EUROPEISKA
KOMMISSIONEN

Bryssel den 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen

{SWD(2013) 31 final}
{SWD(2013) 32 final}

MOTIVERING

Syftet med förslaget till direktiv är att säkerställa en hög gemensam nivå av nät- och informationssäkerhet (NIS). Detta innebär att man förbättrar säkerheten för Internet och de privata nät och informationssystem som behövs för att våra samhällen och ekonomier ska fungera. Detta kommer att uppnås genom att medlemsstaterna åläggs att öka sin beredskap och förbättra sitt samarbete med varandra och genom att operatörer av kritisk infrastruktur, inom områden som energi, transport, och viktiga leverantörer av informationssamhällets tjänster (t.ex. e-handelsplattformar och sociala medier), liksom offentliga förvaltningar åläggs att vidta ändamålsenliga åtgärder för att hantera säkerhetsrisker och rapportera allvarliga incidenter till de behöriga nationella myndigheterna.

Förslaget läggs fram i samband med ett gemensamt meddelande om en europeisk strategi för it-säkerhet från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik. Strategins syfte är att garantera en säker och tillförlitlig digital miljö och samtidigt främja och skydda grundläggande rättigheter och andra centrala värderingar för EU. Förslaget är den viktigaste åtgärden inom strategin. Strategin omfattar också åtgärder inriktade på att öka medvetenheten, utveckla en inre marknad för it-säkerhetsprodukter och it-säkerhetstjänster och på att främja investeringar i forskning och utveckling. Dessa åtgärder kommer att kompletteras av andra för att intensifiera kampen mot it-brottslighet och bygga upp en internationell it-säkerhetspolitik för EU.

1.1. Motiv och syfte med förslaget

Nät- och informationssäkerheten blir allt viktigare för vår ekonomi och vårt samhälle. Den är också en förutsättning när man ska skapa en tillförlitlig miljö för världshandeln med tjänster. Informationssystemen kan dock påverkas av säkerhetsincidenter som beror på t.ex. den mänskliga faktorn, naturfenomen, tekniska fel eller it-attacker. Den här typen av incidenter blir allt mer omfattande, vanliga och komplexa. I kommissionen offentliga onlinesamråd om förbättrad nät- och informationssäkerhet i EU[1] angav 57 % av deltagarna att de under det föregående året hade varit med om nät- och säkerhetsincidenten som haft allvarlig inverkan på deras verksamhet. Bristande nät- och informationssäkerhet kan ha negativ inverkan på viktiga tjänster som är beroende av nätens och informationssystemens integritet. Detta kan hindra företag från att fungera, ge upphov till stora finansiella förluster för EU-ekonomin och få negativa konsekvenser för den samhälleliga välfärden.

[1] Det offentliga onlinesamrådet om förbättrad nät- och informationssäkerhet i EU hölls 23 juli – 15 oktober 2012.

De digitala informationssystemen, och i synnerhet internet, är gränslösa kommunikationsinstrument, som är sammankopplade över medlemsstaternas gränser, och de har stor betydelse för att främja den gränsöverskridande rörligheten för varor, tjänster och personer. Allvarliga störningar av dessa system i en medlemsstat kan påverka andra medlemsstater och EU som helhet. Nätens och informationssystemens motståndskraft och stabilitet är därför viktiga för genomförandet av en digital inre marknad och för att den inre marknaden ska fungera smidigt. Sannolikheten för incidenter, frekvensen av incidenter och oförmågan att garantera ett effektivt skydd kan också undergräva allmänhetens förtroende för och tillit till näten och informationstjänsterna. Exempelvis visade 2012 års Eurobarometer om it-säkerhet att 38 % av internetanvändarna i EU oroar sig för säkerheten vid onlinebetalningar och att de ändrat sitt beteende av detta skäl: 18 % är mindre benägna att köpa varor online och 15 % är mindre benägna att utföra bankärenden online[2].

Den nuvarande situationen i EU, som är ett resultat av den helt frivilliga väg som hittills valts, ger inte ett tillräckligt starkt skydd mot nät- och informationssäkerhetsincidenter och -risker i EU. Existerande nät- och informationssäkerhetskapacitet och nät- och informationssäkerhetsmekanismer räcker helt enkelt inte för att hålla jämna steg med den föränderliga hotbilden eller för att säkra en gemensam hög skyddsnivå i alla medlemsstater.

Trots de initiativ som tagits har medlemsstaterna väldigt olika nivåer vad gäller kapacitet och beredskap, vilket leder till fragmentering i EU. I och med att näten och informationssystemen är sammankopplade försvagas den totala nät- och informationssäkerheten i EU av de medlemsstater som har en otillräcklig skyddsnivå. Detta hindrar också uppbyggandet av förtroendet mellan parterna, vilket är en förutsättning för samarbete och informationsutbyte. Därför är det endast en minoritet bestående av medlemsstater med hög nivå på kapaciteten som samarbetar.

I dagsläget finns det alltså inte någon effektiv mekanism på EU-nivå för ett effektivt samarbete, en effektiv samverkan och ett tillförlitligt informationsutbyte om nät- och informationssäkerhetsincidenter och nät- och informationssäkerhetsrisker mellan medlemsstaterna. Detta kan leda till att osamordnade regleringsåtgärder, ej sammanhållna strategier och olika standarder, vilket medför ett bristfälligt skydd mot nät- och informationssäkerhetsincidenter i EU. Hinder kan också uppstå på den inre marknaden, vilket medför kostnader för att följa reglerna för företag som är verksamma i mer än en medlemsstat.

Slutligen är de aktörer som förvaltar kritisk infrastruktur eller tillhandahåller tjänster som är samhällsnödvändiga inte på lämpligt sätt förpliktade att anta riskhanteringsåtgärder eller utbyta information med berörda myndigheter. Därför saknar företagen effektiva incitament för seriös riskhantering, med riskbedömning och ändamålsenliga åtgärder för att garantera nät- och informationssäkerheten. Dessutom når en stor andel av incidenterna inte de behöriga myndigheterna utan går obemärkt förbi. Information om incidenter är emellertid mycket viktig för att myndigheterna ska kunna reagera, vidta lämpliga åtgärder för att begränsa konsekvenserna och fastställa lämpliga strategiska prioriteringar för nät- och informationssäkerhet.

Enligt det nuvarande regelverket är det endast teleföretagen som är skyldiga att vidta riskhanteringsåtgärder och rapportera allvarliga nät- och informationssäkerhetsincidenter. Det finns dock många andra sektorer som använder sig av IKT och även dessa bör engagera sig i nät- och informationssäkerheten. Ett antal specifika infrastrukturoperatörer och tjänsteleverantörer är särskilt sårbara, eftersom de är starkt beroende av korrekt fungerande nät och informationssystem. Dessa sektorer är mycket viktiga för tillhandahållandet av

[2] Eurobarometer 390/2012.

stödtjänster av central betydelse för vår ekonomi och vårt samhälle, och säkerheten för deras system är särskilt viktig för en fungerande inre marknad. Några exempel är banksektorn, börserna, produktion, överföring och distribution av energi, transporter (luftfart, järnväg, sjöfart), hälso- och sjukvård, internettjänster och offentlig förvaltning.

Sättet att hantera nät- och informationssäkerhet i EU måste därför ändras stegvis. Lagstadgade skyldigheter krävs för att ge alla samma konkurrensförutsättningar och fylla luckor i lagstiftningen. För att åtgärda dessa problem och höja nivån på nät- och informationssäkerheten i Europeiska unionen har det föreslagna direktivet följande syften:

För det första ålägger direktivet alla medlemsstater att se till att de har en miniminivå av nationell kapacitet genom att inrätta nationella myndigheter för nät- och informationssäkerhet, inrätta incidenthanteringsorganisationer (cert) och anta nationella strategier för nät- och informationssäkerhet och nationella samarbetsplaner för nät- och informationssäkerhet.

För det andra bör de behöriga nationella myndigheterna samarbeta inom ett nätverk som tillåter säker och effektiv samordning, inbegripet ett samordnat informationsutbyte samt upptäckt och insatser på EU-nivå. Genom detta nätverk bör medlemsstaterna utbyta information och samarbeta för att bekämpa nät- och informationssäkerhetshot och nät- och informationssäkerhetsincidenter på grundval av den europeiska planen för samarbete inom detta område.

För tredje syftar förslaget till att utifrån ramdirektivets modell för elektronisk kommunikation säkerställa att en riskhanteringskultur utvecklas och att information utbyts mellan privat och offentlig sektor. Företag inom de specifika kritiska sektorer som anges ovan och offentliga förvaltningar kommer att åläggas att bedöma de risker som de står inför och vidta ändamålsenliga åtgärder som står i proportion till hoten för att garantera nät- och informationssäkerheten. De kommer att vara skyldiga att underrätta de behöriga myndigheterna om alla incidenter som utgör ett hot mot deras nät och informationssystem och som på ett allvarligt sätt påverkar kontinuiteten för kritiska tjänster och tillhandahållandet av varor.

1.2. Allmän bakgrund

Redan 2001 beskrev kommissionen nät- och informationssäkerhetens betydelse i sitt meddelande *Nät- och informationssäkerhet: förslag till en europeisk strategi*[3] År 2006 följdes meddelandet upp med antagandet av *En strategi för ett säkert informationssamhälle – "Dialog, partnerskap och användarinflytande"*[4], som syftade till att utveckla en nät- och informationssäkerhetskultur i Europa. De viktigaste delarna av strategin stöddes i en rådsresolution[5].

Den 30 mars 2009 antog kommissionen ett meddelande om skydd av kritisk informationsinfrastruktur[6] som fokuserar på att skydda Europa från it-störningar genom att förbättra säkerheten. Meddelandet sjösatte en handlingsplan för att stödja medlemsstaternas insatser för att säkerställa skydd och svarsåtgärder. Handlingsplanen stöddes i ordförandeskapets slutsatser från ministerkonferensen om kritisk infrastruktur som hölls i Tallinn 2009. Den 18 december 2009 antog rådet en resolution om en europeisk samarbetsstrategi för nät- och informationssäkerhet[7].

---

3 KOM(2001) 298.
4 KOM(2006) 251, http://eur-lex.europa.eu/LexUriServ/site/sv/com/2006/com2006_0251sv01.pdf.
5 2007/068/01.
6 KOM(2009) 149.
7 2009/C 321/01.

I den digitala agendan för Europa[8] som antogs i maj 2010 och rådets slutsatser om denna[9] framhävs att det råder samsyn om att säkerhet och förtroende är grundläggande förutsättningar för allmän användning av informations- och kommunikationsteknik och därmed för att nå målen för smart tillväxt enligt strategin EU 2020[10]. I den digitala agendans kapitel om tillit och säkerhet betonas att alla aktörer måste gå samman och göra heltäckande ansträngningar för att garantera IKT-infrastrukturens säkerhet och motståndskraft, genom att fokusera på förebyggande åtgärder, beredskap och medvetenhet samt på att utveckla effektiva och samordnade säkerhetsmekanismer. Nyckelåtgärd 6 i en digital agenda för Europa uppmanar särskilt till åtgärder för en stärkt politik för nät- och informationssäkerhet på hög nivå.

I sitt meddelande från mars 2011 om skydd av kritisk infrastruktur: ”Resultat och kommande åtgärder: vägen mot global it-säkerhet”[11] inventerade kommissionen de resultat som uppnåtts sedan handlingsplanen för skydd av kritisk infrastruktur antogs 2009. Slutsatsen var att genomförandet av handlingsplanen visat att det inte räcker med rent nationella strategier för att hantera problemen med säkerhet och motståndskraft och att Europa bör fortsätta sina ansträngningar för att få till stånd ett sammanhängande tillvägagångssätt baserat på EU-samarbete. I meddelandet om skydd av kritisk infrastruktur från 2011 aviserades ett antal åtgärder och kommissionen uppmanade medlemsstaterna att inrätta nät- och informationssäkerhetskapacitet och gränsöverskridande samarbete. De flesta av dessa åtgärder har fortfarande inte genomförts trots att tidsgränsen var satt till 2012.

I sina slutsatser av den 27 maj 2011 om kritisk infrastruktur betonar Europeiska unionens råd det akuta behovet av att göra IKT-systemen och IKT-näten motståndskraftiga och säkra mot alla typer av störningar, både oavsiktliga och avsiktliga, uppnå en hög nivå av beredskaps-, säkerhets- och motståndskraftskapacitet i hela EU, uppgradera den tekniska kompetensen så att Europa klarar den utmaning som skyddet av nät och informationsinfrastruktur utgör och främja mekanismer för samarbete mellan medlemsstaterna vid incidenter.

1.3. Gällande EU-bestämmelser och internationella bestämmelser på detta område

Genom förordning (EG) nr 460/2004 inrättade Europeiska gemenskapen 2004 Europeiska byrån för nät- och informationssäkerhet (Enisa)[12], för att bidra till utvecklingen av en nät- och informationssäkerhetskultur på hög nivå inom EU. Ett förslag om att modernisera Enisas mandat antogs den 30 september 2010[13] och är nu under behandling i rådet och Europaparlamentet. Det ändrade regelverket för elektronisk kommunikation[14], som är i kraft sedan november 2009 omfattar säkerhetskrav för leverantörer av elektronisk kommunikation[15]. Dessa säkerhetskrav skulle vara införlivade på nationell nivå i maj 2011.

Alla aktörer som är registeransvariga (t.ex. banker och sjukhus) är enligt regelverket för dataskydd[16] skyldiga att vidta säkerhetsåtgärder för att skydda personuppgifter. Enligt kommissionens förslag från 2012 om allmän uppgiftsskyddsförordning[17] skulle registeransvariga behöva rapportera personuppgiftsbrott till de nationella tillsynsmyndigheterna. Detta betyder att t.ex. ett nät- och informationssäkerhetsbrott som

---

8 KOM(2010) 245.

9 Rådets slutsatser av den 31 maj 2010 om en digital agenda för Europa (10130/10).

10 KOM(2010) 2020 och slutsatser från europeiska rådets möte den 25–26 mars 2010 (EUCO 7/10).

11 KOM(2011) 163.

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:SV:HTML.

13 KOM(2010) 521.

14 Se http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Artiklarna 13a och 13b i ramdirektivet.

16 Direktiv 2002/58/EG av den 12 juli 2002.

17 KOM(2012) 11.

påverkar tillhandahållandet av en tjänst utan att äventyra personuppgifter (t.ex. IKT-avbrott hos ett kraftbolag som leder till strömavbrott) skulle behöva anmälas.

I enlighet med rådets direktiv 2008/114/EG om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna är det europeiska programmet för skydd av kritisk infrastruktur (Epcip)[18] som fastställer den övergripande strategin för skydd av kritiska infrastrukturer i EU. Syftet med Epcip är helt i enlighet med detta förslag och direktivet bör gälla utan att det påverkar tillämpningen av direktiv 2008/114. Epcip ålägger inte operatörer att rapportera betydande säkerhetsöverträdelser och omfattar inga mekanismer för medlemsstaternas samarbete och svarsåtgärder vid incidenter.

Medlagstiftarna håller för närvarande på att diskutera kommissionens förslag till direktiv om angrepp mot informationssystem[19], som syftar till att harmonisera kriminaliseringen av specifika typer av beteenden. Det omfattar endast kriminalisering av specifika typer av beteenden och behandlar inte förebyggande av nät- och informationssäkerhetsrisker och incidenter, svarsåtgärder på nät- och informationssäkerhetsincidenter eller åtgärder för att begränsa konsekvenserna. Detta direktiv bör gälla utan att det påverkar tillämpningen av direktivet om angrepp mot informationssystem.

Den 28 mars 2012 antog kommissionen ett meddelande om inrättande av ett Europeiskt centrum mot it-brottslighet[20]. Detta centrum, som inrättades den 11 januari, ingår i Europeiska polisbyrån (Europol) och ska fungera som sambandspunkt för kampen mot it-brottslighet i EU. Centrumet ska föra samman europeisk expertis för att stödja medlemsstaternas kapacitetsuppbyggnad, tillhandahålla stöd till medlemsstaternas utredningar av it-brott och, i nära samarbete med Eurojust, fungera som kollektiv röst för europeiska utredare av it-brottslighet inom brottsbekämpning och rättsväsende.

De europeiska institutionerna, byråerna och organen har inrättat en egen incidenthanteringsorganisation, Cert-EU.

Internationellt arbetar EU med it-säkerhet både bilateralt och multilateralt. Vid toppmötet mellan EU och USA 2010[21] inrättades en gemensam arbetsgrupp för it-säkerhet och it-brottslighet (*EU-US Working Group on Cybersecurity and Cybercrime*). EU är också en aktiv deltagare i andra relevanta multilaterala forum, som Organisationen för ekonomiskt samarbete och utveckling (OECD), Förenta nationernas generalförsamling, Internationella teleunionen (ITU), Organisationen för säkerhet och samarbete i Europa (OSSE), världstoppmötet om informationssamhället (WSIS) och Forumet för förvaltning av internet (IGF).

2. RESULTAT AV SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

2.1. Samråd med berörda parter och utnyttjande av sakkunskap

Ett offentligt onlinesamråd om förbättrad nät- och informationssäkerhet i EU genomfördes 23 juli–15 oktober 2012. Totalt inkom 160 svar på frågeformuläret.

Det viktigaste resultatet var att aktörerna allmänt höll med om att nät- och informationssäkerheten behövde förbättras i EU**:** 82,8 % av de som svarade ansåg att

[18] KOM(2006) 786, http://eur-lex.europa.eu/LexUriServ/site/sv/com/2006/com2006_0786sv01.pdf.

[19] KOM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:SV:PDF.

[20] KOM(2012) 140 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF.

[21] http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

regeringarna i EU borde göra mer för att säkerställa en hög nivå av nät- och informationssäkerhet. 82,8 % ansåg att användarna av information och system inte var medvetna om existerande nät- och informationssäkerhetshot och -incidenter. 66,3 % skulle i princip vara för krav för att hantera nät- och informationssäkerhetsrisker, och 84,8 % sa att sådana krav borde fastställas på EU-nivå. Ett stort antal svarande ansåg att det var särskilt viktigt att anta nät- och informationssäkerhetskrav i följande sektorer: bank- och finansväsende (91,1 %), energi (89,4 %), transport (81,7 %), hälso- och sjukvård (89,4 %), internettjänster (89,1 %) och offentlig förvaltning (87,5 %). De svarande ansåg också att ett eventuellt krav om rapportering av nät- och informationssäkerhetsbrott till den behöriga nationella myndigheten borde fastställas på EU-nivå (65,1 %) och slog fast att detta krav borde gälla även för offentliga förvaltningar (93,5 %). Slutligen bekräftade de svarande att ett eventuellt krav på den modernaste nät- och informationssäkerhetsriskhanteringen inte skulle medföra några betydande merkostnader för dem (63,4 %) och att ett krav på rapportering av säkerhetsöverträdelser inte skulle medföra några betydande merkostnader (72,3 %).Medlemsstaterna rådfrågades i ett antal berörda rådskonstellationer i samband med det europeiska forumet för medlemsstaterna vid den it-säkerhetskonferens som anordnades av kommissionen och Europeiska utrikestjänsten den 6 juli 2012 och vid särskilda bilaterala möten som sammankallats på begäran av enskilda medlemsstater.

Diskussioner med den privata sektorn fördes också inom det offentligprivata EU-partnerskapet för motståndskraft[22] och vid bilaterala möten. När det gäller den offentliga sektorn höll kommissionen diskussioner med Enisa och Cert på EU-institutionernas vägnar.

2.2. Konsekvensbedömning

Kommissionen har gjort en konsekvensbedömning av följande tre alternativ:

Alternativ 1: Ingen förändring (nollalternativ): fortsatt tillämpning av nuvarande tillvägagångssätt

Alternativ 2: Lagstiftning, bestående av ett lagstiftningsförslag som fastställer en gemensam rättslig EU-ram för nät- och informationssäkerhet när det gäller medlemsstaternas kapacitet, mekanismer för EU-samarbete och krav som ska gälla för viktiga privata aktörer och offentliga förvaltningar.

Alternativ 3: En kombination, som innebär att frivilliga initiativ för medlemsstaternas nät- och informationssäkerhetskapacitet kombineras med lagstadgade krav för viktiga privata aktörer och offentliga förvaltningar.

Kommissionen kom fram till att alternativ 2 skulle ha den starkaste positiva effekterna, eftersom det i hög grad skulle förbättra skyddet mot nät- och informationssäkerhetsincidenter för konsumenter, företag och offentliga organ i EU. I synnerhet skulle de skyldighet som läggs på medlemsstaterna säkerställa tillräcklig beredskap på nationell nivå och bidra till ett klimat av ömsesidigt förtroende, vilket är en förutsättning för effektivt samarbete på EU-nivå. Inrättandet av samarbetsmekanismer på EU-nivå via nätverket skulle ge sammanhållna och samordnade förebyggande åtgärder och svarsåtgärder vid gränsöverskridande nät- och informationssäkerhetsincidenter och -risker. Införandet av krav på genomförande av riskhantering avseende nät- och informationssäkerhet för offentliga förvaltningar och centrala privata aktörer skulle ge starka incitament för effektiv hantering av säkerhetsrisker. Skyldigheten att rapportera nät- och informationssäkerhetsincidenter med betydande konsekvenser borde öka förmågan till svarsåtgärder på incidenter och främja öppenhet och insyn. Genom att sopa rent framför egen dörr skulle Europeiska Unionen kunna öka sin

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

internationella räckvidd och bli ännu mer trovärdig som partner för bilateralt och multilateralt samarbete. EU skulle därmed också ha större möjligheter att främja grundläggande rättigheter och EU:s kärnvärderingar i andra länder.

Den kvantitativa analysen visade att alternativ 2 inte skulle vara oproportionerligt betungande för medlemsstaterna. Kostnaderna för den privata sektorn skulle också vara begränsade eftersom många av de berörda enheterna redan borde uppfylla befintliga säkerhetskrav (såsom registeransvarigas skyldighet att vidta tekniska och organisatoriska åtgärder för att göra personuppgifter säkra, inbegripet nät- och informationssäkerhetsåtgärder). Den nuvarande nivån på utgifterna för säkerhet i den privata sektorn har också beaktats.

Förslaget överensstämmer med de principer som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna, i synnerhet rätten till skydd för privatliv och kommunikation, skyddet av personuppgifter, näringsfriheten, äganderätten, rätten till ett effektivt rättsmedel och rätten att höras. Detta direktiv ska tillämpas i enlighet med dessa rättigheter och principer.

3. FÖRSLAGETS RÄTTSLIGA ASPEKTER

3.1. Rättslig grund

Europeiska unionen har befogenhet att besluta om åtgärder i syfte att upprätta den inre marknaden eller säkerställa dess funktion i enlighet med tillämpliga bestämmelser i fördragen (artikel 26 i fördraget om Europeiska unionens funktionssätt — EUF-fördraget). Enligt artikel 114 i EUF-fördraget kan EU "besluta om åtgärder för *tillnärmning av sådana bestämmelser i lagar och andra författningar i medlemsstaterna* som syftar till att upprätta den inre marknaden och få den att fungera".

Såsom anges ovan är nät och informationssystem viktiga för att främja den gränsöverskridande rörligheten för varor, tjänster och personer. De är ofta sammankopplade, och internet är till sin natur globalt. I och med denna inneboende transnationella dimension kan störningar i en medlemsstat även påverka andra medlemsstater och EU som helhet. Nätens och informationssystemens motståndskraft och stabilitet är därför avgörande för en smidigt fungerande inre marknad.

EU-lagstiftarna har redan konstaterat att det är nödvändigt att harmonisera nät- och informationssäkerhetsbestämmelserna för att säkerställa den inre marknadens utveckling. Ett exempel är förordning 460/2004/EG om inrättandet av Enisa[23], som grundas på artikel 114 i EUF-fördraget.

De skillnader som beror på medlemsstaternas olika nationell kapacitet, politik och skyddsnivå när det gäller nät- och informationssäkerhet skapar hinder på den inre marknaden och gör det motiverat att vidta EU-åtgärder.

3.2. Subsidiaritet

Europeiska åtgärder inom nät- och informationssäkerheten kan motiveras enligt subsidiaritetsprincipen.

För det första, med tanke på nät- och informationssäkerhetens gränsöverskridande natur skulle frånvaro av åtgärder på EU-nivå leda till en situation där varje medlemsstat agerar på egen hand och inte tar hänsyn till att näten och informationssystemen i EU är helt beroende av varandra. En lämplig nivå av samordning mellan medlemsstaterna skulle säkerställa att nät- och informationssäkerhetsriskerna hanteras på rätt sätt i det gränsöverskridande sammanhang

[23] Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet, EUT L 077, 13.3.2004, s. 1.

där de uppstår. Olika lagstiftning om nät- och informationssäkerhet utgör ett hinder för företag som vill bedriva verksamhet i flera länder och står i vägen för globala stordriftsfördelar.

Lagstadgade skyldigheterna på EU-nivå krävs också för att säkra samma konkurrensvillkor för alla och åtgärda kryphål i lagstiftningen. Ett tillvägagångssätt baserat på frivillighet har endast mynnat ut i samarbete inom den minoritet av medlemsstaterna som har en hög skyddskapacitet. För att man ska kunna involvera samtliga medlemsstater måste man säkerställa att alla har den en kapacitet som uppnår nödvändiga miniminivån. De nät- och informationssäkerhetsåtgärder som vidtas av regeringar måste vara enhetliga och samordnas för att begränsa och minimera konsekvenserna av nät- och informationssäkerhetsincidenter. Inom nätverket kommer de behöriga myndigheterna och kommissionen att samarbeta, genom ett utbyte av bästa praxis och med kontinuerligt deltagande av Enisa, för att främja ett enhetligt genomförande av direktivet i hela EU. En samordnad och samverkande nät- och informationssäkerhetspolitik kan därför ha en starkt positiv påverkan på det faktiska skyddet av de grundläggande rättigheterna och i synnerhet rätten till integritetsskydd och skydd av personuppgifter. Åtgärder på EU-nivå skulle därför öka effektiviteten i befintliga nationella strategier och underlätta utvecklingen av sådana.

De föreslagna åtgärderna är också motiverade med utifrån proportionalitetsprincipen. De krav som fastställs för medlemsstaterna ligger på den miniminivå som krävs för att uppnå adekvat beredskap och möjliggöra ett förtroendefullt samarbete. Medlemsstaterna kan ta hänsyn till nationella särdrag samtidigt som det säkerställs att gemensamma EU-principer tillämpas på ett proportionerligt sätt. Det breda tillämpningsområdet innebär att medlemsstaterna kan genomföra direktivet med beaktande av de faktiska riskerna på nationell nivå som identifierats i den nationella nät- och informationssäkerhetsstrategin. Kraven på riskhantering gäller endast för kritiska enheter och omfattar åtgärder som står i proportion till riskerna. I det offentliga samrådet underströks att det är viktigt att säkerheten garanteras för dessa kritiska enheter. Rapporteringskraven skulle endast omfatta incidenter med betydande konsekvenser. Såsom anges ovan skulle åtgärderna inte medföra några oproportionerligt stora kostnader, eftersom många av dessa enheter är registeransvariga som redan i enlighet med nuvarande dataskyddsbestämmelser måste se till att personuppgifter skyddas.

För undvika oproportionerligt stora bördor för små operatörer, i synnerhet små och medelstora företag, står kraven i proportion till den risk som det berörda nätet eller informationssystemet motsvarar och ska inte tillämpas på mikroföretag. Riskerna måste först identifieras av de enheter som omfattas av skyldigheterna, vilka sedan måste besluta om vilka åtgärder som ska vidtas för att begränsa sådana risker.

De angivna målen kan uppnås bättre på EU-nivå än av de enskilda medlemsstaterna med tanke på de gränsöverskridande aspekterna av nät- och informationssäkerhetsincidenter och nät- och informationssäkerhetsrisker. Såsom anges i artikel 5 i fördraget om Europeiska unionen får unionen därför vidta åtgärder i enlighet med subsidiaritetsprincipen. I enlighet med proportionalitetsprincipen går det föreslagna direktivet inte utöver vad som är nödvändigt för att uppnå dessa mål.

För att målen ska uppnås bör kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 290 i EUF-fördraget för att komplettera eller ändra vissa icke väsentliga delar av den grundläggande rättsakten. Kommissionens förslag är också tänkt att stödja göra de skyldigheter som läggs på privata och offentliga aktörer mer proportionella.

För att säkerställa enhetliga villkor för genomförande av den grundläggande rättsakten bör kommissionen ges befogenhet att anta genomförandeakter i enlighet med artikel 291 i fördraget om Europeiska unionens funktionssätt.

I och med att det föreslagna direktivet har stor räckvidd och omfattar tungt reglerade områden, samt med tanke på de rättsliga skyldigheter som härleds från dess kapitel IV, bör anmälningarna av införlivandeåtgärder åtföljas av förklarande dokument. I enlighet med den gemensamma politiska förklaringen från medlemsstaterna och kommissionen om förklarande dokument av den 28 september 2011 har medlemsstaterna åtagit sig att, i de fall detta är berättigat, låta anmälan av införlivandeåtgärder åtföljas av ett eller flera dokument som förklarar förhållandet mellan de olika delarna i direktivet och motsvarande delar i de nationella instrumenten för införlivande. När det gäller detta direktiv anser lagstiftaren det vara motiverat att sådana dokument översänds.

4. BUDGETKONSEKVENSER

Samarbete och informationsutbyte mellan medlemsstaterna bör stödjas genom en säker infrastruktur. Förslaget kommer endast att påverka EU:s budget om medlemsstaterna väljer att anpassa en befintlig infrastruktur (t.ex. sTESTA) och ge kommissionen i uppdrag att genomföra detta i enlighet med den fleråriga budgetramen 2014–2020. Engångskostnaden uppskattas till 1 250 000 euro, som skulle belasta EU-budgeten, budgetpost 09.03.02 (Samtrafikförmåga och interoperabilitet mellan nationella offentliga onlinetjänster samt tillgång till sådana nät — kapitel 09.03, Fonden för ett sammanlänkat Europa — telenät) under förutsättning att tillräckliga medel finns tillgängliga inom fonden för ett sammanlänkat Europa. Alternativt kan medlemsstaterna antingen dela på engångskostnaden för att anpassa en befintlig infrastruktur eller besluta att inrätta en ny infrastruktur och ta kostnaderna, som uppskattas uppgå till omkring 10 miljoner euro per år.

2013/0027 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet 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],

efter att ha hört Europeiska datatillsynsmannen,

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) Nät och informationssystem och nät- och informationstjänster har en viktig roll i samhället. Deras tillförlitlighet och säkerhet är en förutsättning för ekonomisk verksamhet och social välfärd och i synnerhet för den inre marknadens funktion.

(2) Avsiktliga eller oavsiktliga säkerhetsincidenter blir allt mer omfattande och vanliga, vilket utgör ett allvarligt hot mot nätens och informationssystemens funktion. Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande finansiella förluster, undergräva användarnas förtroende och medföra allvarliga konsekvenser för unionens ekonomi.

(3) Som ett kommunikationsinstrument utan gränser har de digitala informationssystemen, och i synnerhet internet, en viktig funktion för att främja den gränsöverskridande rörligheten för varor, tjänster och personer. Denna transnationella natur innebär att störningar i en medlemsstat även kan påverka andra medlemsstater och EU som helhet. Nätens och informationssystemens motståndskraft och stabilitet är därför avgörande för en smidigt fungerande inre marknad.

(4) En samarbetsmekanism bör inrättas på unionsnivå för att möjliggöra informationsutbyte och samordning av upptäckt och samordnade svarsåtgärder när det gäller nät- och informationssäkerhet. För att denna mekanism ska vara effektiv och inkluderande är det viktigt att alla medlemsstater har en minimikapacitet och en strategi som säkerställer en hög nivå av nät- och informationssäkerhet på det egna territoriet. Minimikrav avseende säkerhet bör också gälla för offentliga förvaltningar och operatörer av kritisk informationsinfrastrukturer, för att främja en riskhanteringskultur och säkerställa att de allvarligaste incidenterna rapporteras.

[1] EUT C […], […], s. […].

(5) Detta direktiv bör tillämpas på alla nät och informationssystem, så att alla relevanta incidenter och risker täcks. De skyldigheter som införs för offentliga förvaltningar och marknadsoperatörer bör dock inte tillämpas på företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster enligt Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv)[2], som omfattas av de särskilda säkerhets- och integritetskrav som fastställs i artikel 13a i direktivet; direktivet bör inte heller tillämpas på tillhandahållare av betrodda tjänster.

(6) Den befintliga kapaciteten räcker inte för att säkerställa en hög nivå av nät- och informationssäkerhet i unionen. Medlemsstaterna har väldigt olika nivåer av beredskap, vilket leder till fragmenterade angreppssätt i unionen. Resultatet blir olika grad av skydd för konsumenter och företag, vilket undergräver den allmänna nät- och informationssäkerhetsnivån i unionen. Avsaknaden av gemensamma minimikrav för offentliga förvaltningar och marknadsoperatörer gör det i sin tur omöjligt att inrätta en övergripande och effektiv mekanism för samarbete på unionsnivå.

(7) Effektiva reaktioner på utmaningarna på nät- och informationssäkerhetsområdet förutsätter därför ett övergripande angreppssätt på unionsnivå, som omfattar en gemensam lägsta nivå för kapacitetsuppbyggnad och planering, utbyte av information och samordning av åtgärder samt gemensamma minimikrav avseende säkerhet för alla berörda marknadsoperatörer och offentliga förvaltningar.

(8) Bestämmelserna i detta direktiv bör inte påverka varje enskild medlemsstats möjligheter att vidta de åtgärder som är nödvändiga för att skydda sina väsentliga säkerhetsintressen, för att skydda allmän ordning och säkerhet och för att möjliggöra utredning, upptäckt och åtal av brott. Enligt artikel 346 i EUF-fördraget ska ingen medlemsstat vara skyldig att lämna sådan information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen.

(9) För att uppnå och bibehålla en gemensam hög säkerhetsnivå för nät och informationssystem bör alla medlemsstater ha en nationell nät- och informationssäkerhetsstrategi där de fastställer de strategiska mål och konkreta politiska åtgärder som ska genomföras. Man bör på nationell nivå utarbeta planer för samarbete om nät- och informationssäkerhet med grundläggande krav för att uppnå en kapacitet för svarsåtgärder som möjliggör ett effektivt och verkningsfullt samarbete på nationell nivå och unionsnivå vid incidenter.

(10) För att uppnå ett effektivt genomförande av de bestämmelser som antas i enlighet med detta direktiv bör man i varje medlemsstat inrätta eller utse ett organ med ansvar för samordning av nät- och informationssäkerhetsfrågor som kan fungera som sambandspunkt för det gränsöverskridande samarbetet på unionsnivå. Dessa organ 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 detta direktivs mål.

(11) Samtliga medlemsstater bör ha både den tekniska och organisatoriska kapacitet som krävs för att förebygga, upptäcka, reagera på och begränsa effekterna av incidenter och risker vad gäller nät och informationssystem. Välfungerade incidenthanteringsorganisationer som uppfyller grundläggande krav bör därför inrättas

[2] EGT L 108, 24.4.2002, s. 33.

i alla medlemsstater för att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå.

(12) På grundval av de betydande framsteg som gjorts inom det europeiska forumet för medlemsstaterna (EFMS) när det gäller att främja diskussioner och utbyten av bästa praxis, inbegripet utarbetandet av principer för ett europeiskt samarbete vid cyberkriser bör medlemsstaterna och kommissionen bilda ett nätverk som för samman dem för kontinuerlig kommunikation och stöder deras samarbete. En sådan säker och effektiv samarbetsmekanism bör skapa förutsättningar för ett strukturerat och samordnat genomförande av informationsutbyte, upptäckt och svarsåtgärder på unionsnivå.

(13) Europeiska byrån för nät- och informationssäkerhet (Enisa) bör bistå medlemsstaterna och kommissionen genom att tillhandahålla expertis och rådgivning och främja utbyte av bästa praxis. Vid tillämpningen av detta direktiv bör kommissionen i synnerhet konsultera Enisa. För att medlemsstaterna och kommissionen i rätt tid ska få den information som behövs bör tidiga varningar om incidenter och risker lämnas inom samarbetsnätverket. För att bygga upp kapacitet och kunskap bland medlemsstaterna bör samarbetsnätverket också fungera som ett instrument för utbyte av bästa praxis och bistå sina medlemmar vid kapacitetsuppbyggnad samt leda organiserandet av sakkunnigbedömning och nät- och informationssäkerhetsövningar.

(14) En säker infrastruktur bör upprättas för informationsutbyte så att känslig och konfidentiell information kan utbytas inom samarbetsnätverket. Utan att det påverkar medlemsstaternas skyldighet att anmäla incidenter och risker med en unionsdimension till samarbetsnätverket bör medlemsstater inte få tillgång till konfidentiell information från andra medlemsstater förrän de kan visa att deras tekniska och finansiella resurser, personalresurser och kommunikationsinfrastruktur garanterar att de kan delta i nätverket på ett effektivt, verkningsfullt och säkert sätt.

(15) Eftersom de flesta nät och informationssystem är i privat drift är det mycket viktigt med samarbete mellan offentlig och privat sektor. Marknadsoperatörer bör uppmuntras att upprätta egna informella samarbetsmekanismer för att garantera nät- och informationssäkerheten. De bör också samarbeta med den offentliga sektorn och utbyta information och bästa praxis i utbyte mot operativt stöd vid incidenter.

(16) För att säkra öppenhet och insyn och informera EU-medborgare och marknadsoperatörer ordentligt bör de behöriga myndigheterna skapa en gemensam webbplats för offentliggörande av sådan information om incidenter och risker som inte är konfidentiell.

(17) När information anses konfidentiell enligt unionens bestämmelser och nationella bestämmelser om företagshemlighet bör denna konfidentialitet säkerställas vid genomförande av verksamheter och uppfyllande av mål enligt detta direktiv.

(18) På grundval av i synnerhet de nationella erfarenheterna av krishantering bör kommissionen och medlemsstaterna, i samarbete med Enisa, utarbeta en unionsplan för nät- och informationssäkerhetssamarbete som omfattar samarbetsmekanismer för att bemöta risker och incidenter. Planen bör vederbörligen beaktas när tidiga varningar görs inom samarbetsnätverket.

(19) Anmälan av en tidig varning inom nätverket bör endast krävas när den berörda incidenten eller risken är av sådan omfattning och så allvarlig att den är eller kan bli så betydande att det är nödvändigt med information eller samordning av svarsåtgärderna på unionsnivå. Tidiga varningar bör därför begränsas till faktiska eller potentiella

incidenter eller risker som är av snabbt ökande omfattning, som överstiger den nationella beredskapen eller som påverkar mer än en medlemsstat. För att möjliggöra en riktig utvärdering bör all information av relevans för bedömningen av risken eller incidenten meddelas samarbetsnätverket.

(20) Vid mottagandet av en tidig varning, och vid sin bedömning av den, bör de behöriga myndigheterna enas om samordnade svarsåtgärder i enlighet med unionens plan för nät- och informationssäkerhetssamarbete. Behöriga myndigheter bör, liksom kommissionen, informeras om de åtgärder som vidtas på nationell nivå till följd av de samordnade svarsåtgärderna.

(21) I och med att nät- och informationssäkerhetsproblemen är globala till sin natur behövs ett närmare internationellt samarbete för att förbättra säkerhetsstandarder och informationsutbyten och främja ett gemensamt sätt att hantera nät- och informationssäkerhetsfrågor.

(22) Ansvaret för att garantera nät- och informationssäkerheten vilar i hög grad på offentliga förvaltningar och marknadsoperatörer. En kultur av riskhantering, som inbegriper riskbedömning och genomförande av säkerhetsåtgärder som är anpassade till riskerna, bör främjas och utvecklas genom ändamålsenliga krav i lagstiftning och frivillig branschpraxis. Lika konkurrensvillkor för alla krävs också för ett effektivt fungerande samarbetsnätverk som kan säkerställa ett effektivt samarbete från alla medlemsstater.

(23) Enligt direktiv 2002/21/EG ska företag som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster vidta lämpliga åtgärder för att skydda deras integritet och säkerhet och införa anmälningskrav avseende säkerhetsöverträdelser och integritetsförlust. Enligt Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)[3] ska leverantören av en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa säkerheten i sina tjänster.

(24) Dessa skyldigheter bör utvidgas bortom sektorn för elektronisk kommunikation till viktiga leverantörer av informationssamhällets tjänster, enligt definitionen i Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster[4], som ligger till grund för informationssamhällets tjänster i senare led eller onlineverksamhet, t.ex. e-handelsplattformar, internetbelningsslussar, sociala nät, sökmotorer, molntjänster och onlineförsäljning av tillämpningar. Störningar i denna typ av informationssamhällestjänster hindrar tillhandahållandet av andra informationssamhällestjänster som är beroende av dem. Programutvecklare och hårdvarutillverkare är inte leverantörer av informationssamhällets tjänster och omfattas därför inte. Dessa skyldigheter bör också utvidgas till att omfatta offentliga förvaltningar och operatörer av kritisk infrastruktur som är starkt beroende av informations- och kommunikationsteknik och som behövs för upprätthållandet av centrala ekonomiska eller samhälleliga funktioner som el och gas, transporter, kreditinstitut, börser och hälso- och sjukvård. Störningar i dessa nät och informationssystem skulle påverka den inre marknaden.

---

3 EGT L 201, 31.7.2002, s. 37.

4 EGT L 204, 21.7.1998, s. 37.

(25) Tekniska och organisatoriska åtgärder som införs för offentliga förvaltningar och marknadsoperatörer bör inte omfatta krav på att en viss kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt.

(26) De offentliga förvaltningarna och marknadsoperatörerna bör garantera säkerheten för de nät och system som står under deras kontroll. Det rör sig framför allt om privata nät och system som antingen förvaltas av deras interna it-personal eller vars säkerhet har lagts ut på entreprenad. Säkerheten och anmälningsskyldigheterna bör gälla för relevanta marknadsoperatörer och offentliga förvaltningar oavsett om de själva sköter underhållet på sina nät och informationssystem internt eller om de lägger ut uppgifterna på entreprenad.

(27) För att undvika oproportionerligt stora finansiella och administrativa bördor för små operatörer och användare bör kraven stå i proportion till den risk som det berörda nätet eller informationssystemet utgör, med beaktande av de bästa sådana åtgärderna. Dessa krav bör inte gälla för mikroföretag.

(28) Behöriga myndigheter bör se till att upprätthålla informella och tillförlitliga kanaler för informationsutbyte mellan marknadsoperatörer och mellan offentlig och privat sektor. Vid offentliggörande av incidenter som rapporteras till de behöriga myndigheterna bör allmänhetens intresse av att få information om hot vägas mot eventuella negativ inverkan på ryktet och affärerna för de offentliga förvaltningar och marknadsoperatörer som rapporterar incidenter. Vid genomförandet av anmälningsskyldigheterna bör behöriga myndigheter särskilt ta hänsyn till behovet av att hålla uppgifter om produkters sårbara aspekter strikt konfidentiella till dess att ändamålsenliga säkerhetslösningar släpps.

(29) Behöriga myndigheter bör ha de medel som de behöver för att kunna fullgöra sina förpliktelser, inbegripet befogenhet att få fram tillräckligt med information från marknadsoperatörer och offentliga förvaltningar för att bedöma säkerhetsnivån för nät och informationssystem liksom tillförlitliga och heltäckande data om faktiska incidenter som har inverkat på nätens och informationssystemens drift.

(30) I många fall är det kriminell verksamhet som ligger bakom en incident. Incidenternas kriminella art kan misstänkas även om det inte finns några entydiga bevis från början. I sådana fall bör ett lämpligt samarbete mellan behöriga myndigheter och brottsbekämpande myndigheter ingå i effektiva och omfattande svarsåtgärder på hotet från säkerhetsincidenter. För att främja en säker, trygg och mer motståndskraftig miljö krävs i synnerhet en systematisk rapportering av incidenter som misstänks vara av kriminell art till de brottsbekämpande myndigheterna. Incidenters allvarliga kriminella art bör bedömas i ljuset av EU-lagstiftningen om it-brott.

(31) Säkerheten för personuppgifter äventyras ofta till följd av incidenter. I detta sammanhang bör de behöriga myndigheterna och dataskyddsmyndigheterna samarbeta och utbyta information om alla relevanta frågor för att hantera personuppgiftsbrott till följd av incidenter. Medlemsstaterna ska genomföra skyldigheten att anmäla säkerhetsincidenter på ett sätt som minimerar den administrativa bördan om säkerhetsincidenten också är ett personuppgiftsbrott i linje med förslaget till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter[5]. Genom samarbete med de behöriga myndigheterna och dataskyddsmyndigheterna skulle Enisa kunna vara till hjälp genom att utveckla

[5] SEK(2012) 72 slutlig.

mekanismer och modeller för informationsutbyte så att det inte behövs två anmälningsmallar. Denna enda anmälningsmall skulle underlätta rapporteringen av incidenter som hotar säkerheten för personuppgifter och därigenom lätta den administrativa bördan för företag och offentliga förvaltningar.

(32) Standardisering av säkerhetskrav är en marknadsdriven process. För att säkerställa en konvergerad tillämpning av säkerhetsstandarder bör medlemsstaterna främja efterlevnad eller överensstämmelse med specificerade standarder för att garantera en hög säkerhetsnivå på unionsnivå. Därför kan det vara nödvändigt att utarbeta harmoniserade standarder, i enlighet med 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[6].

(33) Detta direktiv bör ses över med jämna mellanrum, främst i syfte att avgöra behovet av modifieringar med hänsyn till den tekniska utvecklingen eller ändrade marknadsvillkor.

(34) För att se till att samarbetsnätverket fungerar på ett korrekt sätt bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på fastställandet av de kriterier som en medlemsstat ska uppfylla för att ha rätt att delta i det säkra informationsutbytessystemet, ytterligare specificering av de händelser som utlöser tidig varning och definitionen av de omständigheter då marknadsoperatörer och offentliga förvaltningar är skyldiga att anmäla incidenter.

(35) Det är av särskild betydelse att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. Vid förberedelse och utarbetande av delegerade akter bör kommissionen säkerställa att relevanta dokument samtidigt, utan dröjsmål och på lämpligt sätt lämnas till Europaparlamentet och rådet.

(36) För att säkerställa enhetliga villkor för genomförandet av direktivet bör kommissionen ges genomförandebefogenheter när det gäller samarbetet mellan behöriga myndigheter och kommissionen inom samarbetsnätverket, tillträdet till den säkra infrastrukturen för informationsutbyte, unionens samarbetsplan för nät- och informationssäkerhet, formaten och förfarandena för att informera allmänheten om incidenter samt standarderna och/eller de tekniska specifikationerna av betydelse för nät- och informationssäkerhet. Dessa befogenheter bör utövas i enlighet med 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[7].

(37) Vid tillämpningen av direktivet bör kommissionen på lämpligt sätt samarbeta med relevanta sektorskommittéer och organ som inrättas på EU-nivå, i synnerhet inom energi-, transport- och hälso- och sjukvårdsområdet.

(38) Information som den nationella regleringsmyndigheten anser vara konfidentiell i enlighet med unionslagstiftning och nationell lagstiftning om affärshemligheter, får endast utbytas med kommissionen och andra behöriga myndigheter när sådant utbyte är absolut nödvändigt för att tillämpa bestämmelserna i detta direktiv. Den information

---

6 EUT L 316, 14.11.2012, s. 12.

7 EUT L 55, 28.2.2011, s. 13.

som utbyts bör begränsas till vad som är relevant och proportionellt för ändamålet med utbytet.

(39) Utbytet av information om risker och incidenter inom samarbetsnätverket och uppfyllandet av kravet att anmäla incidenter till de behöriga nationella myndigheterna kan förutsätta behandling av personuppgifter. Sådan behandling av personuppgifter är nödvändig för att tillgodose detta direktivs syfte av allmänintresse och är därmed berättigad enligt artikel 7 i direktiv 95/46/EG. I förhållande till detta legitima syfte utgör den inte ett oproportionerligt och oacceptabelt ingripande som påverkar själva kärnan i rätten till skydd av personuppgifter som garanteras enligt artikel 8 i stadgan om de grundläggande rättigheterna. Vid tillämpningen av detta direktiv bör Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar[8] gälla i tillämpliga fall. När uppgifter behandlas av unionens institutioner och organ bör bearbetning i samband med till genomförandet av detta direktiv ske i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.

(40) Eftersom målet för denna förordning, det vill säga att garantera en hög nivå av nät- och informationssäkerhet i unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och eftersom det därför, på grund av åtgärdens verkningar, bättre kan uppnås 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 dessa mål.

(41) Förslaget överensstämmer med de grundläggande rättigheterna och de principer som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna, i synnerhet rätten till skydd för privatliv och kommunikation, skyddet av personuppgifter, näringsfriheten, äganderätten, rätten till ett effektivt rättsmedel och rätten att höras. Detta direktiv måste tillämpas i enlighet med dessa rättigheter och principer.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte och tillämpningsområde

1. Direktivet omfattar åtgärder som ska säkerställa en hög gemensam nivå av nät- och informationssäkerhet (NIS) inom EU.

2. Direktivet omfattar därför följande:

(a) Det fastställer skyldigheter för alla medlemsstater när det gäller förebyggande åtgärder, hantering och svarsåtgärder vid risker och incidenter som påverkar nät och informationssystem.

(b) Det inrättar en samarbetsmekanism mellan medlemsstaterna som ska säkerställa en enhetlig tillämpning av detta direktiv inom unionen och, vid behov, en samordnad

[8] EGT L 145, 31.5.2001, s. 43.

och effektiv hantering och samordnade och effektiva svarsåtgärder vid risker och incidenter som påverkar nät och informationssystem.

(c) Det fastställer säkerhetskrav för marknadsaktörer och offentliga förvaltningar.

3. Säkerhetskraven enligt artikel 14 ska inte tillämpas på företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster enligt direktiv 2002/21/EG, då dessa ska uppfylla de säkerhets- och integritetskrav som fastställs i artiklarna 13a och 13b i det direktivet, eller på leverantörer av betrodda tjänster.

4. Detta direktiv påverkar inte tillämpningen av EU-lagstiftning om it-brottslighet och 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[9]

5. Detta direktiv påverkar inte heller tillämpningen av 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[10] och Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter[11].

6. Informationsutbytet inom samarbetsnätverket enligt kapitel III och anmälan av nät- och informationssäkerhetsincidenter enligt artikel 14 kan förutsätta behandling av personuppgifter. Sådan behandling, som är nödvändig för att tillgodose detta direktivs syfte av allmänintresse ska godkännas av medlemsstaten i enlighet med artikel 7 i direktiv 95/46/EG och direktiv 2002/58/EG, såsom dessa har genomförts i nationell lagstiftning.

Artikel 2

Minimiharmonisering

Medlemsstaterna ska inte vara förhindrade att anta eller behålla bestämmelser som garanterar en högre säkerhetsnivå, utan att det påverkar deras skyldigheter enligt unionslagstiftningen.

Artikel 3

Definitioner

I detta direktiv gäller följande definitioner:

(1) nät och informationssystem:

(a) elektroniskt kommunikationsnät enligt direktiv 2002/21/EG, och

(b) apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlade uppgifter, samt

[9] EUT L 345, 23.12.2008, s. 75.
[10] EGT L 281, 23.11.1995, s. 31.
[11] SEC(2012) 72 final.

(c) datorbehandlade uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av element som omfattas av led a och b för att de skall kunna drivas, användas, skyddas och underhållas.

(2) *säkerhet:* förmågan hos ett nät eller ett informationssystem att, vid en viss tillförlitlighetsnivå, tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda data eller hos besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät och informationssystem.

(3) *risk:* en omständighet eller händelse som har en potentiell negativ inverkan på säkerheten.

(4) *incident:* en omständighet eller händelse som har en faktisk negativ inverkan på säkerheten.

(5) *informationssamhällestjänst:* tjänst enligt artikel 1.2 i direktiv 98/34/EG.

(6) *NIS-samarbetsplan:* en plan som fastställer en ram för organisatoriska roller, ansvarsområden och förfaranden för att bibehålla eller återställa driften av nät och informationssystem som påverkas av en risk eller incident.

(7) *incidenthantering:* alla förfaranden som stödjer analys och begränsning av effekterna av en incident samt svarsåtgärder.

(8) *marknadsoperatör:*

(a) Leverantör av informationssamhällestjänster som möjliggör tillhandahållandet av andra informationssamhällestjänster; en ej uttömmande förteckning över sådana tjänster finns i bilaga II.

(b) Operatör av kritisk infrastruktur som är nödvändig för upprätthållandet av viktig ekonomisk och samhällelig verksamhet inom områdena energi-, transport-, bank-, börs- samt hälso- och sjukvårdsverksamhet; en ej uttömmande förteckning över sådana verksamheter finns i bilaga II.

(9) *standard:* standard som avses i förordning (EU) nr 1025/2012.

(10) *specifikation:* specifikation som avses i förordning (EU) nr 1025/2012.

(11) *leverantör av betrodd tjänst:* fysisk eller juridisk person som tillhandahåller en elektronisk tjänst som består av skapande, kontroll, validering, hantering och bevarande av elektroniska signaturer, elektroniska sigill, elektroniska tidsmärkningar, elektroniska dokument, elektroniska leveranstjänster, autentisering av webbplatser och elektroniska certifikat, inklusive certifikat för elektroniska signaturer och för elektroniska sigill.

KAPITEL II

NATIONELLA RAMVERK FÖR NÄT- OCH INFORMATIONSSÄKERHET

Artikel 4

Princip

Medlemsstaterna ska säkerställa en hög säkerhetsnivå för nät och informationssystem på deras territorium i enlighet med detta direktiv.

Artikel 5

Nationell NIS-strategi och nationell NIS-samarbetsplan

1. Varje medlemsstat ska anta en nationell NIS-strategi som fastställer de strategiska målen och de konkreta politiska åtgärderna och lagstiftningsåtgärderna för att uppnå och upprätthålla en hög nivå av nät- och informationssäkerhet. Den nationella NIS-strategin ska i synnerhet omfatta följande:

(a) Definitionen av mål och prioriteringar för strategin baserat på en aktuell risk- och incidentanalys.

(b) En styrelseram för att uppnå de strategiska målen och prioriteringarna, inklusive en tydlig definition av roller och ansvarsområden för offentliga organ och andra berörda aktörer.

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

(d) Angivelse av utbildnings- och informationsprogram.

(e) Forsknings- och utvecklingsplaner och en beskrivning av hur dessa planer speglar de angivna prioriteringarna.

2. Den nationella NIS-strategin ska innehålla en nationell NIS-samarbetsplan som minst uppfyller följande krav:

(a) En riskbedömningsplan för kartläggning av risker och bedömning av verkningarna av potentiella incidenter.

(b) Definition av roller och ansvarsområden för olika aktörer som deltar i genomförandet av planen.

(c) Definition av samarbets- och kommunikationsprocesser som säkerställer förebyggande, upptäckt, svarsåtgärder, reparation och återhämtning och som anpassas till larmnivån.

(d) En plan för nät- och informationssäkerhetsövningar och -utbildning för att stärka, validera och testa planen. Lärdomar ska dokumenteras och föras in när planen uppdateras.

3. Den nationella NIS-strategin och den nationella NIS-samarbetsplanen ska meddelas kommissionen inom en månad från antagandet.

Artikel 6

Nationell behörig myndighet för säkerheten i nät och informationssystem

1. Varje medlemsstat ska utse en behörig nationell myndighet för säkerheten i nät och informationssystem (*den behöriga myndigheten*).

2. De behöriga myndigheterna ska övervaka tillämpningen av detta direktiv på nationell nivå och bidra till en konsekvent tillämpning i hela unionen.

3. Medlemsstaterna ska se till att de behöriga myndigheterna har tillräckliga tekniska och finansiella resurser samt personalresurser för att på ett effektivt sätt kunna utföra de uppgifter de tilldelas och därigenom uppnå detta direktivs syften. Medlemsstaterna ska se till att de behöriga myndigheterna samarbetar på ett effektivt och säkert sätt via det nätverk som avses i artikel 8.

4. Medlemsstaterna ska se till att de behöriga myndigheterna får de anmälningar av incidenter som görs av offentliga förvaltningar och marknadsoperatörer såsom anges i artikel 14.2 och att de tilldelas de genomförande- och verkställighetsbefogenheter som avses i artikel 15.

5. De behöriga myndigheterna ska när så är lämpligt samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna och dataskyddsmyndigheterna.

6. Varje medlemsstat ska utan dröjsmål meddela kommissionen den behöriga myndighet som utses, denna myndighets uppgifter och alla senare ändringar av detta. Varje medlemsstat ska offentliggöra utnämningen av den behöriga myndigheten.

Artikel 7

Incidenthanteringsorganisation

1. Varje medlemsstat ska inrätta en incidenthanteringsorganisation (*Computer Emergency Response Team, Cert*) som ansvarar för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande som ska uppfylla kraven i bilaga I punkt 1. En incidenthanteringsorganisation får inrättas inom den behöriga myndigheten.

2. Medlemsstaterna ska se till att incidenthanteringsorganisationerna har de tekniska och finansiella resurser och personalresurser som behöver för att effektivt utföra sina uppgifter som anges i bilaga I punkt 2.

3. Medlemsstaterna ska se till att incidenthanteringsorgansationer förlitar sig på en säker och motståndskraftig kommunikations- och informationsinfrastruktur på nationell nivå, och den ska vara förenlig och interoperabel med det säkra system för informationsutbyte som avses i artikel 9.

4. Medlemsstaterna ska underrätta kommissionen om incidenthanteringsorganisationernas resurser och mandat samt om deras förfarande för incidenthantering.

5. Incidenthanteringsorganisationen ska bedriva sin verksamhet under tillsyn av den behöriga myndigheten, som regelbundet ska bedöma om resurserna är tillräckliga, om mandatet är ändamålsenligt och om incidenthanteringsförfarandet är effektivt.

KAPITEL III

SAMARBETE MELLAN BEHÖRIGA MYNDIGHETER

Artikel 8

Samarbetsnätverk

1. De behöriga myndigheterna och kommissionen ska bilda ett nätverk (*samarbetsnätverk*) för att samarbeta om risker och incidenter som påverkar nät och informationssystem.

2. Samarbetsnätverket ska föra samman kommissionen och de behöriga myndigheterna i kontinuerlig kommunikation. På begäran ska Europeiska byrån för nät- och informationssäkerhet (Enisa) bistå samarbetsnätverket med expertis och råd.

3. Inom samarbetsnätverket ska de behöriga myndigheterna göra följande:

   (a) Sprida tidiga varningar om risker och incidenter i enlighet med artikel 10.

(b) Säkerställa samordnade svarsåtgärder i enlighet med artikel 11.

(c) Regelbundet offentliggöra ej konfidentiell information om pågående tidiga varningar och samordnade svarsåtgärder på en gemensam webbplats.

(d) På en begäran av en medlemsstat eller kommissionen gemensamt diskutera och bedöma en eller leda nationella NIS-strategier och nationella NIS-samarbetsplaner enligt artikel 5, inom detta direktivs räckvidd.

(e) På begäran av en medlemsstat eller kommissionen gemensamt diskutera och bedöma incidenthanteringsorganisationernas effektivitet, i synnerhet när NIS-övningar genomförs på unionsnivå.

(f) Samarbeta och utbyta information om alla relevanta frågor med Europeiska it-brottscentrumet inom Europol och med andra relevanta europeiska organ, i synnerhet inom områdena dataskydd, energi, transport, bankverksamhet, börs och hälso- och sjukvård.

(g) Utbyta information och bästa praxis med varandra och med kommissionen och bistå varandra i uppbyggnaden av NIS-kapacitet.

(h) Anordna regelbundna kollegiala granskningar av kapacitet och beredskap.

(i) Anordna NIS-övningar på unionsnivå och delta, såsom lämpligt, i internationella NIS-övningar.

4. Kommissionen ska genom genomförandeakter anta de bestämmelser som är nödvändiga för att underlätta samarbetet mellan behöriga myndigheter och kommissionen enligt punkterna 2 och 3. Dessa genomförandeakter ska antas i enlighet med det samrådsförfarande som avses i artikel 19.2.

Artikel 9

Säkert system för informationsutbyte

1. Känslig och konfidentiell information inom samarbetsnätverket ska utbytas via en säker infrastruktur.

2. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 18 när det gäller definitionen av de kriterier som en medlemsstat ska uppfylla för att godkännas för deltagande i det säkra systemet för informationsutbyte, vad gäller följande:

(a) Medlemsstaten ska ha tillgång till en säker och motståndskraftig kommunikations- och informationsinfrastruktur på nationell nivå, som ska vara förenlig och interoperabel med samarbetsnätverkets säkra infrastruktur i enlighet med artikel 7.3.

(b) Den behöriga myndigheten och incidenthanteringsorganisationen ska ha tillräckliga tekniska och finansiella resurser samt personalresurser för att på ett effektivt och säkert sätt kunna delta i det säkra systemet för informationsutbyte i enlighet med artiklarna 6.3, 7.2 och 7.3.

3. Kommissionen ska genom genomförandeakter besluta om medlemsstaternas tillträde till denna säkra infrastruktur, i enlighet med de kriterier som avses i punkterna 2 och 3. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19.

Artikel 10

Tidig varning

1. De behöriga myndigheterna eller kommissionen ska lämna tidiga varningar inom samarbetsnätverket om de risker eller incidenter som uppfyller minst ett av följande villkor:

   (a) De ökar snabbt i omfattning eller kan öka snabbt i omfattning.

   (b) De överstiger eller kan överstiga den nationella kapaciteten för svarsåtgärder.

   (c) De påverkar eller kan påverka mer än en medlemsstat.

2. I de tidiga varningarna ska de behöriga myndigheterna eller kommissionen meddela all relevant information som de förfogar över och som kan vara till nytta för att bedöma risken eller incidenten.

3. På begäran av en medlemsstat eller på eget initiativ kan kommissionen begära att en medlemsstat inkommer med relevant information om en specifik risk eller incident.

4. Om den risk eller incident som är föremål för en tidig varning misstänks vara av brottslig art ska de behöriga myndigheterna eller kommissionen underrätta Europeiska it-brottscentrumet inom Europol.

5. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 18 när det gäller ytterligare specificering av risker och incidenter som utlöser en tidig varning enligt punkt 1.

Artikel 11

Samordnade svarsåtgärder

1. Efter en tidig varning enligt artikel 10 ska de behöriga myndigheterna, efter att gjort en bedömning av den relevanta informationen enas om samordnade svarsåtgärder i enlighet med unionens NIS-samarbetsplan enligt artikel 12.

2. De olika åtgärder som antas på nationell nivå till följd av de samordnade svarsåtgärderna ska meddelas samarbetsnätverket.

Artikel 12

Unionens NIS-samarbetsplan

1. Kommissionen ska ha befogenhet att genom genomförandeakter anta unionens NIS-samarbetsplan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19.

2. Unionens NIS-samarbetsplan ska omfatta följande:

   (a) För de syften som avses i artikel 10:

      – En definition av format och förfaranden för de behöriga myndigheternas insamling och utbyte av kompatibla och jämförbara uppgifter om risker och incidenter.

      – En definition av förfarandena och kriterierna för samarbetsnätverkets bedömning av risker och incidenter.

   (b) Förfarandena för samordnade svarsåtgärder enligt artikel 11, inklusive definition av roller, ansvarsområden och samarbetsförfaranden.

(c) En plan för NIS-övningar och NIS-utbildning för att stärka, validera och testa planen.

(d) Ett program för överföring av kunskap mellan medlemsstater när det gäller kapacitetsuppbyggnad och ömsesidigt lärande.

(e) Ett program för medvetandehöjande och utbildning mellan medlemsstaterna.

3. Unionens NIS-samarbetsplan ska antas senast ett år efter detta direktivs ikraftträdande och regelbundet revideras.

Artikel 13

Internationellt samarbete

Utan att det påverkar samarbetsnätverkets möjlighet att ha informella internationella samarbeten får unionen ingå internationella avtal med tredjeländer eller internationella organisationer som tillåter och organiserar deras deltagande i vissa av samarbetsnätverkets verksamheter. Sådana avtal ska beakta behovet av ändamålsenligt skydd för personuppgifter som förmedlas via samarbetsnätverket.

KAPITEL IV

SÄKERHET FÖR OFFENTLIGA FÖRVALTNINGARS OCH MARKNADSOPERATÖRERS NÄT OCH INFORMATIONSSYSTEM

Artikel 14

Säkerhetskrav och anmälan av incidenter

1. Medlemsstaterna ska se till att offentliga förvaltningar och marknadsoperatörer vidtar ändamålsenliga tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten för de nät och informationssystem som de kontroller och använder i sin verksamhet. Med beaktande av den senaste tekniken ska dessa åtgärder garantera en säkerhetsnivå som är anpassad till den aktuella risken. I synnerhet ska åtgärder vidtas för att förebygga och minimera de effekter som incidenter som påverkar deras nät och informationssystem har på de kärntjänster som de tillhandahåller och därmed säkerställa kontinuiteten för de tjänster som använder dessa nät och informationssystem.

2. Medlemsstaterna ska säkerställa att offentliga förvaltningar och marknadsoperatörer underrättar den behöriga myndigheten om incidenter som har en betydande inverkan på säkerheten för de kärntjänster som de tillhandahåller.

3. Dessa krav enligt punkterna 1 och 2 gäller för alla marknadsoperatörer som tillhandahåller tjänster inom Europeiska unionen.

4. Den behöriga myndigheten får informera allmänheten eller kräva att de offentliga myndigheterna och marknadsoperatörerna informerar allmänheten, om den fastställer att det ligger i allmänhetens intresse att incidenten röjs. En gång om året ska den behöriga myndigheten lämna in en sammanfattande rapport till samarbetsnätverket om de anmälningar som kommit in och de åtgärder som vidtagits i enlighet med denna punkt.

5. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet artikel 18 när det gäller definition av de omständigheter då offentliga förvaltningar och marknadsoperatörer är skyldiga att anmäla incidenter.

6. Utan att det påverkar tillämpningen av delegerade akter som antas enligt punkt 5 får de behöriga myndigheterna anta riktlinjer och, om nödvändigt, utfärda anvisningar avseende de omständigheter då offentliga förvaltningar och marknadsoperatörer är skyldiga att anmäla incidenter.

7. Kommissionen ska ha befogenhet att genom genomförandeakter definiera format och förfaranden för tillämpningen av punkt 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19.

8. Punkterna 1 och 2 ska inte tillämpas på mikroföretag enligt definitionen i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag[12].

Artikel 15

Genomförande och efterlevnad

1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har de befogenheter de behöver för att utreda fall då offentliga förvaltningar eller marknadsoperatörer inte uppfyllt sina skyldigheter enligt artikel 14 och de effekter som detta har på nätens och informationssystemens säkerhet.

2. Medlemsstaterna ska se till att de behöriga myndigheterna har befogenhet att ålägga att marknadsoperatörer och offentliga förvaltningar

   (a) tillhandahåller den information som behövs för en bedömning av säkerheten i deras nät och informationssystem, inbegripet dokumenterade säkerhetsprinciper, och

   (b) genomgår en säkerhetsrevision som utförs av ett kvalificerat oberoende organ eller av en nationell myndighet och ge den behöriga myndigheten tillgång till resultaten.

3. Medlemsstaterna ska se till att de behöriga myndigheterna har befogenhet att utfärda bindande anvisningar för marknadsoperatörer och offentliga förvaltningar.

4. De behöriga myndigheterna ska anmäla incidenter som misstänks vara av allvarlig brottslig art till de rättsvårdande myndigheterna.

5. De behöriga myndigheterna ska ha ett nära samarbete med de myndigheter som ansvarar för skydd av personuppgifter när de åtgärdar incidenter som medför personuppgiftsbrott.

6. Medlemsstaterna ska säkerställa att alla skyldigheter som införs för offentliga förvaltningar och marknadsoperatörer i enlighet med detta kapitel kan bli föremål för rättslig prövning.

Artikel 16

Standardisering

1. För att säkerställa en enhetlig tillämpning av artikel 14.1 ska medlemsstaterna främja användningen av standarder och/eller specifikationer av relevans för nät- och informationssäkerheten.

[12] EGT L 124, 20.5.2003, s. 36.

2. Kommissionen ska i genomförandeakter utarbeta en lista över de standarder som avses i punkt 1. Listan ska kungöras i *Europeiska unionens officiella tidning*.

KAPITEL V

SLUTBESTÄMMELSER

Artikel 17

Påföljder

1. Medlemsstaterna ska föreskriva påföljder för överträdelser av nationella bestämmelser som har utfärdats med tillämpning av detta direktiv och ska vidta de åtgärder som krävs för att se till att dessa påföljder tillämpas. Påföljderna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska anmäla dessa bestämmelser till kommissionen senast det datum då direktivet införlivas med nationell lagstiftning och skall utan dröjsmål anmäla alla senare ändringar som påverkar dem.

2. När säkerhetsincidenter rör personuppgifter ska medlemsstaterna säkerställa att de påföljder som föreskrivs överensstämmer med de påföljder som föreskrivs i Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter[13].

Artikel 18

Utövande av delegeringen

1. Kommissionens rätt att anta delegerade akter gäller på de villkor som fastställs i denna artikel.

2. Befogenhet att anta de delegerade akter som avses i artiklarna 9.2, 10.5 och 14.5 ska ges till kommissionen. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av femårsperioden. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.

3. Den delegering av befogenhet som avses i artiklarna 9.2, 10.5 and 14.5 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. När kommissionen antagit en delegerad akt ska den samtidigt underrätta Europaparlamentet och rådet.

5. En delegerad akt som antas i enlighet med artiklarna 9.2, 10.5 och 14.5 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att

[13] SEK(2012) 72 slutlig.

invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 19

Kommittéförfarande

1. Kommissionen ska bistås av en kommitté (kommittén för nät- och informationssäkerhet). Denna ska vara en kommitté enligt förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 4 i förordning (EU) nr 182/2011 tillämpas.
3. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Artikel 20

Översyn

Kommissionen ska regelbundet se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet. Den första rapporten ska lämnas senast tre år efter den införlivandedag som avses i artikel 21. För detta syfte kan kommissionen begära att medlemsstaterna utan dröjsmål tillhandahåller information.

Artikel 21

Införlivande

1. Medlemsstaterna ska senast [ett och ett halvt år efter antagandet] anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska till kommissionen genast överlämna texten till dessa bestämmelser.

   De ska tillämpa dessa bestämmelser från och med [ett och ett halvt år efter antagandet].

   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 texterna till de bestämmelser i nationell lagstiftning som de antar inom det område som omfattas av detta direktiv.

Artikel 22

Ikraftträdande

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

Artikel 23

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Bryssel den

På Europaparlaments vägnar
Ordförande

På rådets vägnar
Ordförande

BILAGA I

Krav och uppgifter för incidenthanteringsorganisationen (Cert)

Incidenthanteringsorganisationens krav och uppgifter ska på lämpligt och entydigt sätt fastställas och stödjas genom nationell politik och/eller lagstiftning. Följande ska ingå:

(1) Krav för incidenthanteringsorganisationen

(a) Incidenthanteringsorganisationen ska säkerställa god tillgång till sina kommunikationstjänster genom att undvika felkritiska systemdelar (*single points of failure*) och kunna kontaktas och kontakta andra på flera olika sätt. Kommunikationskanalerna ska vara tydligt specificerade och välkända för användargruppen och samarbetspartner.

(b) Incidenthanteringsorganisationen ska genomföra och förvalta säkerhetsåtgärder för att säkra konfidentialiteten, integriteten, åtkomligheten och äktheten för den information som den får in och behandlar.

(c) Incidenthanteringsorganisationens kontor och de informationssystem som den använder sig av ska vara lokaliserade till säker plats.

(d) Ett kvalitetssystem för tjänsteförvaltningen ska skapas för att följa upp kvaliteten på incidenthanteringsorganisationens arbete och säkerställa kontinuerliga förbättringar. Det ska baseras på tydligt definierade kvalitetsmått som omfattar formella tjänstenivåer och resultatindikatorer.

(e) Kontinuitetsplanering:

- Incidenthanteringsorganisationen ska ha ett ändamålsenligt system för handläggning och dirigering av ansökningar, för att underlätta överlämnanden.
- Incidenthanteringsorganisationen ska ha tillräckligt med personal för att ständigt vara tillgänglig.
- Incidenthanteringsorganisationen ska förlita sig på en infrastruktur vars kontinuitet är säkerställd. Därför måste det finnas redundans vad gäller system och reservlokaler så att incidenthanteringsorganisationen kan säkerställa permanent åtkomst till kommunikationskanalerna.

(2) Incidenthanteringsorganisationens uppgifter

(a) Incidenthanteringsorganisationens uppgifter ska omfatta minst följande:

- Övervakning av incidenter på nationell nivå.
- Tidiga varningar, larm, meddelanden och informationsspridning till relevanta aktörer om risker och incidenter.
- Svarsåtgärder på incidenter.
- Tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet.
- Uppbyggnad av bred medvetenhet hos allmänheten om de risker som är förbundna med onlineaktivitet.
- Anordnande av kampanjer för nät- och informationssäkerhet.

(b) Incidenthanteringsorganisationen ska bygga upp samarbetsrelationer med den privata sektorn.

(c) För att underlätta samarbete ska incidenthanteringsorganisationen främja antagandet och användningen av gemensam eller standardiserad praxis för

– förfaranden för hantering av incidenter och risker,

– klassificeringssystem för incidenter, risker och information,

– systematiserade kvalitetsmått,

– format för informationsutbyte om risker och incidenter samt konventioner för namngivningssystem.

BILAGA II

Lista över marknadsoperatörer

Enligt artikel 3.8 a:

1. E-handelsplattformar.

2. Internetbetalningsslussar.

3. Sociala medier.

4. Sökmotorer

5. Molntjänster.

6. Onlineförsäljning av tillämpningar.

Enligt artikel 3.8 b

1. Energi.

- El- och gasleverantörer.
- Systemansvariga för el- och/eller gasdistributionssystem och återförsäljare till slutkunderna.
- Systemansvariga för gasöverföringssystem, naturgaslager och LNG.
- Systemansvariga för elöverföringssystem.
- Oljeledningar och oljelager.
- El- och gasmarknadsaktörer.
- Operatörer av olje- och naturgasproduktion, raffinaderier och bearbetningsanläggningar.

2. Transporter.

- Lufttrafikföretag (gods- och persontransporter).
- Sjötransportföretag (transportföretag som bedriver persontrafik till havs och längs kuster samt transportföretag som bedriver godstrafik till havs och längs kuster).
- Järnväg (infrastrukturförvaltare, integrerade företag och järnvägstransportföretag).
- Flygplatser.
- Hamnar
- Trafikstyrning och trafikledning.
- Logistiska stödtjänster a) lager- och magasineringstjänster, b) godshantering och c) andra stödverksamheter för transporter).

3. Bankverksamhet: Kreditinstitut i enlighet med artikel 4.1 i direktiv 2006/48/EG.

4. Finansmarknadsinfrastruktur: börser och organisationer för central motpartsclearing.

5. Hälso- och sjukvårdssektorn: Hälso- och sjukvårdsmiljöer (inklusive sjukhus och privata kliniker) och andra enheter som tillhandahåller hälso- och sjukvårdsverksamhet.

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets beteckning

1.2. Berörda politikområden i den verksamhetsbaserade förvaltningen och budgeteringen

1.3. Typ av förslag eller initiativ

1.4. Mål

1.5. Motivering till förslaget eller initiativet

1.6. Tid under vilken åtgärden kommer att pågå respektive påverka resursanvändningen

1.7. Planerad metod för genomförandet

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

2.2. Administrations- och kontrollsystem

2.3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

3.2. Beräknad inverkan på utgifterna

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

3.2.2. Beräknad inverkan på driftsanslagen

3.2.3. Beräknad inverkan på de administrativa anslagen

3.2.4. Förenlighet med den gällande fleråriga budgetramen

3.2.5. Bidrag från tredje part

3.3. Beräknad inverkan på inkomsterna

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets beteckning

Förslag till Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen.

1.2. Berörda politikområden i den verksamhetsbaserade förvaltningen och budgeteringen[37]

- 09 – Kommunikationsnät, innehåll och teknik

1.3. Typ av förslag eller initiativ

☒ Ny åtgärd

☐ Ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd[38]

☐ Befintlig åtgärd vars genomförande förlängs i tiden

☐ Tidigare åtgärd som omformas till eller ersätts av en ny

1.4. Mål

1.4.1. Fleråriga strategiska mål för kommissionen som förslaget eller initiativet är avsett att bidra till

Syftet med direktivförslaget är att säkerställa en hög nivå av nät- och informationssäkerhet i hela EU.

1.4.2. Specifika mål eller verksamheter inom den verksamhetsbudgeterade förvaltningen och budgeteringen som berörs

Förslaget omfattar åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen

De särskilda syftena är följande:

1. Att införa en miniminivå av nät- och informationssäkerhet i medlemsstaterna och därmed höja den allmänna nivån på beredskapen och svarskapaciteten.

2. Att förbättra samarbetet om nät- och informationssäkerhet på EU-nivå för att effektivt kunna bemöta gränsöverskridande incidenter och hot. En säker infrastruktur bör upprättas för informationsutbyte så att känslig och konfidentiell information kan utbytas mellan de behöriga myndigheterna.

3. Att bygga upp en riskhanteringskultur och förbättra informationsförmedlingen mellan privat och offentlig sektor.

Berörda verksamheter enligt den verksamhetsbaserade förvaltningen och budgeteringen

Direktivet omfattar enheter (företag och organisationer, inbegripet vissa små och medelstora företag) i flera sektorer (energi, transport, kreditinstitut, börs, hälso- och sjukvård och företag som har betydelse för viktiga internettjänster) samt offentliga förvaltningar. Det har kopplingar till brottsbekämpning och dataskydd och nät- och informationssäkerhetsaspekter av yttre förbindelser.

- 09 – Kommunikationsnät, innehåll och teknik

[37] Verksamhetsbaserad förvaltning och verksamhetsbaserad budgetering benämns ibland med de interna förkortningarna ABM respektive ABB.

[38] I den mening som avses i artikel 49.6 a respektive 49.6 b i budgetförordningen.

- 02 – Näringsliv
- 32 - Energi
- 06 - Rörlighet och transport
- 17 - Hälsa och konsumentskydd
- 18 – Inrikes frågor
- 19 – Yttre förbindelser
- 33 - Rättsliga frågor
- 12 - Inre marknaden

1.4.3. Verkan eller resultat som förväntas

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

Skyddet av EU:s konsumenter, företag och förvaltningar mot nät- och informationssäkerhetsincidenter och –risker skulle förbättras avsevärt.

Ytterligare detaljer finns i avsnitt 8.2 (Konsekvenserna av alternativ 2 – Lagstiftning) i kommissionens konsekvensanalys som åtföljer det här lagstiftningsförslaget.

1.4.4. Indikatorer för bedömning av resultat eller verkan

Ange vilka indikatorer som ska användas för att följa upp hur förslaget eller initiativet genomförs.

Indikatorerna för övervakning och utvärdering finns i avsnitt 10 i konsekvensanalysen.

1.5. Motivering till förslaget eller initiativet

1.5.1. Behov som ska tillgodoses på kort eller lång sikt

Varje medlemsstat skulle behöva ha

- en nationell NIS-strategi,
- en NIS-samarbetsplan,
- en nationell behörig myndighet för nät- och informationssäkerhet, och
- en incidenthanteringsorganisation (Cert).

På EU-nivå skulle medlemsstaterna vara skyldiga att samarbeta via ett nätverk.

Offentliga förvaltningar och viktiga privata aktörer skulle åläggas att utföra NIS-riskhantering och underrätta de behöriga myndigheterna om nät- och informationssäkerhetsincidenter med betydande inverkan.

1.5.2. Mervärdet av en åtgärd på unionsnivå

I och med att nät- och informationssäkerheten är en gränsöverskridande fråga utgör skillnader i den relevanta lagstiftningen och politiken ett hinder för företag som är verksamma i flera länder och för uppnåendet av globala stordriftsfördelar. Om inget görs på EU-nivå leder det till en situation där varje medlemsstat agerar på egen hand utan hänsyn till att näten och informationssystemen är ömsesidigt beroende av varandra.

De angivna målen kan därför bättre uppnås med hjälp av åtgärder på EU-nivå än av de enskilda medlemsstaterna.

1.5.3. Erfarenheter från liknande försök eller åtgärder

Förslaget bygger på analysen att lagstadgade skyldigheter krävs för att skapa lika konkurrensvillkor för alla och täppa till luckor i lagstiftningen. Inom detta område har ett

tillvägagångssätt baserat på frivillighet endast mynnat ut i samarbete inom den minoritet av medlemsstaterna som har en hög skyddskapacitet.

1.5.4. Förenlighet med andra finansieringsformer och eventuella synergieffekter

Förslaget är helt förenligt med en digital agenda för Europa och därmed med EU:s 2020-strategi. Det är också förenligt med och kompletterar EU:s regelverk för elektronisk kommunikation, EU-direktivet om europeisk kritisk infrastruktur och EU:s dataskyddsdirektiv.

Förslaget läggs fram tillsammans med, och som en viktig del av, det gemensamma meddelandet om en europeisk strategi för it-säkerhet från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik.

1.6. Tid under vilken åtgärden kommer att pågå respektive påverka resursanvändningen

– ☐ Förslag eller initiativ som pågår under begränsad tid

– ☐ Förslaget eller initiativet ska gälla från [den DD/MM]ÅÅÅÅ till [den DD/MM]ÅÅÅÅ.

– ☐ Det påverkar resursanvändningen från ÅÅÅÅ till ÅÅÅÅ.

– ☒ Förslag eller initiativ som pågår under en obegränsad tid

– Införlivandeperioden kommer att inledas omedelbart efter antagandet (som beräknas till 2015) och pågå i 18 månader. Genomförandet av direktivet kommer dock att inledas efter antagandet och kommer att omfatta inrättandet av säker infrastruktur till stöd för medlemsstaternas samarbete,

– följt av en fullskalig verksamhet.

1.7. Planerad metod för genomförandet[39]

– ☒ Direkt centraliserad förvaltning som sköts av kommissionen

– ☒ Indirekt centraliserad förvaltning genom delegering till

– ☐genomförandeorgan

– ☒ byråer/organ som inrättats av gemenskaperna[40]

– ☐ nationella offentligrättsliga organ eller organ som anförtrotts uppgifter som faller inom offentlig förvaltning

– ☐ personer som anförtrotts ansvaret för genomförandet av särskilda åtgärder som följer av avdelning V i fördraget om Europeiska unionen och som anges i den grundläggande rättsakten i den mening som avses i artikel 49 i budgetförordningen

– ☐ Delad förvaltning med medlemsstaterna

– ☐ Decentraliserad förvaltning med tredjeländer

– ☐ Gemensam förvaltning med internationella organisationer, inbegripet Europeiska rymdorganisationen

Vid fler än en metod, ange kompletterande uppgifter under ”Anmärkningar”.

Anmärkningar:
Enisa, som är ett decentraliserat organ inrättat av gemenskaperna, får bistå medlemsstaterna och kommissionen i genomförandet av direktivet på grundval av sitt mandat och genom omfördelning av resurser enligt den fleråriga budgetramen för 2014–2020 för detta organ.

[39] Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

[40] Organ som avses i artikel 185 i budgetförordningen.

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder

Kommissionen kommer regelbundet att se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet.

Kommissionen kommer också att utvärdera åtgärderna för införlivande av direktivet i alla medlemsstater.

Förslaget till FSE ger också utrymme till en utvärdering av metoderna för projektens genomförande och vilken inverkan de har haft, i syfte att bedöma om målen, bland annat i fråga om miljöskydd, har uppnåtts.

2.2. Administrations- och kontrollsystem

2.2.1. Risker som identifierats

- förseningar av projektet i samband med upprättandet av den säkra infrastrukturen

2.2.2. Planerade kontrollmetoder

Avtalen och besluten för genomförandet av åtgärder enligt FSE kommer att omfatta bestämmelser om tillsyn och finansiell kontroll av kommissionen, eller av en företrädare utsedd av kommissionen, samt om revision av revisionsrätten och kontroller på plats som utförs av Europeiska byrån för bedrägeribekämpning (Olaf).

2.2.3. Kostnader och vinster för kontroller och förväntad nivå av bristande uppfyllande

Riskbaserade förhands- och efterhandskontroller och möjligheten till kontroller på plats kommer att säkerställa att kostnaderna för kontroller blir rimliga

2.3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade)

Kommissionen ska se till att unionens ekonomiska intressen skyddas vid genomförandet av åtgärder som finansieras enligt det här direktivet, genom förebyggande åtgärder mot bedrägeri, korruption och annan olaglig verksamhet, genom effektiva kontroller och, om oriktigheter upptäcks, genom återkrav av felaktigt utbetalda medel samt vid behov genom effektiva, proportionella och avskräckande påföljder.

Kommissionen eller dess företrädare och revisionsrätten ska ha befogenhet att utföra revision, på grundval av handlingar och kontroller på plats, hos alla stödmottagare, uppdragstagare och underleverantörer som erhållit unionsfinansiering enligt det här programmet.

Europeiska byrån för bedrägeribekämpning (Olaf) får, i enlighet med förfarandena i förordning (Euratom, EG) nr 2185/96, utföra kontroller på plats och inspektioner hos ekonomiska aktörer som direkt eller indirekt berörs av unionsfinansiering, i syfte att fastställa om det har förekommit bedrägeri, korruption eller annan olaglig verksamhet som påverkar unionens ekonomiska intressen i samband med bidragsavtal, bidragsbeslut eller andra avtal som berörs av sådan finansiering.

Utan att det påverkar tillämpningen av styckena ovan ska befogenheten att utföra revision, kontroller på plats och inspektioner uttryckligen tillerkännas kommissionen,

revisionsrätten och Olaf i samarbetsavtal med tredjeland eller internationella organisationer, bidragsavtal, bidragsbeslut och andra avtal som ingås med tillämpning av det här direktivet.

Enlig FSE ska avtal om bidrag och upphandling baseras på standardavtal, som kommer att omfatta de allmänt tillämpade bedrägeribekämpningsåtgärderna.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

- Befintliga budgetrubriker (även kallade ”budgetposter”)

Redovisa de berörda rubrikerna i budgetramen i nummerföljd och – inom varje sådan rubrik – de berörda budgetrubrikerna i den årliga budgeten i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av anslag	Bidrag			
	Antal [Beskrivning…..….]	Diff./Icke-diff. (41)	från Efta-länder[42]	från kandidat-länder[43]	från tredjeländer	enligt artikel 18.1 aa i budgetförordningen
	09 03 02 Främja samtrafikförmåga och interoperabilitet mellan nationella offentliga tjänster på nätet samt tillgång till sådana nät.	Diff. anslag	NEJ	NEJ	NEJ	NEJ

- Nya budgetrubriker som föreslås (ej tillämpligt)

Redovisa de berörda rubrikerna i den budgetramen i nummerföljd och – inom varje sådan rubrik – de berörda budgetrubrikerna i den årliga budgeten i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av anslag	Bidrag			
	Nummer [Beteckning…..]	Diff./Icke-diff.	från Efta-länder	från kandidatländer	från tredjeländer	enligt artikel 18.1 aa i budgetförordningen
	XX.YY.YY.YY.		JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ

41 Differentierade respektive icke-differentierade anslag.

42 EFTA: European Free Trade Association.

43 Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

3.2. Beräknad inverkan på utgifterna

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	1	Smart tillväxt för alla

GD: <…….>			2015* [44]	År 2016	År 2017	År 2018	Följande år: (2019–2021) och därefter			**TOTALT**
• Driftsanslag										
09 03 02	Åtaganden	(1)	1.250**	0.000						**1.250**
	Betalningar	(2)	0.750	0.250	0.250					**1.250**
Administrativa anslag som finansieras genom ramanslagen för vissa operativa program[45]			**0.000**							**0.000**
Budgetrubrik (nr)		(3)	**0.000**							**0.000**
TOTALA anslag för GD <….>	Åtaganden	=1+1a +3	1.250	0.000						**1.250**
	Betalningar	=2+2a +3	0.750	0.250	0.250					**1.250**

• TOTALA driftsanslag	Åtaganden	(4)	1.250	0.000						**1.250**
	Betalningar	(5)	0.750	0.250	0.250					**1.250**
• TOTALA administrativa anslag som finansieras genom		(6)	**0.000**							

[44] Med år n avses det år då förslaget eller initiativet ska börja genomföras.

[45] Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

ramanslagen för särskilda program										
TOTALA anslag för RUBRIK 1 i den fleråriga budgetramen	Åtaganden	=4+ 6	1.250	0.000						**1.250**
	Betalningar	=5+ 6	0.750	0.250	0.250					**1.250**

* Den exakta tidpunkten kommer att bero på när förslaget antas av den lagstiftande myndigheten (dvs. om direktivet kommer att godkännas under 2014 kommer anpassningen av en befintlig infrastruktur att inledas 2015, annars blir det ett år senare).

** Om medlemsstaterna väljer att använda en befintlig infrastruktur och att låta engångskostnaden för anpassning täckas av EU-budgeten, såsom förklaras under 1.4.3 och 1.7, beräknas kostnaden för att anpassa ett nät till samarbetet mellan medlemsstaterna i enlighet med kapitel III i direktivet (tidig varning, samordnade svarsåtgärder etc.) uppgå till 1 250 000 euro. Det är en aningen större summa än vad som anges i konsekvensanalysen ("omkring 1 miljon euro") eftersom den bygger på en mer exakt beräkning av de olika delar som behövs för en sådan infrastruktur. De olika delar som behövs och kostnaderna för dem baseras på en beräkning som gjorts av JRC, på grundval av deras erfarenhet av utveckling av liknande system för andra områden som folkhälsa, och det rör sig om följande delar: ett system för snabba larm och anmälningar när det gäller nät- och informationssäkerhet (275 000 euro), en plattform för informationsutbyte (400 000 euro), ett system för tidig varning och svarsåtgärder (275 000 euro), en lägescentral (300 000 euro) för totalt 1 250 000 euro. En mer detaljerad genomförandeplan väntas i den kommande genomförbarhetsstudien inom ramen för det särskilda kontraktet SMART 2012/0010: *Feasibility study and preparatory activities for the implementation of a European early warning and response system against cyber-attacks and disruptions*.

Följande ska anges om flera rubriker i budgetramen påverkas av förslaget eller initiativet:

• TOTALA driftsanslag	Åtaganden	(4)	0.000	0.000						
	Betalningar	(5)	0.000	0.000						
• TOTALA administrativa anslag som finansieras genom ramanslagen för särskilda program		(6)	**0.000**	**0.000**						
TOTALA anslag för RUBRIKERNA 1–4 i den fleråriga budgetramen (referensbelopp)	Åtaganden	=4+ 6	1.250	0.000						1.250
	Betalningar	=5+ 6	0.750	0.250	0.250					1.250

Rubrik i den fleråriga budgetramen	**5**	”Administrativa utgifter”

Miljoner euro (avrundat till tre decimaler)

		År **2015**	År **2016**	År **2017**	År **2018**	Följande år: (2019–2021) och därefter			**TOTALT**
GD:CNECT									
• Personal		0.572	0.572	0.572	0.572	0.572	0.572	**0.572**	**4.004**
• Övriga administrativa utgifter		0.318	0.118	0.318	0.118	0.318	0.118	**0.118**	**1.426**
TOTALT GD CNECT	Anslag	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

TOTALA anslag för RUBRIK 5 i den fleråriga budgetramen	(Totala åtaganden = Totala betalningar)	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

Miljoner euro (avrundat till tre decimaler)

		År **2015**[46]	År **2016**	År **2017**	År **2018**	Följande år: (2019–2021) och därefter			**TOTALT**
TOTALA anslag för RUBRIKERNA 1–5 i den fleråriga budgetramen	Åtaganden	2.140	0.690	0.890	0.690	0.890	0.690	0.690	**6.680**
	Betalningar	1.640	0.940	1.140	0.690	0.890	0.690	0.690	**6.680**

[46] Med år n avses det år då förslaget eller initiativet ska börja genomföras.

3.2.2. Beräknad inverkan på driftsanslagen

– ☐ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

– ☑ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

– Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Mål- och resultatbeteckning ⇩			År **2015***		År **2016**		År **2017**		År **2018**		Följande år: (2019–2021) och därefter						**TOTALT**	
			RESULTAT															
	Typ[47]	Genom-snittliga kostna-der	Antal	Kostnad	Antal	Kostnad	Antal	Kostnad	Antal	Kostnad	Antal	Kostnad	Antal	Kostnad	Antal	Kostnad	Totalt antal	Totalt kostnader
MÅL 2[48] Säkert system för informationsutbyte																		
- Resultat	Anpassa infrastruktur																	
Delsumma mål 2			1	1.250**													1	1.250
TOTALA KOSTNADER				1.250														1.250

47 Resultaten som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).

48 Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål…”.

* Den exakta tidpunkten kommer att bero på när förslaget antas av den lagstiftande myndigheten (dvs. om direktivet kommer att godkännas under 2014 kommer anpassningen av en befintlig infrastruktur att inledas 2015, annars blir det ett år senare).

** Se punkt 3.2.1

3.2.3. Beräknad inverkan på de administrativa anslagen

3.2.3.1. Sammanfattning

– ☐ Förslaget/initiativet kräver inte att administrativa anslag tas i anspråk

– ☑ Förslaget/initiativet kräver att administrativa anslag tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

	År **2015**[49]	År **2016**	År **2017**	År **2018**	Följande år: (2019–2021) och därefter			**TOTALT**
RUBRIK 5 i den fleråriga budgetramen								
Personal	0.572	0.572	0.572	0.572	0.572	0.572	0.572	**4.004**
Övriga administrativa utgifter	0.318	0.118	0.318	0.118	0.318	0.118	0.118	**1.426**
Delsumma RUBRIK 5 i den fleråriga budgetramen	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**
Belopp utanför RUBRIK 5[50] **i den fleråriga budgetramen**								
Personal	0.000	0.000						**0.000**
Övriga administrativa utgifter								
Delsumma för belopp utanför RUBRIK 5 i den fleråriga budgetramen	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**
TOTALT	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

Behoven av administrativa anslag ska täckas med de anslag från GD Cnect som redan har avdelats för att förvalta åtgärden och/eller omfördelats, om så krävs kompletterade med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till rådande begränsningar i fråga om budgetmedel.

49 Med år n avses det år då förslaget eller initiativet ska börja genomföras.

50 Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

Europeiska byrån för nät- och informationssäkerhet (Enisa) kan också bistå medlemsstaterna och kommissionen vid genomförandet av direktivet på grundval av dess mandat och genom omfördelning av Enisas resurser enligt den fleråriga budgetramen 2014–2020, dvs. utan någon ytterligare tilldelning av anslag eller personalresurser.

3.2.3.2. Beräknat personalbehov

– ☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk

– ☑ Förslaget/initiativet kräver att kommissionens personalresurser tas i anspråk enligt följande:

I princip kommer det inte att behövas någon ytterligare arbetskraft. De personalresurser som krävs kommer att vara mycket begränsade och kommer att klaras av personal från generaldirektoratet som redan avsatts för förvaltningen av åtgärden.

Uppgifterna ska anges i heltal (eller med högst en decimal)

		År **2015**	År **2016**	År **2017**	År **2018**	Följande år: (2019–2021) och därefter		
• Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)								
09 01 01 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)		4	4	4	4	4	4	4
XX 01 01 02 (vid delegationer)								
XX 01 05 01 (indirekta forskningsåtgärder)								
XX 10 05 01 (direkta forskningsåtgärder)								
• Extern personal (uttryckt i heltidsekvivalenter)								
09 01 02 01 (kontraktsanställda, nationella experter och vikarier – totalt)		1	1	1	1	1	1	1
XX 01 02 02 (kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter vid delegationerna)								
XX 01 04 ***yy*** [51]	- vid huvudkontoret[52]							
	- vid delegationer							
XX 01 05 02 (kontraktsanställda, vikarier samt nationella experter som arbetar med indirekta forskningsåtgärder)								
10 01 05 02 (kontraktsanställda, vikarier och nationella experter som arbetar med direkta forskningsåtgärder)								
Annan budgetrubrik (ange vilken)								

51 Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).

52 Inom förvaltningen av strukturfonderna, Europeiska jordbruksfonden för landsbygdsutveckling (EJFLU) samt Europeiska fiskerifonden (EFF).

TOTALT	**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX motsvarar det politikområde eller den avdelning i budgeten som avses.

Personalbehoven ska täckas med personal inom GD Cnect som redan har avdelats för att förvalta åtgärden i fråga, och/eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Europeiska byrån för nät- och informationssäkerhet (Enisa) kan också bistå medlemsstaterna och kommissionen vid genomförandet av direktivet på grundval av dess mandat och genom omfördelning av Enisas resurser enligt den fleråriga budgetramen 2014–2020, dvs. utan någon ytterligare tilldelning av anslag eller personalresurser.

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda	- Förberedelse av delegerade akter enligt artikel 14.3 - Förberedelse av genomförandeakter enligt artiklarna 8, 9.2, 12, 14.5, 16 - Bidrag till samarbetet via nätverket på både politisk nivå och operativ nivå. - Deltagande i internationella dialoger och eventuellt ingående av internationella avtal
Extern personal	Stöd till alla ovanstående uppgifter enligt behov

3.2.4. Förenlighet med den gällande fleråriga budgetramen

– ☑ Förslaget/initiativet är förenligt med den gällande fleråriga budgetramen

– ☐ Förslaget/initiativet kräver omfördelningar under den berörda rubriken i den fleråriga budgetramen

De beräknade finansiella effekterna på operativa utgifter enligt förslaget kommer att uppträda om medlemsstaterna väljer att anpassa en befintlig infrastruktur och ge kommissionen i uppdrag att genomföra anpassningen av den inom den fleråriga budgetramen för 2014–2020. De berörda engångskostnaderna skulle täckas inom FSE under förutsättning att tillräckliga medel finns tillgängliga. Alternativt kan medlemsstaterna antingen dela på kostnaderna för anpassningen av infrastrukturen eller på kostnaderna för inrättandet av en ny infrastruktur.

– ☐ Förslaget/initiativet förutsätter att flexibilitetsmekanismen utnyttjas eller att den fleråriga budgetramen revideras[53].

Ej tillämpligt.

3.2.5. Bidrag från tredje part

– Det ingår inga bidrag från tredje part i det aktuella förslaget eller initiativet

3.3. Beräknad inverkan på inkomsterna

– ☑ Förslaget/initiativet påverkar inte budgetens inkomstsida.

[53] Se punkterna 19 och 24 i det interinstitutionella avtalet.