträdas av kommittén för säkerhet i nätverks- och informationssystem. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Artikel 23

Översyn

1. Kommissionen ska senast den 9 maj 2019 lämna en rapport till Europaparlamentet och rådet, där den bedömer enhetligheten i medlemsstaternas tillvägagångssätt vid identifieringen av leverantörer av samhällsviktiga tjänster.

2. Kommissionen ska regelbundet se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet. I detta syfte och för att ytterligare främja det strategiska och operativa samarbetet ska kommissionen beakta rapporterna från samarbetsgruppen och CSIRT-nätverket om de erfarenheter som förvärvats på strategisk och operativ nivå. I sin översyn ska kommissionen också bedöma förteckningarna i bilagorna II och III samt enhetligheten i identifieringen av leverantörer av samhällsviktiga tjänster och tjänster i de sektorer som avses i bilaga II. Den första rapporten ska lämnas senast den 9 maj 2021.

Artikel 24

Övergångsbestämmelser

1. Utan att det påverkar tillämpningen av artikel 25 och i syfte att erbjuda medlemsstaterna ytterligare möjligheter till lämpligt samarbete under införlivandeperioden, ska samarbetsgruppen och CSIRT-nätverket börja utföra sina uppgifter enligt artikel 11.3 respektive 12.3 senast den 9 februari 2017.

2. Under perioden från och med den 9 februari 2017 till och med den 9 november 2018 ska samarbetsgruppen, i syfte att hjälpa medlemsstaterna att tillämpa ett enhetligt tillvägagångssätt i förfarandet för identifiering av leverantörer av samhällsviktiga tjänster, diskutera förfarandet för, innehållet i och typen av nationella åtgärder som möjliggör identifiering av leverantörer av samhällsviktiga tjänster inom en särskild sektor i enlighet med de kriterier som anges i artiklarna 5 och 6. Samarbetsgruppen ska på begäran av en medlemsstat också diskutera medlemsstatens utkast till specifika nationella åtgärder som möjliggör identifiering av leverantörer av samhällsviktiga tjänster inom en särskild sektor i enlighet med de kriterier som anges i artiklarna 5 och 6.

3. Senast den 9 februari 2017 ska medlemsstaterna vid tillämpning av denna artikel säkerställa att de är korrekt företrädda i samarbetsgruppen och CSIRT-nätverket.

Artikel 25

Införlivande

1. Medlemsstaterna ska senast den 9 maj 2018 anta och offentliggöra de bestämmelser i lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta.

De ska tillämpa dessa bestämmelser från och med den 10 maj 2018.

När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Medlemsstaterna ska till kommissionen överlämna texten till de centrala bestämmelser i nationell rätt som de antar inom det område som omfattas av detta direktiv.

Artikel 26

Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 27

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Strasbourg den 6 juli 2016.

På Europaparlaments vägnar	*På rådets vägnar*
M. SCHULZ	I. KORČOK
Ordförande	*Ordförande*

BILAGA I

KRAV PÅ ENHETER FÖR HANTERING AV IT-SÄKERHETSINCIDENTER (*COMPUTER SECURITY INCIDENT RESPONSE TEAMS*, NEDAN KALLADE *CSIRT-ENHETER*) SAMT DERAS UPPGIFTER

Kraven på CSIRT-enheter samt deras uppgifter ska på ett lämpligt och entydigt sätt fastställas och stödjas genom nationell politik och/eller lagstiftning. Följande ska ingå:

1. Krav på CSIRT-enheter

   a) CSIRT-enheterna ska säkerställa en hög nivå på tillgången till sina kommunikationstjänster genom att undvika felkritiska systemdelar (*single points of failure*) och ska kunna kontaktas och kontakta andra när som helst och på flera olika sätt. Kommunikationskanalerna ska dessutom vara tydligt specificerade och välkända för användargruppen och samarbetspartner.

   b) CSIRT-enheternas lokaler och de informationssystem som de använder sig av ska vara belägna på säker plats.

   c) Driftskontinuitet:

      i) CSIRT-enheter ska ha ett ändamålsenligt system för handläggning och dirigering av ansökningar, så att överlämnanden underlättas.

      ii) CSIRT-enheter ska ha tillräckligt med personal för att ständigt vara tillgängliga.

      iii) CSIRT-enheter ska förlita sig på en infrastruktur med säkerställd kontinuitet. Därför måste systemen ha inbyggd redundans och reservlokaler finnas tillgängliga.

   d) CSIRT-enheter ska om de så önskar ha möjlighet att delta i internationella samarbetsnätverk.

2. CSIRT-enheters uppgifter

   a) CSIRT-enheters uppgifter ska omfatta minst följande:

      i) Övervakning av incidenter på nationell nivå.

      ii) Tillhandahållande av tidiga varningar, larm, meddelanden och informationsspridning till relevanta aktörer om risker och incidenter.

      iii) Åtgärder till följd av incidenter.

      iv) Tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet.

      v) Deltagande i CSIRT-nätverket.

   b) CSIRT-enheter ska bygga upp samarbetsrelationer med den privata sektorn.

   c) För att underlätta samarbete ska CSIRT-enheter främja antagandet och användningen av gemensam eller standardiserad praxis för

      i) förfaranden för hantering av incidenter och risker,

      ii) klassificeringssystem för incidenter, risker och information.

BILAGA II

TYPER AV ENHETER ENLIGT ARTIKEL 4.4

Sektor	Delsektor	Typ av enhet
1. Energi	a) Elektricitet	— Elföretag enligt definitionen i artikel 2.35 i Europaparlamentets och rådets direktiv 2009/72/EG ([1]) som bedriver ”leverans eller handel” enligt definitionen i artikel 2.19 i det direktivet
		— Systemansvariga för distributionssystemet enligt definitionen i artikel 2.6 i direktiv 2009/72/EG
		— Systemansvariga för överföringssystemet enligt definitionen i artikel 2.4 i direktiv 2009/72/EG
	b) Olja	— Operatörer av oljeledningar
		— Operatörer av oljeproduktion, raffinaderier, bearbetningsanläggningar, lagring och överföring
	c) Gas	— Gashandelsföretag eller gashandlare enligt definitionen i artikel 2.8 i Europaparlamentets och rådets direktiv 2009/73/EG ([2])
		— Systemansvariga för distributionssystemet enligt definitionen i artikel 2.6 i direktiv 2009/73/EG
		— Systemansvariga för överföringssystemet enligt definitionen i artikel 2.4 i direktiv 2009/73/EG
		— Systemansvariga för lagringssystemet enligt definitionen i artikel 2.10 i direktiv 2009/73/EG
		— Systemansvariga för en LNG-anläggning enligt definitionen i artikel 2.12 i direktiv 2009/73/EG
		— Naturgasföretag enligt definitionen i artikel 2.1 i direktiv 2009/73/EG
		— Operatörer av raffinaderier och bearbetningsanläggningar för naturgas
2. Transporter	a) Lufttransport	— Lufttrafikföretag enligt definitionen i artikel 3.4 i Europaparlamentets och rådets förordning (EG) nr 300/2008 ([3])
		— Flygplatsens ledningsenheter enligt definitionen i artikel 2.2 i Europaparlamentets och rådets direktiv 2009/12/EG ([4]), flygplatser enligt definitionen i artikel 2.1 i det direktivet, inbegripet de huvudflygplatser som förtecknas i avsnitt 2 i bilaga II till Europaparlamentets och rådets förordning (EU) nr 1315/2013 ([5]), och enheter som driver kringliggande installationer vid flygplatser

Sektor	Delsektor	Typ av enhet
		— Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänst enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 549/2004 ([6])
	b) Järnvägstransport	— Infrastrukturförvaltare enligt definitionen i artikel 3.2 i Europaparlamentets och rådets direktiv 2012/34/EU ([7])
		— Järnvägsföretag enligt definitionen i artikel 3.1 i direktiv 2012/34/EU, inbegripet tjänsteleverantörer enligt definitionen i artikel 3.12 i direktiv 2012/34/EU
	c) Sjöfart	— Transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster, enligt definitionerna för sjötransport i bilaga I till Europaparlamentets och rådets förordning (EG) nr 725/2004 ([8]), exklusive de enskilda fartyg som drivs av dessa företag
		— Ledningsenheter för hamnar enligt definitionen i artikel 3.1 i Europaparlamentets och rådets direktiv 2005/65/EG ([9]), inbegripet deras hamnanläggningar enligt definitionen i artikel 2.11 i förordning (EG) nr 725/2004, och enheter som sköter anläggningar och utrustning i hamnar
		— Operatörer av sjötrafikinformationstjänster enligt definitionen i artikel 3 o i Europaparlamentets och rådets direktiv 2002/59/EG ([10])
	d) Vägtransport	— Vägmyndigheter enligt definitionen i artikel 2.12 i kommissionens delegerade förordning (EU) 2015/962 ([11]) med ansvar för trafikstyrning och trafikledning
		— Operatörer av intelligenta transportsystem enligt definitionen i artikel 4.1 i Europaparlamentets och rådets direktiv 2010/40/EU ([12])
3. Bankverksamhet		Kreditinstitut enligt definitionen i artikel 4.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013 ([13])
4. Finans-marknads-infrastruktur		— Operatörer av handelsplatser enligt definitionen i artikel 4.24 i Europaparlamentets och rådets direktiv 2014/65/EU ([14])
		— Centrala motparter enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 648/2012 ([15])
5. Hälso- och sjukvårdssektorn	Hälso- och sjukvårdsmiljöer (inklusive sjukhus och privata kliniker)	Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU ([16])

Sektor	Delsektor	Typ av enhet
6. Leverans och distribution av dricksvatten		Leverantörer och distributörer av dricksvatten enligt definitionen i artikel 2.1 a i rådets direktiv 98/83/EG ([17]), dock exklusive distributörer för vilka distribution av dricksvatten endast utgör en del av deras allmänna verksamhet, som består i distribution av andra förnödenheter och varor som inte anses utgöra samhällsviktiga tjänster
7. Digital infrastruktur		— Internetknutpunkter
		— Leverantörer av DNS-tjänster
		— Registreringsenheter för toppdomäner

([1]) Europaparlamentets och rådets direktiv 2009/72/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för el och om upphävande av direktiv 2003/54/EG (EUT L 211, 14.8.2009, s. 55).
([2]) Europaparlamentets och rådets direktiv 2009/73/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för naturgas och om upphävande av direktiv 2003/55/EG (EUT L 211, 14.8.2009, s. 94).
([3]) Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).
([4]) Europaparlamentets och rådets direktiv 2009/12/EG av den 11 mars 2009 om flygplatsavgifter (EUT L 70, 14.3.2009, s. 11).
([5]) Europaparlamentets och rådets förordning (EU) nr 1315/2013 av den 11 december 2013 om unionens riktlinjer för utbyggnad av det transeuropeiska transportnätet och om upphävande av beslut nr 661/2010/EU (EUT L 348, 20.12.2013, s. 1).
([6]) Europaparlamentets och rådets förordning (EG) nr 549/2004 av den 10 mars 2004 om ramen för inrättande av det gemensamma europeiska luftrummet ("ramförordning") (EUT L 96, 31.3.2004, s. 1).
([7]) Europaparlamentets och rådets direktiv 2012/34/EU av den 21 november 2012 om inrättande av ett gemensamt europeiskt järnvägsområde (EUT L 343, 14.12.2012, s. 32).
([8]) Europaparlamentets och rådets förordning (EG) nr 725/2004 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar (EUT L 129, 29.4.2004, s. 6).
([9]) Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd (EUT L 310, 25.11.2005, s. 28).
([10]) Europaparlamentets och rådets direktiv 2002/59/EG av den 27 juni 2002 om inrättande av ett övervaknings- och informationssystem för sjötrafik i gemenskapen och om upphävande av rådets direktiv 93/75/EEG (EGT L 208, 5.8.2002, s. 10).
([11]) Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster (EUT L 157, 23.6.2015, s. 21).
([12]) Europaparlamentets och rådets direktiv 2010/40/EU av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag (EUT L 207, 6.8.2010, s. 1).
([13]) Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och värdepappersföretag och om ändring av förordning (EU) nr 648/2012 (EUT L 176, 27.6.2013, s. 1).
([14]) Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).
([15]) Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 201, 27.7.2012, s. 1).
([16]) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).
([17]) Rådets direktiv 98/83/EG av den 3 november 1998 om kvaliteten på dricksvatten (EGT L 330, 5.12.1998, s. 32).

BILAGA III

TYPER AV DIGITALA TJÄNSTER ENLIGT ARTIKEL 4.5

1. Internetbaserad marknadsplats.
2. Internetbaserad sökmotor.
3. Molntjänster.