EUROPA-
KOMMISSIONEN

Bruxelles, den 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV

om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele EU

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

BEGRUNDELSE

Sigtet med det foreslåede direktiv er at sikre et højt fælles niveau for net- og informationssikkerhed (NIS). Det indebærer forbedring af sikkerheden i Internettet og private netværk og informationssystemer, der er grundstenen i vores samfund og økonomier. Det skal nås ved at pålægge medlemsstaterne at øge deres beredskab og forbedre deres samarbejde med hinanden og ved at pålægge operatører af kritisk infrastruktur, f.eks. energi, transport, og vigtige udbydere af tjenester i informationssamfundet (e-handelsplatforme, sociale netværk osv.) og offentlige myndigheder at vedtage hensigtsmæssige foranstaltninger til styring af sikkerhedsrisici og indberetning af alvorlige hændelser til de nationale kompetente myndigheder.

Dette forslag forelægges i forbindelse med en fælles meddelelse fra Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik om en europæisk strategi for cybersikkerhed. Strategiens mål er at garantere et sikkert og pålideligt digitalt miljø, samtidig med at de grundlæggende rettigheder og andre af EU's grundliggende værdier fremmes og beskyttes. Dette forslag er det vigtigste skridt i denne strategi. Yderligere tiltag i strategien er fokuseret på oplysning, udvikling af et indre marked for cybersikkerhedsprodukter og -tjenester og fremme af F&U-investeringer. Tiltagene vil blive suppleret med andre, der har til formål at optrappe kampen mod cyberkriminalitet og udvikle en cybersikkerhedspolitik for EU.

1.1. Formålene med forslaget

Net- og informationssikkerhed bliver stadig vigtigere for vores økonomi og vores samfund. Net- og informationssikkerhed er også en vigtig forudsætning for at skabe et pålideligt miljø for den verdensomspændende handel med tjenester. Informationssystemer kan dog blive påvirket af sikkerhedshændelser, f.eks. på grund af menneskelige fejl, naturbegivenheder, tekniske fejl eller ondsindede angreb. Disse hændelser bliver stadig mere omfattende, de sker hyppigere, og de er mere komplekse. I forbindelse med Kommissionens offentlige onlinehøring om "forbedring af net- og informationssikkerhed i EU[1]" blev det konstateret, at 57 % af de adspurgte havde oplevet net- og informationssikkerhedshændelser i det forløbne år, som havde alvorlige konsekvenser for deres aktiviteter. Mangel på net- og informationssikkerhed kan bringe vigtige tjenester i fare, som er afhængige af net- og informationssystemers integritet. Dette kan forhindre virksomheder i at fungere, føre til betydelige finansielle tab for EU's økonomi og have en negativ virkning på samfundsvelfærden.

Som et grænseløst kommunikationsinstrument er digitale informationssystemer, og navnlig internettet, forbundet på tværs af medlemsstaterne og spiller en vigtig rolle i forbindelse med fremme af grænseoverskridende bevægelighed for varer, tjenesteydelser og personer. Væsentlige forstyrrelser af disse systemer i én medlemsstat kan berøre andre medlemsstater og EU som helhed. Net- og informationssystemers robusthed og stabilitet er derfor af afgørende betydning for gennemførelsen af det digitale indre marked og for at opnå et velfungerende indre marked. Sandsynligheden for og hyppigheden af hændelser og den manglende evne til at sikre en effektiv beskyttelse underminerer også offentlighedens tillid til net- og informationstjenester: I 2012 Eurobarometer-udgaven om cybersikkerhed blev det konstateret, at 38 % af brugerne er bekymrede over sikkerheden i forbindelse med onlinebetaling og har ændret deres adfærd på grund af betænkeligheder vedrørende

[1] Den offentlige internethøring om forbedring af net- og informationssikkerhed i EUvarede fra 23. juli til 15. oktober 2012.

sikkerheden: 18 % er mindre tilbøjelige til at købe varer på nettet, og 15 % er mindre tilbøjelige til at foretage bankforretninger på nettet[2].

Den nuværende situation i EU, som afspejler den helt frivillige tilgang, som er blevet fulgt til nu, yder ikke tilstrækkelig beskyttelse mod NIS-hændelser og -risici i EU. De nuværende NIS-kapaciteter og -mekanismer er simpelthen utilstrækkelige til at holde trit med truslernes hurtigt skiftende karakter og sikre et fælles højt beskyttelsesniveau i alle medlemsstater.

Til trods for de initiativer, der er iværksat, er medlemsstaternes kapaciteter og beredskab meget forskellige, og det giver en usammenhængende tilgang i EU. Med tanke på, at net og systemer er indbyrdes forbundne, så svækkes EU's net- og informationssikkerhed af de medlemsstater, der har et utilstrækkeligt beskyttelsesniveau. Det hæmmer også opbygningen af tillid mellem ligestillede, som er en forudsætning for samarbejde og informationsudveksling. Som følge heraf er der kun samarbejde mellem et mindretal af medlemsstaterne med høj kapacitet.

Aktuelt er der således ikke nogen effektiv mekanisme på EU-plan for et effektivt samarbejde og samordning og for en pålidelig informationsudveksling om NIS-hændelser og -risici i medlemsstaterne. Det kan føre til ukoordinerede reguleringsindgreb, usammenhængende strategier og forskellige standarder, hvilket medfører en utilstrækkelig NIS-beskyttelse i hele EU. Der kan også opstå hindringer for det indre marked, som medfører overensstemmelsesomkostninger for virksomheder, der opererer i mere end én medlemsstat.

Endelig er de aktører, der forvalter kritisk infrastruktur eller yder tjenester, der er væsentlige for, at vores samfund fungerer, ikke underlagt passende forpligtelser til at indføre risikostyringsforanstaltninger og udveksle oplysninger med relevante myndigheder. På den ene side mangler virksomhederne derfor effektive incitamenter til at gennemføre en seriøs risikostyring, herunder risikovurdering, og til at træffe hensigtsmæssige foranstaltninger til at sikre net- og informationssikkerheden. På den anden side er der en stor del af hændelserne, som ikke rapporteres til de kompetente myndigheder og således ikke opdages. Oplysninger om hændelser er dog væsentlige for de offentlige myndigheder, så de kan reagere og træffe passende afbødende foranstaltninger og fastlægge passende strategiske prioriteter for net- og informationssikkerhed.

Med de nuværende rammebestemmelser er det kun teleselskaber, der skal indføre risikostyringsforanstaltninger og anmelde alvorlige NIS-hændelser. Der er imidlertid mange andre sektorer, der er afhængige af informations- og kommunikationsteknologi som en katalysator, og som derfor også bør være opmærksomme på net- og informationssikkerheden. En række specifikke infrastruktur- og tjenesteudbydere er særligt udsatte på grund af deres store afhængighed af korrekt fungerende net og informationssystemer. Disse sektorer spiller en væsentlig rolle, når det gælder centrale støttetjenester til vores økonomi og samfund, og sikkerheden i deres systemer er af særlig betydning for det indre markeds funktion. Det drejer sig bl.a. om sektorerne bankvæsen, børser, energiproduktion, -transmission og -distribution, transport (luftfart, jernbaner, søtransport), sundhed, internettjenester og offentlige myndigheder.

Der er derfor behov for en ny måde at håndtere net- og informationssikkerhed i EU. Der er brug for lovfæstede forpligtelser, så der skabes lige vilkår, og nuværende huller i lovgivningen lukkes. For at løse problemerne og øge niveauet for net- og informationssikkerhed i Den Europæiske Union er målene med det foreslåede direktiv følgende:

[2] Eurobarometer 390/2012.

For det første pålægger forslaget alle medlemsstaterne at sikre, at de har et minimum af national kapacitet ved at oprette kompetente myndigheder for net- og informationssikkerhed, etablere it-beredskabsenheder (CERT) og vedtage nationale NIS-strategier og NIS-samarbejdsplaner.

For det andet bør de nationale kompetente myndigheder samarbejde i et netværk, der muliggør sikker og effektiv samordning, herunder også koordineret informationsudveksling samt detektering og indsats på EU-plan. Inden for dette netværk bør medlemsstaterne med udgangspunkt i EU's NIS-samarbejdsplan udveksle information og samarbejde for at imødegå NIS-trusler og -hændelser.

For det tredje sigter forslaget - med rammedirektivet om elektronisk kommunikation som forlæg - mod at sørge for, at der udvikles risikostyringskultur, og at der udveksles oplysninger mellem den private og offentlige sektor. Virksomheder i de særlig kritiske sektorer, der er nævnt i det foregående, og offentlige myndigheder vil blive forpligtet til at foretage en vurdering af de risici, de står overfor, og til at vedtage passende og forholdsmæssige foranstaltninger til at sikre net- og informationssikkerheden. Disse enheder vil skulle underrette de kompetente myndigheder om enhver hændelse, som i alvorlig grad truer deres net og informationssystemer, og som har væsentlig indvirkning på kritiske tjenesters kontinuitet og levering af varer.

1.2. Generel baggrund

Allerede i 2001 i sin meddelelse "Net- og informationssikkerhed: Forslag til en europæisk strategi" understregede Kommissionen den tiltagende vigtighed af net- og informationssikkerhed[3]. Den blev fulgt op med vedtagelsen af en strategi for et sikkert informationssamfund[4] i 2006, som sigter mod at udvikle en net- og informationssikkerhedskultur i Europa. Rådet godkendte strategiens vigtigste elementer i en resolution[5].

Kommissionen vedtog endvidere den 30. marts 2009 en meddelelse om beskyttelse af kritisk informationsinfrastruktur[6], der satte fokus på beskyttelsen af Europa mod cyberkriminalitet ved hjælp af øget sikkerhed. Med meddelelsen lanceredes en handlingsplan for at støtte medlemsstaternes indsats for at sørge for at forebygge og reagere på angreb. Handlingsplanen blev godkendt i formandskabets konklusioner fra ministerkonferencen om beskyttelse af kritisk informationsinfrastruktur i Tallinn i 2009. Den 18. december 2009 vedtog Rådet en resolution om en samordnet europæisk strategi for net- og informationssikkerhed[7].

Den digitale dagsorden for Europa[8], der blev vedtaget i maj 2010, og Rådets konklusioner[9] i denne forbindelse fremhævede det fælles udgangspunkt, at tillid og sikkerhed er grundlæggende forudsætninger for en almen udbredelse af ikt og dermed for at nå målene om "intelligent vækst" ifølge Europa 2020-strategien[10]. I den digitale dagsordens kapitel om tillid og sikkerhed understreges behovet for, at alle aktører samarbejder om en helhedsindsats for at garantere ikt-infrastrukturens sikkerhed og robusthed ved at fokusere på forebyggelse, beredskab og oplysning, og for at der udvikles effektive og koordinerede sikkerhedsmekanismer. Navnlig nøgletiltag 6 i den digitale dagsorden for Europa opfordrer til

---

3 KOM(2001) 298.
4 COM(2006) 251 .
5 2007/068/01.
6 KOM(2009) 149.
7 2009/C 321/01).
8 KOM(2010) 245.
9 Rådets konklusioner af 31. maj 2010 om den digitale dagsorden for Europa (10130/10).
10 KOM(2010) 2020 og Det Europæiske Råds konklusioner af 25. og 26. marts 2010 (EUCO 7/10).

foranstaltninger, der sigter mod en styrket og højt profileret net- og informationssikkerhedspolitik.

I sin meddelelse om beskyttelse af kritisk informationsinfrastruktur fra marts 2011 om "resultater og næste skridt: vejen til global internetsikkerhed"[11] gjorde Kommissionen status over de resultater, der er opnået siden vedtagelsen af handlingsplanen for beskyttelse af kritisk informationsinfrastruktur i 2009, og konkluderede, at gennemførelsen af planen viste, at rent nationale måder at takle udfordringerne med hensyn til sikkerhed og robusthed ikke er tilstrækkelige, og at Europa bør fortsætte sine bestræbelser på at udvikle en sammenhængende og samarbejdsorienteret strategi for hele EU. Meddelelsen fra 2011 om beskyttelse af kritisk informationsinfrastruktur bebudede en række foranstaltninger, og Kommissionen opfordrer medlemsstaterne til at oprette NIS-kapaciteter og grænseoverskridende samarbejde. De fleste af disse foranstaltninger skulle have været afsluttet i 2012, men er endnu ikke gennemført.

I sine konklusioner af 27. maj 2011 om beskyttelse af kritisk informationsinfrastruktur understregede Rådet for Den Europæiske Union det presserende behov for at gøre ikt-systemer og -net modstandsdygtige og sikre over for alle mulige forstyrrelser, uanset om disse er utilsigtede eller ej, at udvikle et højt niveau af beredskab, sikkerhed og robusthed i hele EU, at forbedre de tekniske kompetencer, så Europa kan håndtere beskyttelsen af net og informationsinfrastruktur, og at fremme samarbejdet mellem medlemsstaterne, når det gælder om at udvikle samarbejdsmekanismer mellem medlemsstaterne i forbindelse med hændelser.

1.3. Gældende EU-lovgivning og internationale bestemmelser på det område, som forslaget vedrører

Ved forordning (EF) nr. 460/2004 oprettede Det Europæiske Fællesskab i 2004 Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA)[12] med henblik på at bidrage til at sikre et højt beskyttelsesniveau og udvikling af en net- og informationssikkerhedskultur i EU. Et forslag om ajourføring af ENISA's mandat blev vedtaget den 30. september 2010[13] og er til drøftelse i Rådet og Europa-Parlamentet. De reviderede lovrammer for elektronisk kommunikation[14], der trådte i kraft i november 2009, pålægger udbyderne af elektronisk kommunikation forpligtelser[15]. Disse forpligtelser skulle gennemføres i national lovgivning senest i maj 2011.

Alle aktører, der er de registeransvarlige (for eksempel banker eller hospitaler) er underlagt forpligtelser i henhold til lovrammerne for databeskyttelse[16] om at indføre sikkerhedsforanstaltninger til beskyttelse af personoplysninger. Derudover vil registeransvarlige i henhold til Kommissionens forslag fra 2012 om en generel databeskyttelsesforordning[17] skulle anmelde overtrædelser i forbindelse med personoplysninger til de nationale tilsynsmyndigheder. Det betyder f.eks., at et NIS-sikkerhedsbrud, der berører udførelsen af en tjenesteydelse uden at kompromittere persondata (f.eks. et ikt-nedbrud hos et el-selskab, som medfører et strømudfald) ikke vil skulle anmeldes.

I henhold til direktiv 2008/114 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre beskriver "det europæiske

---

11 KOM(2011) 163.

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

13 KOM(2010) 521.

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

15 Artikel 13a og 13b i rammedirektivet.

16 Direktiv 2002/58/EU af 12. juli 2002.

17 KOM(2012) 11.

program for beskyttelse af kritisk infrastruktur (EPCIP)[18]" den "generelle" strategi for beskyttelse af kritisk infrastruktur i EU. Målene for EPCIP-programmet er fuldt ud i overensstemmelse med dette forslag, og direktivet berører ikke direktiv 2008/114. EPCIP-programmet forpligter ikke operatørerne til at anmelde væsentlige brud på sikkerheden og opstiller ikke mekanismer, så medlemsstaterne kan samarbejde og reagere på hændelser.

Europa-Parlamentet og Rådet drøfter i øjeblikket Kommissionens forslag til et direktiv om angreb på informationssystemer[19], der har til formål at harmonisere kriminaliseringen af særlige typer adfærd. Det omfatter kun kriminalisering af særlige typer adfærd og handler ikke om forebyggelse af NIS-risici og -hændelser, reaktioner på NIS-hændelser eller afbødning af deres virkninger. Nærværende direktiv bør anvendes, uden at det berører direktivet om angreb på informationssystemer.

Den 28. marts 2012 vedtog Kommissionen en meddelelse om oprettelse af et europæisk center for bekæmpelse af it-kriminalitet (EC3)[20]. Centret, som blev oprettet den 11. januar 2013, vil være en del af Den Europæiske Politienhed (Europol) og fungere som kontaktpunkt i kampen mod cyberkriminalitet i EU. EC3 skal samle den europæiske ekspertise om cyberkriminalitet og støtte medlemsstaternes kapacitetsopbygning, yde støtte til medlemsstaternes cyberkriminalitetundersøgelser og i tæt samarbejde med Eurojust fungere som den kollektive stemme for europæiske cyberkriminalitetsefterforskere inden for retshåndhævelse og retsvæsen.

Den Europæiske Unions institutioner, agenturer og organer har oprettet deres egne it-beredskabsenheder, kaldet CERT-EU.

På internationalt plan arbejder EU med cybersikkerhed både bilateralt og multilateralt. Ved topmødet mellem EU og USA i 2010[21] blev der oprettet en EU-USA-arbejdsgruppe om cybersikkerhed og cyberkriminalitet. EU er også aktiv i en række andre relevante multilaterale fora, f.eks. Organisationen for Økonomisk Samarbejde og Udvikling (OECD), FN's Generalforsamling (UNGA), Den Internationale Telekommunikationsunion (ITU), Organisationen for Sikkerhed og Samarbejde i Europa (OSCE), FN's verdenstopmøde om informationssamfundet (WSIS) og Internet Governance Forum (IGF).

2. RESULTAT AF HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER

2.1. Høring af interesserede parter og ekspertbistand

En offentlig onlinehøring vedrørende forbedring af net- og informationssikkerhed i EU fandt sted mellem den 23. juli og 15. oktober 2012. Kommissionen modtog i alt 160 svar på onlinespørgeskemaet.

Det vigtigste resultat var, at de interesserede parter viste, at der er generel opbakning til synspunktet, at der er behov for at forbedre net- og informationssikkerheden i hele EU. Det gælder især følgende: 82,8 % af de adspurgte mente, at regeringerne i EU bør gøre mere for at sikre en høj grad af net- og informationssikkerhed; 82,8 % var af den opfattelse, at brugere af oplysninger og systemer var uvidende om eksisterende NIS-trusler og -hændelser; 66,3 %, ville principielt gå ind for at indføre et lovfæstet krav om NIS-risikostyring; og 84,8 % sagde, at sådanne krav bør fastsættes på EU-plan. Mange af de adspurgte mente, at det ville være

[18] KOM(2006) 786 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

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

[20] COM(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.

vigtigt at vedtage NIS-krav i følgende sektorer, navnlig: bank- og finansieringsvirksomhed (91,1 %), energi (89,4 %), transport (81,7 %), sundhedsvæsen (89,4 %), internettjenester (89,1 %) og offentlige myndigheder (87,5 %). Respondenterne mente også, at hvis et krav om at anmelde NIS-sikkerhedsbrud til den nationale kompetente myndighed blev indført, bør dette fastsættes på EU-plan (65,1 %), og de bekræftede, at de offentlige myndigheder også bør være underlagt et sådant krav (93,5 %). Endelig bekræftede respondenterne, at et krav om at gennemføre NIS-risikostyring på det aktuelle tekniske stade ikke ville påføre dem væsentlige meromkostninger (63,4 %), og at et krav om at anmelde brud på sikkerheden ikke medfører væsentlige meromkostninger (72,3 %).

Medlemsstaterne blev hørt i en række relevante rådssammensætninger, inden for rammerne af det europæiske forum for medlemsstaterne (EFMS) på konferencen om cybersikkerhed organiseret af Kommissionen og EU-Udenrigstjenesten den 6. juli 2012 og på særlige bilaterale møder, som blev indkaldt på anmodning af individuelle medlemsstater.

Der blev også afholdt drøftelser med den private sektor under det europæiske offentlig-private partnerskab for en robust infrastruktur (EPR3)[22] og ved bilaterale møder. For så vidt angår den offentlige sektor, har Kommissionen afholdt drøftelser med ENISA og CERT for EU-institutionerne.

2.2. Konsekvensanalyse

Kommissionen har foretaget en konsekvensanalyse af følgende tre politiske løsninger:

Løsningsmodel 1: Fortsætte som hidtil (referencescenariet): bibeholde den nuværende tilgang

Løsningsmodel 2: En reguleringstilgang bestående af et lovforslag om fælles EU-regler for net- og informationssikkerhed hvad angår medlemsstaternes kapaciteter, mekanismer for samarbejde på EU-plan og krav til vigtige private aktører og offentlige myndigheder

Løsningsmodel 3: En blandet tilgang, som kombinerer frivillige initiativer vedrørende medlemsstaternes NIS-kapaciteter og mekanismer for samarbejde på EU-plan med de forskriftsmæssige krav til vigtige private aktører og offentlige myndigheder.

Kommissionen konkluderede, at løsningsmodel 2 vil have de største positive virkninger, da den i væsentlig grad vil øge beskyttelsen af EU's forbrugere, virksomheder og regeringer mod NIS-hændelser. Navnlig de forpligtelser, der pålægges medlemsstaterne, ville sikre tilstrækkeligt beredskab på nationalt plan og bidrage til et klima af gensidig tillid, som er en forudsætning for effektivt samarbejde på EU-plan. Oprettelsen af samarbejdsmekanismer på EU-plan via netværket ville give en sammenhængende og koordineret forebyggelse og reaktion på grænseoverskridende NIS-hændelser og -risici. Indførelsen af krav til at gennemføre NIS-risikostyring for offentlige myndigheder og vigtige private aktører ville skabe et stærkt incitament til en effektiv sikkerhedsrisikostyring. Forpligtelsen til at anmelde NIS-hændelser med en betydelig virkning vil øge mulighederne for at reagere over for hændelser og fremme gennemsigtighed. Ved at feje for sin egen dør vil EU desuden kunne få en større international gennemslagskraft og blive en endnu mere troværdig partner i forbindelse med bilateralt og multilateralt samarbejde. EU ville dermed være bedre rustet til at fremme de grundlæggende rettigheder og EU's centrale værdier i udlandet.

Den kvantitative vurdering viste, at model 2 ikke pålægger medlemsstaterne en uforholdsmæssig stor byrde. Omkostningerne for den private sektor vil også være begrænset, da mange af de berørte parter allerede skal opfylde gældende sikkerhedskrav (dvs. en forpligtelse for de registeransvarlige til at træffe tekniske og organisatoriske foranstaltninger

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

for at sikre personoplysninger, herunder NIS-foranstaltninger). Eksisterende udgifter til sikkerhed i den private sektor er også blevet taget i betragtning.

Dette forslag overholder de principper, der anerkendes i Den Europæiske Unions charter om grundlæggende rettigheder, navnlig retten til respekt for privatlivet og kommunikation, beskyttelsen af personoplysninger, frihed til at oprette og drive egen virksomhed, ejendomsretten og retten til effektive retsmidler for en domstol og ret til at blive hørt. Direktivet skal gennemføres i overensstemmelse med disse rettigheder og principper.

3. FORSLAGETS JURIDISKE ASPEKTER

3.1. Retsgrundlag

Den Europæiske Union har beføjelse til at vedtage foranstaltninger med henblik på at oprette eller sikre et velfungerende indre marked i overensstemmelse med de relevante bestemmelser i traktaterne (artikel 26 i traktaten om Den Europæiske Unions funktionsmåde (TEUF). Ifølge artikel 114 i TEUF, kan EU vedtage foranstaltninger med henblik på indbyrdes tilnærmelse af medlemsstaternes love og administrative bestemmelser, der vedrører det indre markeds oprettelse og funktion.

Som anført i det foregående er net og informationssystemer væsentlige for at fremme grænseoverskridende bevægelighed for varer, tjenesteydelser og personer. De er ofte indbyrdes forbundne, og internettet er i sig selv globalt. Denne givne transnationale dimension betyder, at en forstyrrelse af disse systemer i én medlemsstat kan berøre andre medlemsstater og EU som helhed. Net og informationssystemers robusthed og stabilitet er derfor afgørende for at opnå et velfungerende indre marked.

EU-lovgiveren har allerede erkendt behovet for at harmonisere NIS-regler for at sikre udviklingen af det indre marked. Dette gælder især for forordning 460/2004 om oprettelse af ENISA[23], som er baseret på artikel 114 i TEUF.

Forskellene som følge af uensartede nationale NIS-kapaciteter, -politikker og -beskyttelsesniveauer i de enkelte medlemsstater medfører hindringer for det indre marked og berettiger et EU-initiativ.

3.2. Subsidiaritet

En indsats på EU-plan inden for net- og informationssikkerhed er berettiget ud fra subsidiaritetsprincippet.

For det første vil manglende intervention på EU-plan på baggrund af net- og informationssikkerheds grænseoverskridende karakter føre til en situation, hvor de enkelte medlemsstater handler hver for sig og ikke tager hensyn til den indbyrdes afhængighed mellem EU's net og informationssystemer. En passende grad af samordning mellem medlemsstaterne ville kunne sikre, at NIS-risici tackles effektivt i den tværnationale sammenhæng, hvori de opstår. Forskelle i NIS-forskrifter er en hindring for virksomheder, der ønsker at drive virksomhed i flere lande, og for opnåelsen af globale stordriftsfordele.

For det andet er der behov for lovfæstede forpligtelser på EU-plan for at skabe lige vilkår og lukke huller i lovgivningen. En tilgang baseret på frivillighed har kun ført til samarbejde mellem et mindretal af medlemsstaterne med højt kapacitetsniveau. For at inddrage alle medlemsstaterne er det nødvendigt at sikre, at de alle har det krævede minimumskapacitetsniveau. NIS-foranstaltninger, der vedtages af det offentlige, skal være i

[23] Europa-Parlamentets og Rådets forordning (EF) nr. 460/2004 af 10. marts 2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed (EUT L 077 af 13.3.2004, s. 1).

overensstemmelse med hinanden og samordnes for at begrænse og mindske følgerne af NIS-hændelser. Inden for netværket vil de kompetente myndigheder og Kommissionen gennem en udveksling af bedste praksis og en vedvarende inddragelse af ENISA samarbejde om at fremme en konvergerende gennemførelse af direktivet i hele EU. Herudover kan en samordnet og samarbejdsorienteret NIS-politik have en stærkt positiv virkning, når det gælder en reel beskyttelse af grundlæggende rettigheder, herunder især retten til beskyttelse af personoplysninger og privatlivets fred. En indsats på EU-plan ville derfor gøre eksisterende nationale politikker mere effektive og lette deres videreudvikling.

De foreslåede foranstaltninger er også begrundet ud fra et proportionalitetssynspunkt. Kravene til medlemsstaterne er fastsat til det minimum, der er nødvendigt for at opnå et hensigtsmæssigt beredskab og for at muliggøre et samarbejde baseret på tillid. Det giver også medlemsstaterne mulighed for at tage behørigt hensyn til nationale forhold og sikrer, at de fælles EU-principper anvendes på en forholdsmæssig måde. Det brede anvendelsesområde gør, at medlemsstaterne kan gennemføre direktivet med udgangspunkt i de faktiske bestående risici på nationalt niveau, som er udpeget i den nationale NIS-strategi. Kravene om at indføre risikostyring er kun målrettet mod kritiske enheder og pålægger foranstaltninger, som står i et rimeligt forhold til risiciene. Den offentlige høring understregede betydningen af at garantere disse kritiske enheders sikkerhed. Indberetningskravene vil kun gælde hændelser med en væsentlig virkning. Som nævnt i det foregående, vil foranstaltningerne ikke medføre uforholdsmæssigt store omkostninger, da mange af disse enheder som registeransvarlige allerede er omfattet af de nuværende databeskyttelsesregler vedrørende personoplysninger.

For at undgå, at der pålægges små operatører, herunder navnlig SMV, uforholdsmæssigt store byrder, står kravene i rimeligt forhold til de risici, der udgøres af det pågældende net eller informationssystem og bør ikke gælde for mikrovirksomheder. Risiciene vil først skulle identificeres af de enheder, som forpligtelserne gælder for, og de vil skulle beslutte, hvilke foranstaltninger der skal vedtages for at afbøde sådanne risici.

De opstillede mål kan bedre nås på EU-plan end af medlemsstaterne alene på grund af de tværnationale aspekter af NIS-hændelser og -risici. EU kan derfor vedtage foranstaltninger i overensstemmelse med subsidiaritetsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet går dette direktiv ikke videre, end hvad der er nødvendigt for nå disse mål.

Med henblik på at nå målene bør Kommissionen have beføjelse til at vedtage delegerede retsakter, jf. artikel 290 i traktaten om Den Europæiske Unions funktionsmåde, der udbygger eller ændrer visse ikke-væsentlige bestemmelser i basisretsakten. Kommissionens forslag tilstræber også at understøtte forholdsmæssighed, når private og offentlige operatører pålægges forpligtelser.

For at sikre ensartede betingelser for gennemførelsen af basisretsakten, bør Kommissionen have beføjelse til at vedtage gennemførelsesretsakter i overensstemmelse med artikel 291 i traktaten om Den Europæiske Unions funktionsmåde.

Navnlig i betragtning af det brede anvendelsesområde for det foreslåede direktiv, at det vedrører stærkt regulerede områder, og de retlige forpligtelser, der afledes fra direktivets kapitel IV, bør meddelelsen af gennemførelsesforanstaltninger være ledsaget af forklarende dokumenter. I overensstemmelse med medlemsstaternes og Kommissionens fælles politiske erklæring om forklarende dokumenter af 28. september 2011 har medlemsstaterne forpligtet sig til i berettigede tilfælde at lade meddelelsen af deres gennemførelsesbestemmelser ledsage af et eller flere dokumenter, som forklarer forholdet mellem komponenterne i et direktiv og de tilsvarende dele af de nationale gennemførelsesinstrumenter. Med hensyn til dette direktiv finder lovgiveren, at fremsendelsen af sådanne dokumenter er begrundet.

4. VIRKNING FOR BUDGETTET

Samarbejde og informationsudveksling mellem medlemsstaterne bør understøttes af en sikret infrastruktur. Forslaget vil kun have virkninger for EU's budget, hvis medlemsstaterne vælger at tilpasse en bestående infrastruktur (f.eks. sTESTA) og ønsker, at Kommissionen skal gennemføre dette inden for den flerårige finansielle ramme for 2014-2020. Engangsudgiften anslås til 1 250 000 EUR og vil skulle afholdes over EU's budgetpost 09.03.02 (at fremme sammenkobling og interoperabilitet mellem de nationale offentlige online-tjenester samt adgangen til disse net — kapitel 09.03, Connecting Europe-faciliteten — telenet) på betingelse af, at faciliteten har tilstrækkelige midler hertil. Alternativt kan medlemsstaterne enten dele engangsudgiften til tilpasning af en bestående infrastruktur eller beslutte at oprette en ny infrastruktur og afholde omkostningerne, som skønnes at være ca. 10 mio. EUR pr. år.

2013/0027 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV

om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele EU

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR –

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[1],

efter høring af Den Europæiske Tilsynsførende for Databeskyttelse,

efter den almindelige lovgivningsprocedure og

ud fra følgende betragtninger:

(1) Net og informationssystemer og -tjenester spiller en afgørende rolle i samfundet. Det er af afgørende betydning for de økonomiske aktiviteter og den sociale velfærd og navnlig for et velfungerende indre marked, at de er pålidelige og sikre.

(2) Omfanget og hyppigheden af forsætlige eller utilsigtede sikkerhedshændelser er tiltagende og udgør en alvorlig trussel for driften af net og informationssystemer. Sådanne hændelser kan hindre gennemførelsen af økonomiske aktiviteter, medføre betydelige finansielle tab, underminere brugernes tillid og forårsage stor skade for Unionens økonomi.

(3) På grund af sin rolle som kommunikationsinstrument uden grænser spiller digitale informationssystemer og navnlig Internettet en væsentlig rolle, når det gælder at fremme grænseoverskridende bevægelighed for varer, tjenesteydelser og personer. På grund af den tværnationale karakter vil væsentlige forstyrrelser af sådanne systemer i én medlemsstat også kunne påvirke andre medlemsstater og Unionen som helhed. Net og informationssystemers robusthed og stabilitet er derfor afgørende for et velfungerende indre marked.

(4) Der bør etableres en samarbejdsmekanisme på EU-plan, som giver mulighed for informationsudveksling og koordineret detektering og reaktion i forbindelse med net- og informationssikkerhed (NIS). Hvis denne mekanisme skal være effektiv og inklusiv, er det vigtigt, at alle medlemsstater har et minimum af kapacitet og en strategi, der sikrer en høj grad af net- og informationssikkerhed på deres område. Der bør også gælde minimumssikkerhedskrav for de offentlige myndigheder og operatørerne af kritisk informationsinfrastruktur for at fremme en risikostyringskultur og sikre, at de mest alvorlige hændelser anmeldes.

[1] EUT C […] af […], s. […].

(5) For at dække alle relevante hændelser og risici bør dette direktiv gælde for alle net og informationssystemer. De forpligtelser, der pålægges offentlige myndigheder og markedsaktører bør dog ikke gælde for virksomheder, der udbyder offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, jf. direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet)[2], og som er undergivet specifikke sikkerheds- og integritetskrav, der er fastlagt i det pågældende direktivs artikel 13a, og de bør heller ikke gælde for tillidstjenesteudbydere.

(6) Den eksisterende kapacitet er ikke tilstrækkelig til at sikre et højt NIS-niveau i EU. Medlemsstaterne har meget forskellige beredskabsniveauer, hvilket giver en usammenhængende tilgang i EU som helhed. Det fører til et uensartet beskyttelsesniveau for forbrugere og virksomheder og undergraver det samlede NIS-niveau i EU. Manglende fælles minimumskrav til offentlige myndigheder og markedsaktører gør det også umuligt at iværksætte en overordnet og effektiv samarbejdsmekanisme på EU-plan.

(7) En effektiv reaktion på de sikkerhedsproblemer, der opstår i net og informationssystemer, forudsætter en samlet strategi på EU-plan, der omfatter fælles mindstekrav til kapacitetsopbygning og planlægning, udveksling af oplysninger og samordning af aktioner og fælles mindstesikkerhedskrav for alle berørte markedsaktører og offentlige myndigheder.

(8) Bestemmelserne i dette direktiv bør ikke være til hinder for, at hver medlemsstat kan træffe de nødvendige foranstaltninger for at sikre beskyttelsen af sine væsentlige sikkerhedsinteresser, af hensyn til den offentlige orden og sikkerhed og for at tillade efterforskning, detektering og retsforfølgelse af straffelovsovertrædelser. I henhold til artikel 346 i TEUF er ingen medlemsstat forpligtet til at meddele oplysninger, hvis udbredelse efter dens opfattelse ville stride mod dens væsentlige sikkerhedsinteresser.

(9) Hver medlemsstat bør have en national NIS-strategi, der fastlægger de strategiske mål og konkrete politiske foranstaltninger, der skal gennemføres for at nå og bibeholde et fælles højt NIS-niveau. Der bør udvikles NIS-samarbejdsplaner på nationalt plan, som opfylder de væsentlige krav, for at opnå et beredskabsniveau, der giver mulighed for et effektivt og velfungerende samarbejde nationalt og på EU-plan i tilfælde af hændelser.

(10) Med sigte på en effektiv gennemførelse af de bestemmelser, som vedtages i henhold til dette direktiv, bør der i hver medlemsstat oprettes eller udpeges et organ, som har til opgave at koordinere net- og informationssikkerhed og fungere som kontaktpunkt i forbindelse med grænseoverskridende samarbejde på EU-niveau. Disse organer bør have tilstrækkelige tekniske, finansielle og menneskelige ressourcer til at sikre, at de på en effektiv og virksom måde kan udføre de opgaver, som de pålægges, og dermed opfylde målene i dette direktiv.

(11) Alle medlemsstater bør være udstyret med passende teknisk og organisatorisk kapacitet, til at forebygge, detektere, reagere på og afhjælpe NIS-hændelser og -risici. Der bør derfor oprettes velfungerende it-beredskabsenheder (CERT), som opfylder de væsentlige krav, i alle medlemsstater for at sikre en effektiv og kompatibel kapacitet, der kan reagere på hændelser og risici og sikre et effektivt samarbejde på EU-plan.

(12) Med udgangspunkt i de betydelige fremskridt inden for det europæiske forum for medlemsstaterne (EFMS) med at fremme drøftelser og udvekslinger om god politisk

[2] EFT L 108 af 24.4.2002, s. 33.

praksis, herunder udvikling af principper for et europæisk cyberkrisesamarbejde, bør medlemsstaterne og Kommissionen etablere et permanent kommunikationsnetværk og støtte deres samarbejde. Denne sikre og effektive samarbejdsmekanisme burde muliggøre en struktureret og koordineret informationsudveksling, detektering og indsats på EU-plan.

(13) Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) bør bistå medlemsstaterne og Kommissionen med ekspertise og rådgivning og ved at fremme udveksling af bedste praksis. Kommissionen bør navnlig rådføre sig med ENISA for så vidt angår anvendelsen af dette direktiv. For at sikre effektiv og rettidig information til medlemsstaterne og Kommissionen bør der udsendes tidlig varsling om hændelser og risici via samarbejdsnetværket. Med sigte på opbygning af kapacitet og viden blandt medlemsstaterne bør samarbejdsnetværket også fungere som et redskab til udveksling af bedste praksis til støtte for medlemmernes arbejde med kapacitetsopbygning, styring af tilrettelæggelse af peer reviews og NIS-øvelser.

(14) Der bør oprettes en sikret infrastruktur til informationsudveksling for at give mulighed for udveksling af følsomme og fortrolige oplysninger inden for samarbejdsnetværket. Uden at dette berører medlemsstaternes pligt til at anmelde hændelser og risici med en EU-dimension til samarbejdsnetværket, bør adgangen til fortrolige oplysninger fra andre medlemsstater kun gives til de medlemsstater, der påviser, at deres tekniske, finansielle og menneskelige ressourcer og procedurer såvel som deres kommunikationsinfrastruktur garanterer deres effektive, virksomme og sikre deltagelse i netværket.

(15) Da de fleste net og informationssystemer er privatejede, er samarbejde mellem den offentlige og private sektor afgørende. Markedsaktørerne bør tilskyndes til at benytte deres egne uformelle samarbejdsmekanismer for at sikre net- og informationssikkerheden. De bør også samarbejde med den offentlige sektor og udveksle oplysninger og bedste praksis i udvekslingen af operationel støtte i tilfælde af hændelser.

(16) For at sikre gennemsigtighed og informere EU-borgerne og markedsaktørerne korrekt bør de kompetente myndigheder etablere et fælles websted, hvor der offentliggøres ikke-fortrolige oplysninger om hændelser og risici.

(17) Hvis oplysningerne betragtes som fortrolige i overensstemmelse med EU's regler og nationale regler om forretningshemmeligheder, skal denne fortrolighed sikres under udførelsen af aktiviteterne og opfyldelsen af målene i dette direktiv.

(18) På grundlag af bl.a. nationale erfaringer med krisestyring og i samarbejde med ENISA bør Kommissionen og medlemsstaterne udvikle en EU-samarbejdsplan for net- og informationssikkerhed, som fastsætter samarbejdsmekanismer til imødegåelse af risici og hændelser. Der bør tages behørigt hensyn til denne plan i forbindelse med tidlig varsling via samarbejdsnetværket.

(19) Udsendelse af en tidlig varsling inden for netværket bør kun finde sted, hvis den pågældende hændelse eller risiko kan nå et så væsentligt omfang eller blive så alvorlig, at der er behov for oplysninger eller samordning af indsatsen på EU-plan. Tidlige varslinger bør derfor begrænses til de faktiske eller potentielle hændelser eller risici, som hurtigt eskalerer, overstiger den nationale beredskabskapacitet eller berører mere end én medlemsstat. Alle oplysninger, der er relevante for vurderingen af en risiko eller hændelse bør meddeles samarbejdsnetværket, så der kan foretages en korrekt evaluering.

(20) Ved modtagelse af en tidlig varsling og vurderingen heraf bør de kompetente myndigheder enes om en samordnet indsats i henhold til EU's NIS-samarbejdsplan. De kompetente myndigheder og Kommissionen bør underrettes om de foranstaltninger, der er vedtaget på nationalt plan som følge af den samordnede indsats.

(21) I betragtning af NIS-problemernes globale karakter er der behov for et tættere internationalt samarbejde om at forbedre sikkerhedsstandarderne og informationsudvekslingen og for at fremme en fælles global tilgang til NIS-problemstillinger.

(22) Ansvaret for at sikre net- og informationssikkerheden ligger i vid udstrækning hos de offentlige myndigheder og markedsaktørerne. En risikostyringskultur med risikovurdering og gennemførelse af sikkerhedsforanstaltninger, som er passende i forhold til risiciene, bør fremmes og udvikles gennem passende forskriftsmæssige krav og en frivillig indsats fra industriens side. Etablering af lige vilkår er også afgørende for et velfungerende samarbejdsnetværk, så man sikrer et effektivt samarbejde fra alle medlemsstater.

(23) I direktiv 2002/21/EF fastsættes det, at de virksomheder, der udbyder offentligt tilgængelige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, skal træffe passende foranstaltninger til at beskytte deres integritet og sikkerhed, og direktivet indfører desuden anmeldelsespligt for brud på sikkerheden og integritetstab. I henhold til Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation)[3] skal udbydere af offentligt tilgængelige elektroniske kommunikationstjenester træffer passende tekniske og organisatoriske foranstaltninger til at beskytte deres tjenester.

(24) Disse forpligtelser bør udvides til ud over den elektroniske kommunikationssektor også at gælde for vigtige udbydere af informationssamfundstjenester som defineret i direktiv 98/34/EF af 22. juni 1998 om en informationsprocedure med hensyn til tekniske standarder og forskrifter samt forskrifter for informationssamfundets tjenester[4], som er grundlaget for efterfølgende informationssamfundstjenester og onlineaktiviteter, f.eks. e-handelsplatforme, internetbetalingsportaler, sociale netværk, søgemaskiner, cloud computing-tjenester og applikationsforhandlere. En forstyrrelse af disse informationssamfundshjælpetjenester medfører at andre af informationssamfundets tjenester, som er afhængige af dem som vigtige input, ikke kan fungere. Softwareudviklere og hardwarefabrikanter udbyder ikke informationssamfundstjenester og er derfor ikke omfattet. Forpligtelserne bør udvides til også at omfatte offentlige myndigheder og operatører af kritisk infrastruktur, som er stærkt afhængige af informations- og kommunikationsteknologi, og som er af afgørende betydning for opretholdelsen af vigtige økonomiske eller samfundsmæssige funktioner som f.eks. elektricitet og gas, transport, kreditinstitutter, fondsbørser og sundhedssektoren. En forstyrrelse af disse net og informationssystemer vil påvirke det indre marked.

(25) Tekniske og organisatoriske foranstaltninger, der pålægges offentlige myndigheder og markedsaktører, bør ikke kræve, at et bestemt kommercielt informations- og kommunikationsteknologiprodukt konstrueres, udvikles eller fremstilles på en bestemt måde.

---

[3] EFT L 201 af 31.7.2002, s. 37.

[4] EFT L 204 af 21.7.1998, s. 37.

(26) De offentlige myndigheder og markedsaktørerne bør sikre beskyttelsen af net og systemer, der er under deres kontrol. Det vil hovedsageligt være private net og systemer, hvor administrationen varetages af deres eget it-personale, eller hvor sikkerhedsopgaverne er outsourcet. Sikkerheds- og anmeldelsesforpligtelserne bør gælde for de relevante markedsaktører og offentlige myndigheder, uanset om de selv står for vedligeholdelsen af deres net og informationssystemer eller outsourcer denne opgave.

(27) Med sigte på at undgå, at mindre operatører og brugere pålægges en uforholdsmæssig stor finansiel og administrativ byrde, bør kravene stå i et rimeligt forhold til den risiko, der er forbundet med det pågældende net eller informationssystem, under hensyntagen til sådanne foranstaltningers aktuelle stade. Kravene bør ikke gælde for mikrovirksomheder.

(28) De kompetente myndigheder bør tage behørigt hensyn til nødvendigheden af at bevare uformelle og pålidelige kanaler til informationsudveksling mellem markedsaktørerne og mellem den offentlige og den private sektor. Ved offentliggørelse af hændelser, der anmeldes til de kompetente myndigheder, bør der foretages en nøje afvejning af offentlighedens interesse i at blive informeret om trusler i forhold til mulige imageskader og kommercielle skader for de offentlige myndigheder og markedsoperatører, der anmelder hændelser. Ved gennemførelsen af anmeldelsespligten bør de kompetente myndigheder være særlig opmærksomme på behovet for at holde oplysninger om produkters sårbarhed strengt fortrolige, indtil der udsendes passende sikkerhedsopdateringer.

(29) Kompetente myndigheder bør have de nødvendige midler til at varetage deres opgaver, herunder beføjelser til at indhente tilstrækkelige oplysninger fra markedsaktører og offentlige myndigheder til at kunne vurdere sikkerhedsniveauet i net og informationssystemer samt pålidelige og omfattende oplysninger om faktiske hændelser, der har påvirket driften af net og informationssystemer.

(30) Kriminelle aktiviteter er i mange tilfælde grunden til en hændelse. Der kan være mistanke om, at en hændelse har en kriminel baggrund, også selv om det ikke står tilstrækkeligt klart fra begyndelsen. I denne forbindelse bør et passende samarbejde mellem de kompetente myndigheder og de retshåndhævende myndigheder være et led i en effektiv og omfattende indsats mod sikkerhedsrelaterede hændelser. Hvis et sikkert, beskyttet og mere robust miljø skal fremmes, kræver det en systematisk anmeldelse af hændelser af en formodet alvorlig kriminel karakter til de retshåndhævende myndigheder. Den alvorlige kriminelle karakter af hændelser bør vurderes på baggrund af EU's lovgivning om bekæmpelse af cyberkriminalitet.

(31) Personoplysninger er i mange tilfælde kompromitteret som følge af hændelser. De kompetente myndigheder og databeskyttelsesmyndighederne bør i denne forbindelse samarbejde og udveksle oplysninger om alle relevante spørgsmål for at håndtere brud på sikkerheden af personoplysninger som følge af hændelser. Medlemsstaterne gennemfører forpligtelsen til at anmelde sikkerhedsrelaterede hændelser på en måde, der reducerer den administrative byrde, hvis en sikkerhedsrelateret hændelse er også er et brud på persondatasikkerheden i henhold til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger[5]. Ved at fungere som forbindelsesled mellem de kompetente myndigheder og databeskyttelsesmyndighederne kan ENISA bidrage til at udvikle

[5] SEK(2012) 72 endelig.

informationsudvekslingsmekanismer og -skabeloner, så det ikke er nødvendigt med to forskellige udformninger af skabelonerne til anmeldelse. Denne fælles anmeldelsesskabelon gør det nemmere at anmelde hændelser, hvor der er sket brud på sikkerheden i forbindelse med personoplysninger, og letter derved den administrative byrde for virksomhederne og de offentlige myndigheder.

(32) Standardisering af sikkerhedskrav er en markedsstyret proces. Medlemsstaterne bør for at sikre en konvergerende anvendelse af sikkerhedsstandarder tilskynde til overholdelse af eller overensstemmelse med specificerede standarder for at sikre et højt sikkerhedsniveau på EU-plan. Med dette mål for øje kan det være nødvendigt at udarbejde udkast til harmoniserede standarder, som bør udformes i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF[6].

(33) Kommissionen bør regelmæssigt tage dette direktivs bestemmelser op til fornyet overvejelse, særlig med henblik på at afgøre, om der er behov for ændringer i lyset af skiftende teknologiske betingelser og markedsvilkår.

(34) Hvis samarbejdsnetværket skal kunne fungere korrekt, bør beføjelserne til at vedtage retsakter i overensstemmelse med artikel 290 i traktaten om Den Europæiske Unions funktionsmåde delegeres til Kommissionen for så vidt angår definitionen af de kriterier, der skal være opfyldt for, at en medlemsstat kan få tilladelse til at deltage i det sikrede informationsudvekslingssystem, den nærmere fastlæggelse af begivenheder, som skal udløse tidlig varsling, og definition af, hvornår markedsoperatører og offentlige myndigheder er forpligtet til at anmelde hændelser.

(35) Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau. Kommissionen bør i forbindelse med forberedelsen og udarbejdelsen af delegerede retsakter sørge for samtidig, rettidig og hensigtsmæssig fremsendelse af relevante dokumenter til Europa-Parlamentet og Rådet.

(36) For at sikre ensartede betingelser for gennemførelsen af dette direktiv bør gennemførelsesbeføjelser overdrages til Kommissionen for så vidt angår samarbejdet mellem de kompetente myndigheder og Kommissionen inden for samarbejdsnetværket, adgangen til den sikrede informationsudvekslingsinfrastruktur, EU's NIS-samarbejdsplan, formater og procedurer til informering af offentligheden om hændelser og standarder og/eller tekniske specifikationer, der er relevante for net- og informationssikkerhed. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser[7].

(37) I forbindelse med anvendelsen af dette direktiv bør Kommissionen i det nødvendige omfang varetage kontakten med relevante sektorudvalg og relevante organer på EU-niveau, herunder navnlig inden for områderne energi, transport og sundhed.

---

6 EUT L 316 af 14.11.2012, s. 12.

7 EUT L 55 af 28.2.2011, s. 13.

(38) Oplysninger, der betragtes som fortrolige af en kompetent myndighed i henhold til EU-regler og nationale regler om forretningshemmeligheder, bør kun udveksles med Kommissionen og andre kompetente myndigheder, hvis det er strengt nødvendigt for anvendelsen af dette direktiv. Udveksling af oplysninger bør kun ske i det omfang, det er relevant, og omfanget bør står i et rimeligt forhold til formålet med udvekslingen.

(39) Udveksling af information om risici og hændelser i samarbejdsnetværket og overholdelse af kravet om anmeldelse af hændelser til de nationale kompetente myndigheder kan kræve behandling af personoplysninger. En sådan behandling af personoplysninger er nødvendig for at opfylde de mål af almen interesse, der forfølges med dette direktiv, og er dermed er berettiget i henhold til artikel 7 i direktiv 95/46/EF. Den udgør derfor ikke i forhold til disse legitime mål et uforholdsmæssigt og uacceptabelt indgreb, der krænker selve kernen i retten til beskyttelse af personoplysninger, der er sikret ved artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder. I forbindelse med anvendelsen af dette direktiv bør Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter[8] finde anvendelse i nødvendigt omfang. Når oplysningerne behandles af EU-institutioner og -organer, bør en sådan behandling som led i gennemførelsen af dette direktiv ske i overensstemmelse med forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger.

(40) Målet for dette direktiv, nemlig at sikre et højt niveau af net- og informationssikkerhed i Unionen, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne alene og kan derfor på grund af handlingens omfang eller virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går direktivet ikke ud over, hvad der er nødvendigt for at nå disse mål.

(41) Dette forslag overholder de grundlæggende rettigheder og de principper, der anerkendes i Den Europæiske Unions charter om grundlæggende rettigheder, herunder navnlig retten til respekt for privatlivet og kommunikation, beskyttelsen af personoplysninger, frihed til at oprette og drive egen virksomhed, ejendomsretten og retten til effektive retsmidler for en domstol og ret til at blive hørt. Direktivet skal gennemføres i overensstemmelse med disse rettigheder og principper —

VEDTAGET DETTE DIREKTIV:

[8] EFT L 145 af 31.5.2001, s. 43.

KAPITEL I

GENERELLE BESTEMMELSER

Artikel 1

Genstand og anvendelsesområde

1. Dette direktiv fastsætter foranstaltninger til sikring af et højt fælles niveau for net- og informationssikkerhed (i det følgende benævnt "NIS") i Den Europæiske Union.

2. Direktivet:

(a) fastsætter forpligtelser for alle medlemsstater vedrørende forebyggelse, håndtering af og reaktion på risici og hændelser, der berører net og informationssystemer

(b) etablerer en samarbejdsmekanisme mellem medlemsstaterne for at sikre en ensartet anvendelse af dette direktiv i Unionen og om nødvendigt en koordineret og effektiv håndtering af og reaktion på risici og hændelser, der berører net og informationssystemer

(c) fastsætter sikkerhedskrav for markedsoperatører og offentlige myndigheder.

3. De sikkerhedskrav, der er fastsat i artikel 14, gælder ikke for virksomheder, der udbyder offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, jf. direktiv 2002/21/EF, som er omfattet af de specifikke sikkerheds- og integritetskrav, der er fastsat i det pågældende direktivs artikel 13a og 13b, og de gælder heller ikke for tillidstjenesteudbydere.

4. Dette direktiv berører ikke EU's lovgivning om cyberkriminalitet og Rådets direktiv 2008/114/EF af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den[9].

5. Dette direktiv berører heller ikke Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger[10] og heller ikke Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og heller ikke Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger[11].

6. Udvekslingen af information inden for samarbejdsnetværket, jf. kapitel III, og anmeldelsen af NIS-hændelser, jf. artikel 14, kan kræve behandling af personoplysninger. En sådan behandling, som er nødvendig for at nå målene i den offentlige interesse, der forfølges ved dette direktiv, godkendes af medlemsstaten i henhold til artikel 7 i direktiv 95/46/EF og direktiv 2002/58/EF som gennemført i den nationale lovgivning.

---

9 EUT L 345 af 23.12.2008, s. 75.

10 EFT L 281 af 23.11.1995, s. 31.

11 SEC(2012) 72 final.

Artikel 2

Minimumsharmonisering

Medlemsstaterne er ikke afskåret fra at vedtage eller bibeholde bestemmelser, der sikrer et højere sikkerhedsniveau, idet dette dog ikke berører deres forpligtelser i henhold til EU-lovgivningen.

Artikel 3

Definitioner

I dette direktiv forstås ved:

(1) "net og informationssystem":

(a) et elektronisk kommunikationsnet som omhandlet i direktiv 2002/21/EF og

(b) enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede enheder, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af edb-data, samt

(c) edb-data, som lagres, behandles, fremfindes eller overføres af elementer i litra a) og b) i forbindelse med deres drift, brug, beskyttelse og vedligeholdelse

(2) "sikkerhed": et nets eller et informationssystems evne til, på et givet tillidsniveau, at modstå uheld, ulovlige handlinger og handlinger i ond hensigt, der er til skade for disponibiliteten, autenticiteten, integriteten og fortroligheden i forbindelse med arkiverede og overførte data og de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via dette net eller system

(3) "risiko": enhver omstændighed eller begivenhed, der har en potentiel negativ indvirkning på sikkerheden

(4) "hændelse": enhver omstændighed eller begivenhed, der har en faktisk negativ indvirkning på sikkerheden

(5) "informationssamfundstjeneste": tjenesteydelser som omhandlet i artikel 1, nr. 2, i direktiv 98/34/EF

(6) "NIS-samarbejdsplan": en plan, som fastlægger rammerne for organisatoriske roller, ansvarsområder og procedurer for at opretholde eller genoprette funktionen af net og informationssystemer i tilfælde af en risiko eller en hændelse, der berører dem

(7) "håndtering af hændelser": alle procedurer til analyse og begrænsning af samt reaktion på en hændelse

(8) "markedsoperatør":

(a) en leverandør af informationssamfundstjenester, som gør det muligt at levere andre informationssamfundstjenester; en ikke-udtømmende liste findes i bilag II

(b) en operatør af kritisk infrastruktur, der er af afgørende betydning for opretholdelsen af centrale økonomiske og samfundsmæssige aktiviteter på områderne energi, transport, bankvæsen, børser og sundhed; en ikke-udtømmende liste findes i bilag II

(9) "standard": en standard som omhandlet i forordning (EU) nr. 1025/2012

(10) "specifikation": en specifikation som omhandlet i forordning (EU) nr. 1025/2012

(11) "tillidstjenesteudbyder": enhver fysisk eller juridisk person, som udbyder en hvilken som helst elektronisk tjeneste, der omfatter generering, verificering, validering, håndtering og bevaring af elektroniske signaturer, elektroniske segl, elektroniske tidsstempler, elektroniske dokumenter, elektroniske leveringstjenester, webstedsautentifikation og elektroniske certifikater, herunder certifikater for elektroniske signaturer og elektroniske segl.

KAPITEL II

NATIONALE RAMMER FOR NET- OG INFORMATIONSSIKKERHED

Artikel 4

Princip

Medlemsstaterne sikrer et højt sikkerhedsniveau for net og informationssystemer på deres område i overensstemmelse med dette direktiv.

Artikel 5

Nationale NIS-strategier og nationale NIS-samarbejdsplaner

1. Hver medlemsstat vedtager en national NIS-strategi, der fastlægger de strategiske mål og konkrete politiske og lovgivningsmæssige foranstaltninger med henblik på at nå og opretholde et højt niveau for net- og informationssikkerhed. De nationale NIS-strategier skal navnlig omfatte:

(a) fastsættelse af strategiens mål og prioriterede områder med udgangspunkt i en ajourført risikovurderings- og hændelsesanalyse

(b) styringsmæssige rammer for at nå de strategiske mål og prioriteringer, herunder en klar definition af roller og ansvar for de statslige organer og andre relevante aktører

(c) fastlæggelse af de generelle foranstaltninger vedrørende beredskab, indsats og genopretning, herunder mekanismer for samarbejde mellem den offentlige og den private sektor

(d) en angivelse af teoretiske og praktiske uddannelsesprogrammer og oplysningsprogrammer

(e) forsknings- og udviklingsplaner og en beskrivelse af, hvordan disse planer afspejler de fastlagte prioriteter

2. Den nationale NIS-strategi skal omfatte en national NIS-samarbejdsplan, som mindst omfatter

(f) en risikovurderingsplan til brug ved identifikation af risici og vurdering af potentielle begivenheders konsekvenser

(g) definition af roller og ansvarsområder for de forskellige aktører, der er involveret i planens gennemførelse

(h) definition af samarbejds- og kommunikationsprocesser, som sikrer forebyggelse, detektion, reaktion, reparation og genopretning, og moduleret i forhold til alarmniveauet

(i) en køreplan for NIS-øvelser og praktisk uddannelse for at styrke, validere og teste planen. Høstede erfaringer dokumenteres og indarbejdes i ajourføringer af planen.

3. De nationale NIS-strategier og de nationale NIS-samarbejdsplaner fremsendes til Kommissionen senest en måned efter deres vedtagelse.

Artikel 6

Nationale kompetente myndigheder for net og informationssystemer

4. Hver medlemsstat udpeger en national kompetent myndighed for sikkerheden af net og informationssystemer (i det følgende benævnt "kompetent myndighed").

5. De kompetente myndigheder overvåger anvendelsen af dette direktiv på nationalt plan og bidrager til en konsekvent anvendelse i hele EU.

6. Medlemsstaterne sikrer, at de kompetente myndigheder har tilstrækkelige tekniske, finansielle og menneskelige ressourcer til på en effektiv og virksom måde at udføre de opgaver, de pålægges, og dermed opfylde målene i dette direktiv. Medlemsstaterne sikrer et effektivt, virksomt og sikkert samarbejde mellem de kompetente myndigheder via det netværk, der er omhandlet i artikel 8.

7. Medlemsstaterne sikrer, at de kompetente myndigheder modtager anmeldelser af hændelser fra de offentlige myndigheder og markedsaktørerne som fastsat i artikel 14, stk. 2, og overdrages de gennemførelses- og håndhævelsesbeføjelser, der er omhandlet i artikel 15.

8. De kompetente myndigheder konsulterer og samarbejder, hvor det er hensigtsmæssigt, med de relevante retshåndhævende nationale myndigheder og databeskyttelsesmyndigheder.

9. Hver medlemsstat underretter straks Kommissionen om udpegelsen af den kompetente myndighed, dens opgaver og enhver senere ændring heraf. Hver medlemsstat offentliggør sin udpegelse af den kompetente myndighed.

Artikel 7

It-beredskabsenhed (CERT)

10. Hver medlemsstat opretter en it-beredskabsenhed, som er ansvarlig for at håndtere hændelser og risici i henhold til en nøje fastlagt proces, der skal opfylde kravene i bilag I, punkt 1. En it-beredskabsenhed kan oprettes som en del af den kompetente myndighed.

11. Medlemsstaterne sikrer, at sådanne enheder har passende tekniske, finansielle og menneskelige ressourcer til at udføre deres opgaver, som er fastlagt i bilag I, punkt 2.

12. Medlemsstaterne sikrer, at it-beredskabsenheden kan benytte sikker og robust kommunikations- og informationsinfrastruktur på nationalt plan, som skal være kompatibel og interoperabel med det sikrede informationsudvekslingssystem, der er omhandlet i artikel 9.

13. Medlemsstaterne underretter Kommissionen om it-beredskabenhedens ressourcer, mandat og procedurer for håndtering af hændelser.

14. It-beredskabsenheden handler under tilsyn af den kompetente myndighed, som regelmæssigt foretager en vurdering af tilstrækkeligheden af it-beredskabsenhedens ressourcer og mandat og af effektiviteten af dens procedurer for håndtering af hændelser.

KAPITEL III

SAMARBEJDE MELLEM KOMPETENTE MYNDIGHEDER

Artikel 8

Samarbejdsnetværk

15. De kompetente myndigheder og Kommissionen opretter et netværk ("samarbejdsnetværk") med henblik på at samarbejde om indsatsen mod risici og hændelser i forbindelse med net og informationssystemer.

16. Samarbejdsnetværket etablerer en permanent kommunikationsforbindelse mellem Kommissionen og de kompetente myndigheder. På anmodning bistår Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) samarbejdsnetværket med sin ekspertise og rådgivning.

17. Inden for samarbejdsnetværket skal de kompetente myndigheder:

(a) rundsende tidlige varslinger om risici og hændelser, jf. artikel 10

(b) sikre en samordnet reaktion, jf. artikel 11

(c) med jævne mellemrum offentliggøre ikke-fortrolige oplysninger om igangværende tidlige varslinger og samordnede reaktioner på en fælles hjemmeside

(d) på anmodning af en medlemsstat eller Kommissionen i fællesskab drøfte og evaluere en eller flere af de i artikel 5 omhandlede nationale NIS-strategier og nationale NIS-samarbejdsplaner inden for dette direktivs anvendelsesområde

(e) på anmodning af en medlemsstat eller af Kommissionen i fællesskab drøfte og evaluere effektiviteten af it-beredskabsenhederne, herunder navnlig i forbindelse med gennemførelsen af NIS-øvelser på EU-plan

(f) samarbejde og udveksle oplysninger om alle relevante emner med Europol's europæiske center for bekæmpelse af cyberkriminalitet og med andre relevante europæiske organer, herunder navnlig på områderne databeskyttelse, energi, transport, bankvæsen, børser og sundhed

(g) udveksle oplysninger og bedste praksis med hinanden og Kommissionen og bistå hinanden med at opbygge NIS-kapacitet

(h) gennemføre regelmæssige peer reviews af kapacitet og beredskab

(i) gennemføre NIS-øvelser på EU-plan og deltage i internationale NIS-øvelser i det nødvendige omfang.

18. Kommissionen fastsætter ved hjælp af gennemførelsesretsakter de nødvendige modaliteter for at lette samarbejdet mellem de kompetente myndigheder og Kommissionen, jf. stk. 2 og 3. Disse gennemførelsesretsakter vedtages efter rådgivningsproceduren i artikel 19, stk. 2.

Artikel 9

Sikret informationsudvekslingssystem

19. Udveksling af følsomme og fortrolige oplysninger i samarbejdsnetværket skal ske via en sikret infrastruktur.

20. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i henhold til artikel 18 for så vidt angår definition af de kriterier, der skal være opfyldt for, at en medlemsstat kan få adgang til at deltage i det sikrede informationsudvekslingssystem, herunder:

(j) der skal være en sikker og robust national kommunikations- og informationsinfrastruktur, som er kompatibel og interoperabel med samarbejdsnetværkets sikrede infrastruktur, jf. artikel 7, stk. 3, og

(k) medlemsstatens kompetente myndighed og it-beredskabsenhed skal have tilstrækkelige tekniske, finansielle og menneskelige ressourcer og procedurer til en effektiv, virksom og sikker deltagelse i det sikrede informationsudvekslingssystem, jf. artikel 6, stk. 3, artikel 7, stk. 2, og artikel 7, stk. 3.

21. Kommissionen vedtager ved hjælp af gennemførelsesretsakter afgørelser om medlemsstaternes adgang til den sikrede infrastruktur i henhold til de i stk. 2 og 3 omhandlede kriterier. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 19, stk. 3.

Artikel 10
Tidlig varsling

22. De kompetente myndigheder eller Kommissionen rundsender tidlige varslinger i samarbejdsnetværket om risici og hændelser, der opfylder mindst én af følgende betingelser:

(l) de eskalerer hurtigt eller kan hurtigt eskalere

(m) de overstiger eller kan overstige den nationale reaktionskapacitet

(n) de påvirker eller kan påvirke mere end én medlemsstat.

23. I forbindelse med tidlige varslinger meddeler de kompetente myndigheder og Kommissionen alle relevante oplysninger i deres besiddelse, som kan være nyttige ved vurderingen af risikoen eller hændelsen.

24. På anmodning af en medlemsstat eller på eget initiativ kan Kommissionen anmode en medlemsstat om at fremlægge alle relevante oplysninger vedrørende en specifik risiko eller hændelse.

25. Hvis risikoen eller hændelsen formodes at være af kriminel karakter, underretter de kompetente myndigheder eller Kommissionen Europol's europæiske center for bekæmpelse af cyberkriminalitet.

26. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 18 for så vidt angår yderligere specifikation af risici og hændelser, der udløser en tidlig varsling som omhandlet i stk. 1.

Artikel 11
Samordnet indsats

27. Efter en tidlig varsling som omhandlet i artikel 10 skal de kompetente myndigheder, når de har vurderet de relevante oplysninger, enes om en samordnet indsats i overensstemmelse med EU's NIS-samarbejdsplan, der er omhandlet i artikel 12.

28. De forskellige foranstaltninger, der vedtages på nationalt plan som følge af den samordnede indsats, meddeles samarbejdsnetværket.

Artikel 12

EU's NIS-samarbejdsplan

29. Kommissionen tillægges beføjelser til ved hjælp af gennemførelsesretsakter at vedtage en NIS-samarbejdsplan for Unionen. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 19, stk. 3.

30. EU's NIS-samarbejdsplan skal indeholde:

(o) i forbindelse med artikel 10:

– en definition af formatet og procedurerne for de kompetente myndigheders indsamling og deling af forenelige og sammenlignelige oplysninger om risici og hændelser

– en definition af procedurerne og kriterierne for samarbejdsnetværkets vurdering af risici og hændelser

(p) de procedurer, der skal følges i forbindelse med den samordnede indsats i medfør af artikel 11, herunder identifikation af roller og ansvarsområder samt samarbejdsprocedurer

(q) en køreplan for NIS-øvelser og praktisk uddannelse for at styrke, validere og teste planen

(r) et program for videnoverførsel mellem medlemsstaterne til brug ved kapacitetsopbygning og peer learning

(s) et program til gensidig oplysning og uddannelse medlemsstaterne imellem.

31. EU's NIS-samarbejdsplan vedtages senest et år efter dette direktivs ikrafttræden og tages regelmæssigt op til fornyet overvejelse.

Artikel 13

Internationalt samarbejde

Uden at det berører samarbejdsnetværkets muligheder for at iværksætte uformelt internationalt samarbejde, kan Unionen indgå internationale aftaler med tredjelande eller internationale organisationer, som giver disse mulighed for og tilrettelægger deres deltagelse i nogle af samarbejdsnetværkets aktiviteter. En sådan aftale skal tage hensyn til behovet for at sikre tilstrækkelig beskyttelse af de personoplysninger, der rundsendes i samarbejdsnetværket.

KAPITEL IV

OFFENTLIGE MYNDIGHEDERS OG MARKEDSAKTØRERS NET- OG INFORMATIONSSYSTEMSIKKERHED

Artikel 14

Sikkerhedskrav og anmeldelse af hændelser

32. Medlemsstaterne sikrer, at de offentlige myndigheder og markedsaktørerne træffer passende tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net og informationssystemer, som de kontrollerer og anvender til deres aktiviteter. Under hensyntagen til teknologiens aktuelle stade skal disse foranstaltninger garantere et sikkerhedsniveau, der står i forhold til risikoen. Der skal navnlig træffes foranstaltninger for at forhindre og minimere virkningen af hændelser, der berører deres net og informationssystem for de centrale tjenester, de leverer, og dermed sikre kontinuiteten af de tjenester, der understøttes af disse net og informationssystemer.

33. Medlemsstaterne sikrer, at de offentlige myndigheder og markedsaktørerne foretager en anmeldelse til den kompetente myndighed af hændelser, der har en betydelig indvirkning på sikkerheden af de centrale tjenester, de leverer.

34. Kravene i stk. 1 og 2 finder anvendelse på alle markedsoperatører, som leverer tjenester i Den Europæiske Union.

35. Den kompetente myndighed kan underrette offentligheden eller kræve, at de offentlige myndigheder og markedsaktørerne gør det, hvis den beslutter, at offentliggørelse af hændelsen er i offentlighedens interesse. En gang om året forelægger den kompetente myndighed en sammenfattende rapport for samarbejdsnetværket om de anmeldelser, den har modtaget, og de foranstaltninger, der er truffet i henhold til dette stykke.

36. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 18 for så vidt angår definition af tilfælde, hvor offentlige myndigheder og markedsaktører er forpligtet til at anmelde hændelser.

37. Med forbehold af enhver delegeret retsakt, der er vedtaget i henhold til stk. 5, kan de kompetente myndigheder vedtage retningslinjer og om nødvendigt udstede instrukser om de omstændigheder, hvorunder de offentlige myndigheder og markedsaktører har pligt til at anmelde hændelser.

38. Kommissionen kan ved hjælp af gennemførelsesretsakter fastlægge vilkår, formater og procedurer for gennemførelsen af stk. 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 19, stk. 3.

39. Stk. 1 og 2 gælder ikke for mikrovirksomheder som defineret i Kommissionens anbefaling nr. 2003/361/EF af 6. maj 2003 vedrørende definition af mikro-, små og mellemstore virksomheder[12].

[12] EUT L 124 af 20.5.2003, s. 36.

Artikel 15

Gennemførelse og håndhævelse

40. Medlemsstaterne sikrer, at de kompetente myndigheder har de nødvendige beføjelser til at undersøge tilfælde af offentlige myndigheders og markedsaktørers manglende opfyldelse af deres forpligtelser i henhold til artikel 14 og virkningerne heraf for net og informationssystemers sikkerhed.

41. Medlemsstaterne sikrer, at de kompetente myndigheder har beføjelse til at pålægge markedsaktørerne og offentlige myndigheder at:

(t) forelægge de oplysninger, der nødvendige for at vurdere sikkerheden af deres net og informationssystemer, herunder en dokumenteret sikkerhedspolitik

(u) underkaste sig en sikkerhedsaudit udført af et kvalificeret uafhængigt organ eller en national myndighed og stille resultaterne heraf til rådighed for den kompetente myndighed.

42. Medlemsstaterne sikrer, at de kompetente myndigheder har beføjelse til at udstede bindende instrukser til markedsaktørerne og de offentlige myndigheder.

43. De kompetente myndigheder anmelder hændelser af formodet alvorlig kriminel karakter til de retshåndhævende myndigheder.

44. De kompetente myndigheder indgår i et tæt samarbejde med persondatabeskyttelsesmyndigheder, når de håndterer hændelser, som medfører brud på persondatasikkerheden.

45. Medlemsstaterne sikrer, at alle forpligtelser, der pålægges offentlige myndigheder og markedsaktører i medfør af dette kapitel, kan indbringes for domstolene.

Artikel 16

Standardisering

46. For at sikre en konvergerende anvendelse af artikel 14, stk. 1, tilskynder medlemsstaterne til at benytte standarder og/eller specifikationer, der er relevante for net- og informationssikkerhed.

47. Kommissionen opstiller ved hjælp af gennemførelsesretsakter en liste over de standarder, der er nævnt i stk. 1. Listen offentliggøres i Den Europæiske Unions Tidende .

KAPITEL V

AFSLUTTENDE BESTEMMELSER

Artikel 17

Sanktioner

48. Medlemsstaterne fastsætter regler om sanktioner for overtrædelse af de nationale bestemmelser, der er vedtaget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger til at sikre håndhævelsen heraf. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsernes grovhed og have afskrækkende virkning. Medlemsstaterne giver senest på datoen for dette direktivs gennemførelse i national

lovgivning Kommissionen meddelelse om disse bestemmelser og meddeler omgående senere ændringer af betydning for bestemmelserne.

49. Medlemsstaterne sikrer, når en sikkerhedsrelateret hændelse omfatter personoplysninger, at de påtænkte sanktioner er forenelige med de sanktioner, der er fastsat i forordningen fra Europa-Parlamentet og Rådet om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger[13].

Artikel 18

Udøvelse af de delegerede beføjelser

50. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.

51. Beføjelsen til at vedtage delegerede retsakter, der er omhandlet i artikel 9, stk. 2, artikel 10, stk. 5, og artikel 14, stk. 5, tillægges Kommissionen. Kommissionen udarbejder en rapport vedrørende delegationen af beføjelser senest ni måneder inden udløbet af femårsperioden. Delegationen af beføjelser forlænges stiltiende for perioder af samme varighed, medmindre Europa-Parlamentet eller Rådet modsætter sig en sådan forlængelse senest tre måneder inden udløbet af hver periode.

52. De delegerede beføjelser i artikel 9, stk. 2, artikel 10, stk. 5, og artikel 14, stk. 5, kan til enhver tid tilbagekaldes af Europa-Parlamentet eller af Rådet. En afgørelse om tilbagekaldelse bringer delegationen af beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning fra dagen efter offentliggørelsen i Den Europæiske Unions Tidende eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

53. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidig Europa-Parlamentet og Rådet meddelelse herom.

54. En delegeret retsakt vedtaget i henhold til artikel 9, stk. 2, artikel 10, stk. 5, og artikel 14, stk. 5, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret Kommissionen om, at de ikke agter at gøre indsigelse. Denne frist forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 19

Udvalgsprocedure

55. Kommissionen bistås af et udvalg ("Udvalget for Net- og Informationssikkerhed"). Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.

56. Når der henvises til dette stykke, finder artikel 4 i forordning (EU) nr. 182/2011 anvendelse.

57. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

[13] SEC(2012) 72 final

Artikel 20

Revision

Kommissionen tager regelmæssigt dette direktivs funktion op til revision og forelægger en rapport for Europa-Parlamentet og Rådet. Den første rapport forelægges senest tre år efter gennemførelsesdatoen i artikel 21. Kommissionen kan med henblik herpå anmode medlemsstaterne om hurtigst muligt at fremsende oplysninger.

Artikel 21

Gennemførelse

58. Medlemsstaterne vedtager og offentliggør senest den [et og et halvt år efter vedtagelsen] de love og administrative bestemmelser, der er nødvendige for at efterkomme dette direktiv. De meddeler straks Kommissionen teksten til disse love og bestemmelser.

    Medlemsstaterne anvender disse bestemmelser fra [et og et halvt år efter vedtagelsen].

    Disse love og bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for henvisningen fastsættes af medlemsstaterne.

59. Medlemsstaterne meddeler Kommissionen teksten til de vigtigste nationale bestemmelser, som de udsteder på det område, der er omfattet af dette direktiv.

Artikel 22

Ikrafttræden

Dette direktiv træder i kraft på [tyvendedagen] efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Artikel 23

Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den […].

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*

BILAG I

Krav til it-beredskabsenheden (CERT) og enhedens opgaver

Kravene til it-beredskabsenheden og enhedens opgaver skal være tilstrækkeligt og klart defineret og understøttet af national politik og/eller relevante forskrifter. De skal omfatte følgende elementer:

(12) Krav til it-beredskabsenheden

(a) It-beredskabsenheden skal sikre omfattende disponibilitet for sine kommunikationstjenester ved at undgå svage punkter og have flere midler til at blive kontaktet og til at kontakte andre. Desuden skal kommunikationskanalerne være tydeligt angivet og kendt af andre it-beredskabsenheder og samarbejdspartnere.

(b) It-beredskabsenheden skal gennemføre og administrere sikkerhedsforanstaltninger, der har til formål at sikre fortroligheden, integriteten, disponibiliteten og autenticiteten af oplysninger, som enheden modtager og behandler.

(c) It-beredskabsenhedens kontorer og de underliggende informationssystemer skal være placeret i sikrede områder.

(d) Der oprettes et service management-kvalitetssystem for at følge op på it-beredskabsenhedens resultater og sikre løbende forbedringer af processer. Det skal være baseret på klart definerede måleenheder, der omfatter formelle serviceniveauer og vigtige resultatindikatorer.

(e) Driftskontinuitet:

- It-beredskabsenheden skal være udstyret med et passende system til at administrere og videresende anmodninger, så overdragelser lettes
- It-beredskabsenheden skal have tilstrækkeligt personale til at sikre disponibilitet døgnet rundt
- It-beredskabsenheden råder over en infrastruktur, hvis driftskontinuitet er sikret. Med dette mål for øje etableres der redundante systemer og backup-arbejdsområder til it-beredskabsenheden for at sikre en permanent adgang til kommunikationsmidlerne.

(13) It-beredskabsenhedens opgaver

(a) It-beredskabsenhedens opgaver omfatter som minimum:

- overvågning af hændelser på nationalt plan
- tidlig varsling, advarsler, meddelelser og formidling af information til berørte parter om risici og hændelser
- håndtering af hændelser
- dynamiske risiko- og hændelsesanalyser og situationsrapporter
- bred offentlig oplysning om risiciene i forbindelse med onlineaktiviteter
- tilrettelæggelse af NIS-kampagner

(b) It-beredskabsenheden skal etablere et samarbejde med den private sektor.

(c) For at lette samarbejdet fremmer it-beredskabsenheden vedtagelse og anvendelse af fælles eller standardiseret praksis for:

- procedurer for håndtering af hændelser og risici
- systemer til klassificering af hændelser, risici og oplysninger
- taksonomier for måleenheder
- formater for informationsudveksling risici, hændelser og navngivningskonventioner for systemer.

BILAG II

Liste over markedsaktører

Jf. artikel 3, stk. 8, litra a):

1. E-handelsplatforme

2. Internetbetalingsportaler

3. Sociale netværk

4. Søgemaskiner

5. Cloud computing-tjenester

6. Applikationsforhandlere

Jf. artikel 3, stk. 8, litra b):

1. Energi

- el- og gasleverandører
- operatører af el- og/eller gasdistributionssystemer og detailhandlere, der levere til endelige forbrugere
- operatører af naturgastransmissionssystemer, operatører af naturgaslagre og LNG-operatører
- operatører af el-transmissionssystemer
- olierørledninger og olielagre
- operatører på el- og gasmarkedet
- operatører af olie- og gasproduktion, raffinaderier og behandlingsanlæg

2. Transport

- luftfartsselskaber (gods og passagerer)
- søtransport (virksomheder som udfører passagertransport og/eller godstransport i højsøfarvand eller kystnært farvand)
- jernbaner (infrastrukturforvaltere, integrerede selskaber og jernbanetransportvirksomheder)
- lufthavne
- havne
- trafikledelses- og kontroloperatører
- logistiske hjælpetjenester (a) opbevaring og oplagring, b) lasthåndtering og c) andre hjælpetjenester i forbindelse med transport)

3. Bankvæsen: kreditinstitutioner i henhold til artikel 4, stk. 1, i direktiv 2006/48/EF.

4. Finansmarkedsinfrastrukturer: børser og centrale modpartsclearingcentraler.

5. Sundhedssektoren: sundhedstjenestemiljøer (herunder hospitaler og private klinikker) og andre organisationer, der leverer sundhedstjenester.

LEGISLATIVE FINANCIAL STATEMENT

1. 1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

Forslag til Europa-Parlamentets og Rådets direktiv om foranstaltninger, der skal sikre et højt fælles niveau af net- og informationssikkerhed i hele EU.

1.2. Berørt politikområde inden for ABM/ABB-strukturen[37]

- 09 – Kommunikationsnet, indhold og teknologi

1.3. Forslagets/initiativets art

☒ Forslaget/initiativet drejer sig om en **ny foranstaltning**

☐ Forslaget/initiativet drejer sig om **en ny foranstaltning som opfølgning på et pilotprojekt/en forberedende foranstaltning**[38]

☐ Forslaget/initiativet drejer sig om **forlængelse af en eksisterende foranstaltning**

☐ Forslaget/initiativet drejer sig om **omlægning af en foranstaltning til en ny foranstaltning**

1.4. Mål

1.4.1. Det eller de af Kommissionens flerårige strategiske mål, som forslaget/initiativet vedrører

Sigtet med det foreslåede direktiv er at sikre et højt fælles niveau for net- og informationssikkerhed (NIS) i hele EU.

1.4.2. Specifikke mål og berørte ABM/ABB-aktiviteter

I forslaget fastlægges der foranstaltninger, der skal sikre et højt fælles niveau af net- og informationssikkerhed i hele EU

De specifikke mål er:

1. At indføre et minimumsniveau for NIS i medlemsstaterne og dermed øge det generelle beredskabs- og indsatsniveau.

2. At forbedre NIS-samarbejdet på EU-plan med henblik på at imødegå grænseoverskridende hændelser og trusler effektivt. Der vil blive oprettet en sikker infrastruktur til informationsudveksling for at give mulighed for udveksling af følsomme og fortrolige oplysninger mellem de kompetente myndigheder.

3. At skabe en risikostyringskultur og forbedre udvekslingen af oplysninger mellem den private og offentlige sektor.

Berørte ABM/ABB-aktiviteter

Direktivet omfatter enheder (virksomheder og organisationer, herunder visse SMV'er) i en række sektorer (energi, transport, kreditinstitutioner og børser, sundhedspleje og katalysatorer af centrale internettjenester) samt offentlige myndigheder. Det omhandler forbindelserne med retshåndhævelse og databeskyttelse og NIS-aspekter inden for rammerne af de eksterne forbindelser.

- 09 – Kommunikationsnet, indhold og teknologi

- 02 - Erhvervspolitik

[37] ABM: Activity Based Management (aktivitetsbaseret ledelse) ABB: Activity Based Budgeting (aktivitetsbaseret budgettering).

[38] Jf. artikel 49, stk. 6, litra a) eller b), i finansforordningen.

- 32 - Energi
- 06 - Mobilitet og transport
- 17 - Sundhed og forbrugerbeskyttelse
- 18 – Indre anliggender
- 19 – Eksterne forbindelser
- 33 - Retlige anliggender
- 12- Indre marked

1.4.3. Forventede resultater og virkninger

Angiv, hvilke virkninger forslaget/initiativet forventes at få for modtagerne/målgruppen.

Beskyttelsen af EU's forbrugere, virksomheder og offentlige myndigheder mod NIS-hændelser, -trusler og -risici vil blive væsentligt forbedret.

Yderligere oplysninger findes i afsnit 8.2 (Virkningerne af løsningsmodel 2 – Reguleringstilgang) i konsekvensanalysen i det arbejdsdokument fra Kommissionens tjenestegrene, der ledsager dette forslag.

1.4.4. Virknings- og resultatindikatorer

Angiv indikatorerne til kontrol af forslagets/initiativets gennemførelse.

Indikatorerne for overvågning og evaluering er angivet i afsnit 10 i konsekvensanalysen.

1.5. Forslagets/initiativets begrundelse

1.5.1. Behov, der skal opfyldes på kort eller lang sigt

Hver enkelt medlemsstat vil skulle have:

- en national NIS-strategi
- en NIS-samarbejdsplan
- en NIS-kompetent national myndighed og
- et it-beredskabsenhed (Computer Emergency Response Team - CERT)

På EU-plan vil medlemsstaterne skulle samarbejde via et netværk.

Offentlige forvaltninger og centrale private aktører ville skulle foretage NIS-risikostyring og underrette de kompetente myndigheder NIS-hændelser med en betydelig virkning.

1.5.2. Merværdien ved en indsats fra EU's side

Da NIS er grænseoverskridende, udgør forskellene mellem de relevante lovgivninger og politikker en hindring for virksomhedernes muligheder for at drive virksomhed i flere lande og opnå globale stordriftsfordele. Hvis der ikke sættes ind på EU-plan, vil der opstå en situation, hvor de enkelte medlemsstater handler hver for sig uden hensyntagen til den indbyrdes afhængighed mellem net og informationssystemer.

Målene kan derfor bedre opfyldes gennem en indsats på EU-plan, snarere end af medlemsstaterne alene.

1.5.3. Erfaringer fra lignende foranstaltninger

Forslaget udspringer af den analyse, at det er nødvendigt med forskriftsmæssige forpligtelser til at skabe lige vilkår og lukke visse huller i lovgivningen. På dette område har en tilgang, der er baseret på frivillighed, ført til, at der kun finder samarbejde sted mellem et mindretal af medlemsstaterne med højt kapacitetsniveau.

1.5.4. Sammenhæng med andre relevante instrumenter og eventuel synergivirkning

Forslaget er i fuld overensstemmelse med den digitale dagsorden for Europa og derfor med EU's 2020-strategi. Det er også i overensstemmelse med og supplerer EU's regelsæt for elektronisk kommunikation, EU-direktivet om europæisk kritisk infrastruktur og EU-direktivet om databeskyttelse.

Forslaget ledsager og er et afgørende element i meddelelsen fra Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik om den europæiske strategi for cybersikkerhed.

1.6. Varighed og finansielle virkninger

– ☐ Forslag/initiativ af begrænset varighed

– ☐ Forslag/initiativ gældende fra [DD/MM]ÅÅÅÅ til [DD/MM]ÅÅÅÅ

– ☐ Finansielle virkninger fra ÅÅÅÅ til ÅÅÅÅ

– ☒ Forslag/initiativ af ubegrænset varighed

– Gennemførelsesperioden begynder umiddelbart efter vedtagelsen (efter planen i 2015) og vil vare 18 måneder. Gennemførelsen af direktivet vil dog starte efter vedtagelsen og vil medføre etablering af en sikker infrastruktur, der skal støtte medlemsstaternes samarbejde.

– derefter gennemførelse i fuldt omfang.

1.7. Påtænkte forvaltningsmetoder[39]

– ☒ Direkte central forvaltning ved Kommissionen

– ☒ Indirekte central forvaltning ved uddelegering af gennemførelsesopgaver til:

– ☐forvaltningsorganer

– ☒ organer oprettet af Fællesskaberne[40]

– ☐ nationale offentligretlige organer/organer med offentlige tjenesteydelsesopgaver

– ☐ personer, som har fået pålagt at gennemføre specifikke aktioner i henhold til afsnit V i traktaten om Den Europæiske Union, og som er identificeret i den relevante basisretsakt, jf. finansforordningens artikel 49

– ☐ Delt forvaltning sammen med medlemsstaterne

– ☐ Decentral forvaltning sammen med tredjelande

– ☐ Fælles forvaltning sammen med internationale organisationer, herunder Den Europæiske Rumorganisation

Hvis der angives flere forvaltningsmetoder, gives der en nærmere forklaring i afsnittet "Bemærkninger".

Bemærkninger:

ENISA, som er et decentralt organ, der er oprettet af Fællesskaberne, kan bistå medlemsstaterne og Kommissionen med at gennemføre direktivet på grundlag af sit mandat og ved den omfordeling af ressourcer af midler, der under FFR for 2014-2020 er forudset til dette organ.

[39] Forklaringer vedrørende forvaltningsmetoder og referencer ti finansforordningen findes på webstedet BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] Organer omhandlet i finansforordningens artikel 185.

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om kontrol og rapportering

Angiv hyppighed og betingelser:

Kommissionen vil med jævne mellemrum vurdere, hvordan direktivet fungerer, og aflægge rapport til Europa-Parlamentet og Rådet.

Kommissionen vil også vurdere, om medlemsstaterne gennemfører direktivet korrekt.

CEF-forslaget åbner ligeledes mulighed for at evaluere den metode, der er benyttet til at gennemføre de pågældende projekter, og virkningen af deres gennemførelse, således at det kan bedømmes, om de fastsatte mål, herunder miljøbeskyttelsesmål, er opfyldt.

2.2. Forvaltnings- og kontrolsystem

2.2.1. Konstaterede risici

- Forsinkelser i projektgennemførelsen i forbindelse med opbygningen af sikker infrastruktur

2.2.2. Påtænkte kontrolmetoder

Aftalerne og beslutningerne om gennemførelse af foranstaltningerne under CEF vil indeholde bestemmelser om tilsyn og finanskontrol, der gennemføres af Kommissionen eller af en bemyndiget repræsentant for Kommissionen, samt om revision, der gennemføres af Revisionsretten, og kontrol på stedet, der foretages af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF).

2.2.3. Omkostninger og fordele ved kontrollen og omfanget af sandsynlig misligholdelse

Gennem risikobaseret forudgående og efterfølgende kontrol og mulighed for revision på stedet vil det blive sikret, at omkostningerne ved kontrollen er rimelige.

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

Angiv eksisterende eller påtænkte forebyggelses- og beskyttelsesforanstaltninger.

I forbindelse med gennemførelsen af aktiviteter, som finansieres under dette direktiv, træffer Kommissionen passende foranstaltninger til at sikre, at Unionens finansielle interesser beskyttes ved hjælp af foranstaltninger til forebyggelse af svig, bestikkelse og andre ulovlige aktiviteter, ved hjælp af effektiv kontrol og, såfremt der konstateres uregelmæssigheder, ved hjælp af inddrivelse af de uretmæssigt udbetalte beløb og efter omstændighederne ved hjælp af sanktioner, der skal være effektive, stå i rimeligt forhold til overtrædelsens grovhed og have en afskrækkende virkning.

Kommissionen eller dennes repræsentanter og Revisionsretten har beføjelse til at foretage dokumentrevision og revision på stedet for alle støttemodtagere, kontrahenter eller underkontrahenter og tredjeparter, som har modtaget EU-midler under programmet.

Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) har beføjelse til at foretage kontrol på stedet hos erhvervsvirksomheder, der direkte eller indirekte er berørt af en sådan finansiering, efter bestemmelserne i forordning (Euratom, EF) nr. 2185/96 for at fastslå, om der foreligger svig, korruption eller anden ulovlig aktivitet, der berører

EU's finansielle interesser i forbindelse med en tilskudsaftale eller -afgørelse eller en kontrakt vedrørende EU-finansiering.

Samarbejdsaftaler med tredjelande og internationale organisationer, aftaler om tilskud, afgørelser om ydelse af tilskud og kontrakter som følge af gennemførelsen af denne forordning skal udtrykkeligt give Kommissionen, Revisionsretten og OLAF beføjelse til at foretage denne kontrol og inspektion på stedet; denne bestemmelse berører ikke stk. 1, 2 og 3.

CEF omfatter bestemmelser om, at aftaler om tilskud og indkøb skal være baseret på standardmodeller, som vil indeholde de foranstaltninger mod svig, der almindeligvis gælder.

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1. Berørt(e) udgiftspost(er) i budgettet og udgiftsområde(r) i den flerårige finansielle ramme

- Eksisterende udgiftsposter på budgettet

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne

Udgifts-område i den flerårige finansielle ramme	Budgetpost	Udgiftens art	Bidrag			
	Nummer [Betegnelse ……...…….]	OB/IOB (41)	fra EFTA-lande[42]	fra kandidat-lande[43]	fra tredje-lande	iht. finansforordning¬ens artikel 18, stk. 1, litra aa)
	09 03 02 Fremme af sammenkobling og interoperabilitet mellem de nationale offentlige onlinetjenester samt adgang til disse net.	OB	NEJ	NEJ	NEJ	NEJ

- Nye budgetposter, som der er søgt om (ikke relevant)

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne

Udgifts-område i den flerårige finansielle ramme	Budgetpost	Udgiftens art	Bidrag			
	Nummer [Udgiftsområde …….……..]	OB/IOB	fra EFTA-lande	fra kandidat-lande	fra tredje-lande	iht. finansforordning¬ens artikel 18, stk. 1, litra aa)
	[XX.YY.YY.YY]		JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ

41 OB = opdelte bevillinger/IOB = ikke-opdelte bevillinger.

42 EFTA: Den Europæiske Frihandelssammenslutning.

43 Kandidatlande og, efter omstændighederne, potentielle kandidatlande på Vestbalkan.

3.2. Anslåede virkninger for udgifterne

3.2.1. Sammenfatning af de anslåede virkninger for udgifterne

i mio. EUR (3 decimaler)

Udgiftsområde i den flerårige finansielle ramme	1	Intelligent og inklusiv vækst

GD: <…….>			2015* [44]	År **2016**	År **2017**	År **2018**	Efterfølgende år (2019-2021) og derefter			**I ALT**
• Aktionsbevillinger										
09 03 02	Forpligtelser	(1)	1,250**	0,000						**1,250**
	Betalinger	(2)	0,750	0,250	0,250					**1,250**
Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer[45]			**0.000**							**0,000**
Budgetpostens nummer		(3)	**0,000**							**0,000**
Bevillinger I ALT til GD <…….>	Forpligtelser	=1+1a +3	1,250	0,000						**1,250**
	Betalinger	=2+2a +3	0,750	0,250	0,250					**1,250**

• Aktionsbevillinger I ALT	Forpligtelser	(4)	1,250	0,000						**1,250**
	Betalinger	(5)	0,750	0,250	0,250					**1,250**

[44] År N er det år, hvor gennemførelsen af forslaget/initiativet begynder.

[45] Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller aktioner (tidligere BA-poster), indirekte forskning, direkte forskning.

• Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer I ALT		(6)	**0.000**							
Bevillinger I ALT under UDGIFTSOMRÅDE 1 i den flerårige finansielle ramme	Forpligtelser	=4+ 6	1,250	0,000						**1,250**
	Betalinger	=5+ 6	0,750	0,250	0,250					**1,250**

* Det præcise tidspunkt afhænger af, hvornår forslaget vedtages af den lovgivende myndighed (dvs. hvis direktivet godkendes i løbet af 2014, starter tilpasningen af en eksisterende infrastruktur i 2015, og ellers et år senere).

** Hvis medlemsstaterne vælger at benytte en eksisterende infrastruktur og at dække engangsomkostningerne til tilpasning under EU-budgettet, jf. punkt 1.4.3 og 1.7, anslås omkostningerne til tilpasning af et netværk til støtte for samarbejdet mellem medlemsstaterne i henhold til direktivets kapitel III (tidlig varsling, samordnet indsats osv.) til 1 250 000 EUR. Dette beløb er en smule højere end det, der er anført i konsekvensanalysen (”ca. 1 million EUR”), da det er baseret på et mere præcist skøn over de nødvendige elementer i en sådan infrastruktur. De nødvendige elementer og de dermed forbundne omkostninger er baseret på en vurdering foretaget af JRC på grundlag af dets erfaring med at udvikle lignende systemer for andre områder som f.eks. folkesundhed, og vil omfatte følgende: Et system for hurtig varsling og underretning for NIS (275 000 EUR); en platform for informationsudveksling (400 000 EUR); et system for tidlig varsling og indsats (275 000 EUR); et situationsrum (300 000 EUR) for et samlet beløb på 1 250 000 EUR. Der forventes at foreligge en mere detaljeret gennemførelsesplan i forbindelse med den kommende gennemførlighedsundersøgelse under den specifikke SMART-kontrakt 2012/0010: ”Gennemførlighedsundersøgelse og forberedelser i forbindelse med gennemførelsen af et europæisk system for tidlig varsling og indsats mod cyberangreb og forstyrrelser".

Hvis flere udgiftsområder påvirkes af forslaget/initiativet:

• Aktionsbevillinger I ALT	Forpligtelser	(4)	0,000	0,000						
	Betalinger	(5)	0,000	0,000						
• Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer I ALT		(6)	**0.000**	**0,000**						
Bevillinger I ALT under UDGIFTSOMRÅDE 1-4 i den flerårige finansielle ramme (referencebeløb)	Forpligtelser	=4+ 6	1,250	0,000						1.250
	Betalinger	=5+ 6	0,750	0,250	0,250					1.250

Udgiftsområde i den flerårige finansielle ramme	**5**	"Administration"

i mio. EUR (3 decimaler)

		År **2015**	År **2016**	År **2017**	År **2018**	Efterfølgende år (2019-2021) og derefter			**I ALT**
GD: CNECT									
• Menneskelige ressourcer		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Andre administrationsudgifter		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
I ALT GD CNECT	Bevillinger	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5.430**

Bevillinger I ALT under UDGIFTSOMRÅDE 5 i den flerårige finansielle ramme	(Forpligtelser i alt = betalinger i alt)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5.430**

i mio. EUR (3 decimaler)

		År **2015**[46]	År **2016**	År **2017**	År **2018**	Efterfølgende år (2019-2021) og derefter			**I ALT**
Bevillinger I ALT under UDGIFTSOMRÅDE 1-5 i den flerårige finansielle ramme	Forpligtelser	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6.680**
	Betalinger	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6.680**

[46] År n er det år, hvor gennemførelsen af forslaget/initiativet begynder.

3.2.2. Anslåede virkninger for aktionsbevillingerne

– ☐ Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

– ☑ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

– Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Der angives mål og resultater ⇩			År **2015***		År **2016**		År **2017**		År **2018**		Efterfølgende år (2019-2021) og derefter						**I ALT**	
	RESULTATER																	
	Type resultater[47]	Resultaternes gnsntl. omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Samlede resultater (antal)	Samlede omkost-ninger
SPECIFIKT MÅL NR. 2[48] Sikret infrastruktur til informationsudveksling																		
- Resultat	Tilpasning af infrastruktur																	
Subtotal for specifikt mål nr. 2			1	1,250**													1	1,250
OMKOSTNINGER I ALT				1,250														1,250

47 Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

48 Som beskrevet i del 1.4.2., "Specifikke mål …"

* Det præcise tidspunkt afhænger af, hvornår forslaget vedtages af den lovgivende myndighed (dvs. hvis direktivet godkendes i løbet af 2014, starter tilpasningen af en eksisterende infrastruktur i 2015, og ellers et år senere).

***Se punkt 3.2.1

3.2.3. Anslåede virkninger for administrationsbevillingerne

3.2.3.1. **Resumé**

– ☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

– ☑ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (3 decimaler)

	År **2015**[49]	År **2016**	År **2017**	År **2018**	Efterfølgende år (2019-2021) og derefter			**I ALT**
UDGIFTSOMRÅDE 5 i den flerårige finansielle ramme								
Menneskelige ressourcer	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Andre administrationsudgifter	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Subtotal UDGIFTSOMRÅDE 5 i den flerårige finansielle ramme	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
Uden for UDGIFTSOMRÅDE 5[50] **i den flerårige finansielle ramme**								
Menneskelige ressourcer	0,000	0,000						**0.000**
Andre administrationsudgifter								
Subtotal uden for UDGIFTSOMRÅDE 5 i den flerårige finansielle ramme	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
I ALT	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Administrationsbevillingerne vil blive dækket ved hjælp af de bevillinger, som GD CNECT allerede har afsat til forvaltningen af aktionen, og/eller ved GD'ets omfordeling, hvortil kommer de eventuelle yderligere bevillinger, som tildeles det ansvarlige GD i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

[49] År n er det år, hvor gennemførelsen af forslaget/initiativet begynder.

[50] Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller aktioner (tidligere BA-poster), indirekte forskning, direkte forskning.

Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) vil kunne bistå medlemsstaterne og Kommissionen med at gennemføre direktivet på grundlag af dets mandat og ved omfordeling af ressourcerne under FFR for 2014-2020 til dette agentur, dvs. uden tildeling af yderligere budgetmæssige og menneskelige ressourcer.

3.2.3.2. Anslået behov for menneskelige ressourcer

– ☐ Forslaget/initiativet medfører ikke anvendelse af menneskelige ressourcer

– ☑ Forslaget/initiativet medfører anvendelse af menneskelige ressourcer i Kommissionen som anført nedenfor:

I princippet er der ikke behov for yderligere menneskelige ressourcer. Personalebehovet vil være meget begrænset og vil blive dækket af medarbejdere fra det GD, som allerede er udpeget til at varetage forvaltningen af foranstaltningen.

Overslag angives i hele tal (eller med højst én decimal)

		År **2015**	År **2016**	År **2017**	År **2018**	Efterfølgende år (2019-2021) og derefter		
• Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)								
09 01 01 01 (i hovedsædet og i Kommissionens repræsentationskontorer)		4	4	4	4	4	4	4
XX 01 01 02 (i delegationerne)								
XX 01 05 01 (indirekte forskning)								
10 01 05 01 (direkte forskning)								
• Eksternt personale (i fuldtidsækvivalenter)[51]								
09 01 02 01 (KA, V, UNE under den samlede bevillingsramme)		1	1	1	1	1	1	1
XX 01 02 02 (KA, V, UED, LA og UNE i delegationerne)								
XX 01 04 ***yy***[52]	- i hovedsædet							
	- i delegationerne							

[51] KA: kontraktansatte, V: vikarer, UED: unge eksperter ved delegationerne, LA: lokalt ansatte, UNE: udstationerede nationale eksperter.

[52] Delloft for eksternt personale under aktionsbevillingerne (tidligere BA-poster).

	gationerne							
XX 01 05 02 (KA, V, UNE – indirekte forskning)								
10 01 05 02 (KA, V, UNE - direkte forskning)								
Andre budgetposter (skal angives)								
I ALT		**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX angiver det berørte politikområde eller budgetafsnit.

Personalebehovet vil blive dækket ved hjælp af det personale, som GD CNECT allerede har afsat til aktionen, og/eller interne rokader i GD'et, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige GD i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) vil kunne bistå medlemsstaterne og Kommissionen med at gennemføre direktivet på grundlag af dets nuværende mandat og ved omfordeling af ressourcerne under FFR for 2014-2020 til dette agentur, dvs. uden tildeling af yderligere budgetmæssige og menneskelige ressourcer.

Opgavebeskrivelse:

Tjenestemænd og midlertidigt ansatte	- Forberedelse af delegerede retsakter i henhold til artikel 14, stk. 3 - Forberedelse af gennemførelsesretsakter i henhold til artikel 8, artikel 9, stk. 2, artikel 12, artikel 14, stk. 5, artikel 16 - Bidrag til samarbejde via netværket, både på politisk og operationelt plan. - Deltagelse i internationale drøftelser og eventuelt indgåelse af internationale aftaler
Eksternt personale	Støtte til ovenstående opgaver efter behov.

3.2.4. Forenelighed med indeværende flerårige finansielle ramme

– ☑ Forslaget/initiativet er foreneligt med indeværende flerårige finansielle ramme

– ☐ Forslaget/initiativet kræver omlægning af det relevante udgiftsområde i den flerårige finansielle ramme

Forslaget vil få de anslåede finansielle virkninger, hvis medlemsstaterne vælger at tilpasse eksisterende infrastruktur og anmoder Kommissionen om at gennemføre en tilpasning af den i henhold til den flerårige finansielle ramme for 2014-2020. Den dertil knyttede engangsomkostning vil være omfattet af CEF på betingelse af, at der er tilstrækkeligt midler til rådighed. Alternativt kan medlemsstaterne dele omkostningerne ved tilpasningen af infrastrukturen eller omkostningerne ved etableringen af en ny infrastruktur.

– ☐ Forslaget/initiativet kræver, at fleksibilitetsinstrumentet anvendes, eller at den flerårige finansielle ramme revideres[53].

Ikke relevant.

3.2.5. Tredjemands bidrag til finansieringen

– Forslaget/initiativet indeholder ikke bestemmelser om samfinansiering med tredjemand.

3.3. Anslåede virkninger for indtægterne

– ☑ Forslaget/initiativet har ingen finansielle virkninger for indtægterne

[53] Jf. punkt 19 og 24 i den interinstitutionelle aftale.