EUROPESE
COMMISSIE

Brussel, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Voorstel voor een

RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD

houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen

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

TOELICHTING

Doel van de voorgestelde richtlijn is het waarborgen van een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging (NIB). Dit betekent dat de beveiliging van het Internet en de particuliere netwerken en informatiesystemen die de werking van onze samenleving en economie ondersteunen, moet worden verbeterd. Dit doel kan worden bereikt door de lidstaten ertoe te verplichten hun paraatheid te verbeteren en beter met elkaar samen te werken, en door zowel exploitanten van kritieke infrastructuur (voor, onder meer, energie en transport) als essentiële aanbieders van informatiemaatschappijdiensten (zoals platforms voor elektronische handel en sociale netwerken) en overheden ertoe te verplichten adequate maatregelen te nemen om beveiligingsrisico's te beheren en ernstige incidenten aan de nationale bevoegde autoriteiten te rapporteren.

Dit voorstel wordt gepresenteerd samen met de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid over een Europese strategie voor cyberbeveiliging. Doel van de strategie is een beveiligde en betrouwbare digitale omgeving te waarborgen en tegelijkertijd de grondrechten en andere essentiële waarden van de EU te bevorderen en te beschermen. Dit voorstel vormt de kernactie van de strategie. Andere acties in het kader van de strategie op dit gebied zijn gericht op bewustmaking, ontwikkeling van een interne markt voor cyberbeveiligingsproducten en -diensten en bevordering van investeringen in O&O. Deze acties zullen worden aangevuld door weer andere acties voor het intensiveren van de bestrijding van cybercriminaliteit en het ontwikkelen van een internationaal cyberbeveiligingsbeleid voor de EU.

1.1. Motivering en doel van het voorstel

NIB wordt steeds belangrijker voor onze economie en onze samenleving. Bovendien is het onmogelijk om een betrouwbare omgeving voor de wereldwijde handel in diensten te creëren zonder NIB. Toch kunnen informatiesystemen te lijden krijgen van beveiligingsincidenten, zoals menselijke fouten, natuurgerelateerde omstandigheden, technisch falen of kwaadwillige aanvallen. Dergelijke incidenten nemen toe in omvang, frequentie en complexiteit. Uit de openbare online-raadpleging van de Commissie over het verbeteren van de netwerk- en informatiebeveiliging in de EU[1] is gebleken dat 57 % van de respondenten het afgelopen jaar last heeft gehad van NIB-incidenten die hun activiteiten ernstig hebben beïnvloed. Falende NIB kan vitale diensten die afhangen van de integriteit van de netwerk- en informatiesystemen, in gevaar brengen. Dit kan tot gevolg hebben dat bedrijven hun werk niet meer kunnen doen, de economie van de EU aanzienlijke financiële verliezen lijdt en de samenleving aan welzijn inboet.

Bovendien zijn digitale informatiesystemen, in het bijzonder het internet, communicatie-instrumenten zonder grenzen, die dus over de grenzen van de lidstaten met elkaar verbonden zijn en een essentiële rol spelen in het vergemakkelijken van grensoverschrijdend verkeer van goederen, diensten en personen. Ingrijpende verstoringen van deze systemen in één lidstaat kunnen voelbaar worden in andere lidstaten en in de EU als geheel. Voor de verwezenlijking van de digitale eengemaakte markt en de vlotte werking van de interne markt is het daarom van wezenlijk belang dat netwerk- en informatiesystemen zowel veerkrachtig als stabiel zijn. Bovendien verliest het publiek zijn vertrouwen in netwerk- en informatiediensten als incidenten zich met steeds grotere waarschijnlijkheid en frequentie voordoen en niet voor doeltreffende beveiliging kan worden gezorgd. Zo heeft het Eurobarometer-onderzoek over

[1] Deze raadpleging liep van 23 juli tot 15 oktober 2012.

cyberbeveiliging uit 2012 aan het licht gebracht dat 38 % van de internetgebruikers in de EU zich zorgen maakt over de veiligheid van online-betalingen en zijn gedrag als gevolg van die bezorgdheid over beveiliging heeft veranderd: respectievelijk 18 % en 15 % van hen zal minder waarschijnlijk producten online kopen en gebruikmaken van online bankieren[2].

Het bestaande beveiligingsniveau in de EU is een weerspiegeling van de louter op vrijwilligheid gebaseerde aanpak die tot dusverre is gevolgd en biedt onvoldoende bescherming tegen EU-wijde NIB-incidenten en -risico's. De huidige capaciteit en de bestaande mechanismen voor NIB volstaan eenvoudigweg niet om gelijke tred met de zeer uiteenlopende gevaren te houden en om in alle lidstaten hetzelfde hoge beschermingsniveau te waarborgen.

Hoewel in dit verband al initiatieven zijn genomen, verschilt het capaciteits- en paraatheidsniveau sterk van lidstaat tot lidstaat, wat een versnippering in de wijze van aanpakken in de EU te zien geeft. Aangezien netwerken en systemen onderling verbonden zijn, is het EU-wijde NIB-niveau maar net zo sterk als dat van de lidstaat met het laagste beschermingsniveau. Een dergelijke situatie maakt het de partijen bovendien moeilijk elkaar te vertrouwen, terwijl dat precies de voorwaarde is om samen te werken en informatie uit te wisselen. Gevolg: slechts een minderheid van lidstaten, elk met een hoog capaciteitsniveau, werkt samen.

Daarom bestaat op EU-niveau momenteel geen efficiënt mechanisme aan de hand waarvan de lidstaten doeltreffend kunnen samenwerken en in vertrouwen informatie kunnen uitwisselen op het gebied van NIB-incidenten en -risico's. Dit kan resulteren in ongecoördineerde regelgeving, onsamenhangende strategieën en uiteenlopende normen, met als gevolg ontoereikende bescherming tegen NIB-risico's in de EU. Voorts kunnen marktbelemmeringen ontstaan die nalevingskosten creëren voor bedrijven die in meer dan één lidstaat actief zijn.

[2] Eurobarometer 390/2012.

Tot slot zij erop gewezen dat voor de spelers die kritieke infrastructuur beheren of diensten aanbieden welke essentieel zijn voor de werking van onze maatschappij, geen adequate verplichtingen gelden om risicobeheermaatregelen te nemen en informatie uit te wisselen met betrokken autoriteiten. Dit betekent, enerzijds, dat bedrijven onvoldoende worden gestimuleerd om een ernstig risicobeheerbeleid te voeren, onder meer door de risico's te beoordelen en maatregelen te nemen die borg staan voor NIB, en, anderzijds, dat een groot aandeel van de incidenten niet tot de bevoegde autoriteiten doordringt en onopgemerkt blijft. Informatie over incidenten is echter van essentieel belang om de overheden in staat te stellen op incidenten te reageren, de juiste risicobeperkende maatregelen te nemen en adequate strategische prioriteiten voor NIB vast te stellen.

Op grond van het bestaande regelgevingskader moeten alleen de telecombedrijven risicobeheermaatregelen nemen en ernstige NIB-incidenten rapporteren. Tal van andere sectoren blijven dus buiten beeld, hoewel zij afhankelijk zijn van ICT als faciliterende factor en daarom ook belang hebben bij NIB. Bepaalde specifieke aanbieders van infrastructuur en diensten zijn bijzonder kwetsbaar omdat zij sterk afhankelijk zijn van correct werkende netwerk- en informatiesystemen. Deze sectoren spelen een essentiële rol door onmisbare ondersteunende diensten voor onze economie en onze samenleving te leveren, en de beveiliging van hun systemen is dan ook van bijzonder belang voor de werking van de interne markt. Het gaat onder meer om de volgende sectoren: banken, beurzen, opwekking, transport en distributie van energie, lucht-, spoor- en zeevervoer, gezondheid, internetdiensten en de overheid.

Gezien deze achtergrond moet de aanpak van NIB in de EU stapsgewijs worden veranderd. Om een gelijk speelveld te creëren en bestaande lacunes in de wetgeving te dichten, moeten wettelijke verplichtingen worden vastgesteld. Om de problemen in dit verband op te lossen en het NIB-niveau in de Europese Unie te verhogen, worden in het onderhavige richtlijnvoorstel de volgende doelstellingen vooropgesteld.

In de eerste plaats moet elke lidstaat zorgen voor een minimale nationale capaciteit door voor NIB bevoegde autoriteiten aan te wijzen, computercrisisteams op te zetten (Computer Emergency Response Teams – CERT's) en nationale NIB-strategieën en -samenwerkingsplannen vast te stellen.

In de tweede plaats moeten de nationale bevoegde autoriteiten samenwerken in het kader van een netwerk dat beveiligde en doeltreffende coördinatie, inclusief gecoördineerde informatie-uitwisseling, alsmede opsporing en reactie op EU-niveau mogelijk maakt. De lidstaten moeten via dit netwerk informatie uitwisselen en samenwerken om NIB-dreigingen en -incidenten aan te pakken op basis van het Europese NIB-samenwerkingsplan.

In de derde plaats moet er, uitgaande van het model van de kaderrichtlijn voor elektronische communicatie, voor worden gezorgd dat een cultuur van risicobeheer ingang vindt en dat de particuliere en de openbare sector onderling informatie uitwisselen. Zowel bedrijven uit de hierboven genoemde specifieke kritieke sectoren als overheden zullen ertoe worden verplicht de risico's waarmee zij worden geconfronteerd, te beoordelen, passende en evenredige maatregelen te nemen om NIB te waarborgen en aan de bevoegde autoriteiten verslag uit te brengen over incidenten die hun netwerken en informatiesystemen ernstig in gevaar brengen en de continuïteit van kritieke diensten en de levering van goederen significant beïnvloeden.

1.2. Algemene context

Reeds in 2001 wijst de Commissie in haar mededeling "Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak" op het toenemende belang van NIB[3]. Daarop

[3] COM(2001) 298.

volgt in 2006 de mededeling "Een strategie voor een veilige informatiemaatschappij"[4], die moet leiden tot een cultuur van NIB in Europa. De Raad bekrachtigt de voornaamste punten daarvan in een resolutie[5].

Op 30 maart 2009 stelt de Commissie een mededeling over bescherming van kritieke informatie-infrastructuur[6] vast waarin zij met name nagaat hoe Europa aan de hand van betere beveiliging kan worden beschermd tegen cyberverstoringen. In de mededeling wordt een actieplan voorgesteld om de inspanningen van de lidstaten om preventie en reactie te waarborgen, te ondersteunen. Het actieplan wordt bekrachtigd in de conclusies van het voorzitterschap van de ministerconferentie over de bescherming van kritieke informatie-infrastructuur die in 2009 in Tallinn is gehouden. Op 18 december 2009 neemt de Raad een resolutie aan over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging[7].

In de Digitale agenda voor Europa[8] (DAE), die in mei 2010 wordt aangenomen, en in de desbetreffende conclusies van de Raad[9] wordt gewezen op het gemeenschappelijke besef dat vertrouwen en beveiliging essentiële vereisten zijn om tot een ruime verbreiding van ICT te komen en dus ook om de doelstellingen van de dimensie "slimme groei" van de Europa 2020-strategie te bereiken[10]. In de DAE, meer bepaald in het hoofdstuk over vertrouwen en beveiliging, wordt onderstreept dat alle belanghebbende partijen de handen in elkaar moeten slaan om enerzijds in het kader van een holistische aanpak de beveiliging en de veerkracht van de ICT-infrastructuur te waarborgen door gericht in te zetten op preventie, paraatheid en bewustmaking, en anderzijds doeltreffende en gecoördineerde beveiligingsmechanismen te ontwikkelen. Kernactie 6 van de Digitale agenda voor Europa in het bijzonder heeft tot doel maatregelen vast te stellen voor een versterkt NIB-beleid op hoog niveau.

In haar mededeling van maart 2011 over de bescherming van kritieke informatie-infrastructuur "Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid"[11] maakt de Commissie een inventaris op van de resultaten die geboekt zijn sinds het actieplan voor de bescherming van kritieke informatie-infrastructuur in 2009 is vastgesteld. Zij concludeert naar aanleiding van de tenuitvoerlegging van het actieplan dat louter nationale maatregelen voor het aanpakken van de uitdagingen op het gebied van beveiliging en veerkracht niet volstaan en dat Europa moet blijven werken aan een samenhangende en op samenwerking gebaseerde EU-wijde aanpak. In deze mededeling uit 2011 kondigt de Commissie een aantal acties aan en roept zij de lidstaten op om NIB-capaciteit en grensoverschrijdende samenwerking van de grond te tillen. Deze acties moesten voor het merendeel in 2012 worden afgerond, maar zijn inmiddels nog niet ten uitvoer gelegd.

In zijn conclusies van 27 mei 2011 over bescherming van kritieke informatie-infrastructuur beklemtoont de Raad van de Europese Unie de noodzaak om IT-systemen en -netwerken voldoende robuust te maken en ze te beveiligen tegen alle mogelijke accidentele of opzettelijke verstoringen, om in de EU een hoge mate van paraatheid, veiligheid en robuustheid te ontwikkelen, om de technische bekwaamheid te vergroten opdat Europa de

---

4 COM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/nl/com/2006/com2006_0251nl01.pdf.
5 2007/068/01.
6 COM(2009) 149.
7 2009/C 321/01.
8 COM(2010) 245.
9 Conclusies van de Raad van 31 mei 2010 over de digitale agenda voor Europa (10130/10).
10 COM(2010) 2020 en conclusies van de Europese Raad van 25 en 26 maart 2010 (EUCO 7/10).
11 COM(2011) 163.

uitdaging kan aangaan om de netwerken en de informatie-infrastructuur te beveiligen, en om samenwerking tussen de lidstaten te bevorderen door regelingen voor samenwerking tussen de lidstaten bij incidenten uit te werken.

1.3. Bestaande Europese en internationale bepalingen op dit gebied

In 2004 heeft de Europese Gemeenschap op grond van Verordening (EG) nr. 460/2004 het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA)[12] opgericht, dat tot taak heeft te zorgen voor een hoog niveau van netwerk- en informatiebeveiliging en een cultuur van netwerk- en informatiebeveiliging in de Europese Unie. Op 30 september 2010[13] is een voorstel tot modernisering van het mandaat van ENISA aangenomen dat momenteel in de Raad en het Europees Parlement wordt behandeld. Krachtens het herziene regelgevingskader voor elektronische communicatie[14] dat sinds november 2009 van kracht is, moeten aanbieders van elektronischecommunicatiediensten verplichtingen op het gebied van beveiliging in acht nemen[15]. Deze verplichtingen moesten uiterlijk in mei 2011 in nationaal recht zijn omgezet.

Alle spelers die tevens voor de gegevensverwerking verantwoordelijk zijn (zoals banken en ziekenhuizen), moeten op grond van het regelgevingskader inzake gegevensbescherming[16] beveiligingsmaatregelen nemen om persoonsgegevens te beschermen. Voorts wordt in het uit 2012 daterende voorstel van de Commissie inzake een algemene verordening gegevensbescherming[17] voorgesteld de voor de verwerking verantwoordelijke ertoe te verplichten inbreuken in verband met persoonsgegevens te melden aan de nationale toezichthoudende autoriteit. Dit houdt bijvoorbeeld in dat inbreuken in verband met NIB-beveiliging die gevolgen hebben voor de levering van een dienst, maar geen risico inhouden voor persoonsgegevens (zoals het uitvallen van de ICT's bij een elektriciteitsbedrijf als gevolg van een stroompanne) niet hoeven te worden gemeld.

De overkoepelende benadering voor bescherming van kritieke infrastructuur in de EU is vastgelegd in Richtlijn 2008/114/EG inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren[18]. De doelstellingen van die richtlijn komen volledig overeen met de richtlijn die nu wordt voorgesteld en die onverminderd Richtlijn 2008/114/EG dient te worden toegepast. Richtlijn 2008/114/EG behelst geen verplichting voor de exploitanten om significante inbreuken in verband met beveiliging te melden. Evenmin worden bij die richtlijn mechanismen in het leven geroepen om de samenwerking en de reactie van lidstaten bij incidenten in goede banen te leiden.

De EU-instellingen met wetgevingsbevoegdheden buigen zich momenteel over een voorstel van de Commissie voor een richtlijn over aanvallen op informatiesystemen[19] die tot doel heeft de strafrechtelijke behandeling van specifieke soorten gedragingen te harmoniseren. Dit voorstel heeft uitsluitend betrekking op de strafrechtelijke behandeling van specifieke soorten gedragingen, en niet op de preventie van NIB-risico's en -incidenten, noch op de reactie op

---

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

13 COM(2010) 521.

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

15 Artikelen 13 bis en 13 ter van de kaderrichtlijn.

16 Richtlijn 2002/58/EG van 12 juli 2002.

17 COM(2012) 11.

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

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

NIB-incidenten en de mildering van de impact ervan. De onderhavige richtlijn dient van toepassing te zijn onverminderd de richtlijn over aanvallen op informatiesystemen.

Op 28 maart 2012 heeft de Commissie een mededeling aangenomen over de oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit[20]. Dit centrum is op 11 januari 2013 opgericht als onderdeel van Europol en vormt de spil in de strijd tegen cybercriminaliteit in de EU. Het is de bedoeling om in het Europees Centrum voor de bestrijding van cybercriminaliteit alle expertise op het gebied van cybercriminaliteit samen te brengen en zodoende de lidstaten te ondersteunen bij capaciteitsopbouw en bij onderzoeken in verband met cybercriminaliteit. Daarnaast moet het centrum, in nauwe samenwerking met Eurojust, de collectieve spreekbuis worden voor alle onderzoekers die in Europa in wetshandhavings- en gerechtelijke instanties actief zijn op het gebied van cybercriminaliteit.

De instellingen, agentschappen en organen van de EU hebben hun eigen computercrisisteam ("EU-CERT") om zich te beveiligen tegen computercriminaliteit en -incidenten.

In internationale fora werkt de EU zowel op bilateraal als op multilateraal niveau aan cyberbeveiliging. Zo is naar aanleiding van de topontmoeting van de EU en de VS[21] een EU-VS-werkgroep inzake cyberbeveiliging en cybercriminaliteit opgericht. Voorts is de EU actief in andere ter zake relevante multilaterale fora, zoals de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO), de Algemene Vergadering van de Verenigde Naties, de Internationale Telecommunicatie Unie (ITU), de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE), de Wereldtop over de informatiemaatschappij (WSIS) en het Forum voor internetbeheer.

2. RESULTATEN VAN DE RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

2.1. Raadpleging van de betrokken partijen en gebruik van expertise

Van 23 juli tot 15 oktober 2012 is online een openbare raadpleging gehouden met als onderwerp de verbetering van NIB in de EU. De Commissie heeft in totaal 160 reacties op de online-vragenlijst ontvangen.

Belangrijkste resultaat is dat de belanghebbende partijen het doorgaans eens zijn met de stelling dat NIB in de EU aan verbetering toe is. Meer in het bijzonder vindt 82,8 % van de respondenten dat de regeringen in de EU meer moeten doen om een hoog NIB-niveau te garanderen, is 82,8 % van mening dat gebruikers van informatie en systemen zich niet bewust zijn van bestaande NIB-dreigingen en -incidenten, is 66,3 % in beginsel voor de invoering van een wettelijke vereiste om NIB-risico's te beheren, en spreekt 84,8 % zich uit voor de vaststelling van dergelijke vereisten op EU-niveau. Een groot aantal respondenten vindt het belangrijk dat met name in de volgende sectoren NIB-vereisten worden vastgesteld: het bankwezen en de financiële wereld (91,1 %), energie (89,4 %), transport (81,7 %), gezondheid (89,4 %), internetdiensten (89,1 %) en de overheid (87,5 %). Voorts zijn de respondenten van mening dat indien een verplichting om inbreuken in verband met NIB-beveiliging aan de nationale bevoegde autoriteit te melden, wordt ingevoerd, deze verplichting op EU-niveau moet worden vastgesteld (65,1 %) en ook door de overheden moet worden nagekomen (93,5 %). Tot slot geven de respondenten aan dat de eis om het risicobeheer in verband met NIB volgens de stand van de techniek ten uitvoer te leggen, geen

[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.

significante extra kosten voor hen met zich mee zou brengen (63,4 %), net zomin als de eis om inbreuken in verband met beveiliging te rapporteren (72,3 %).

De lidstaten zijn eveneens geraadpleegd: in verschillende Raadsformaties, in het kader van het Europees Forum voor de lidstaten, naar aanleiding van de conferentie over cyberbeveiliging die de Europese Commissie en de Europese dienst voor extern optreden op 6 juli 2012 hebben gehouden, en in gespecialiseerde bilaterale vergaderingen die op verzoek van individuele lidstaten zijn belegd.

Ook met de particuliere sector zijn besprekingen gevoerd, meer bepaald in het kader van het Europees publiek-privaat partnerschap voor veerkracht[22] en in bilaterale vergaderingen. Met betrekking tot de openbare sector heeft de Commissie gesprekken gehad met ENISA en, voor wat de Europese instellingen betreft, met de CERT.

2.2. Effectbeoordeling

De Commissie heeft voor drie beleidsopties een effectbeoordeling uitgevoerd.

Optie 1: Status-quo (basisscenario): de huidige aanpak wordt voortgezet.

Optie 2: Regelgeving, bestaande uit een wetgevingsvoorstel tot vaststelling van een gemeenschappelijk EU-wetskader voor NIB wat betreft de capaciteit van de lidstaten, mechanismen voor samenwerking op EU-niveau en vereisten voor essentiële particuliere spelers en overheden.

Optie 3: Een combinatie van op vrijwilligheid gebaseerde initiatieven voor de NIB-capaciteit van de lidstaten en mechanismen voor samenwerking op EU-niveau met wettelijke vereisten voor essentiële particuliere spelers en overheden.

De Commissie komt tot de slotsom dat optie 2 de grootste positieve impact zou hebben, aangezien zowel consumenten als ondernemingen en overheden in de EU aanzienlijk beter tegen NIB-incidenten zouden worden beschermd. Met name zouden de verplichtingen waaraan de lidstaten moeten voldoen, niet alleen borg staan voor een adequate paraatheid op nationaal niveau, maar ook bijdragen tot een klimaat van wederzijds vertrouwen – per slot van rekening een voorwaarde voor doeltreffende samenwerking op EU-niveau. Mechanismen om op EU-niveau via het netwerk samen te werken, zouden het mogelijk maken om bij grensoverschrijdende NIB-incidenten en -risico's zowel preventie als reactie samenhangend en gecoördineerd aan te pakken. De invoering van vereisten om NIB-risicobeheer voor overheden en essentiële particuliere spelers ten uitvoer te leggen, zou een krachtige stimulans creëren om beveiligingsrisico's doeltreffend te beheren. De verplichting om NIB-incidenten met een aanzienlijke impact te rapporteren, zou de capaciteit om op incidenten te reageren versterken en de transparantie bevorderen. Bovendien zou de EU, door haar zaken op orde te brengen, haar internationale invloed kunnen uitbreiden en haar – nu al aanzienlijke – geloofwaardigheid als partner op bilateraal en multilateraal niveau nog meer kracht kunnen bijzetten. De EU zou dan ook in een betere positie verkeren om de grondrechten en essentiële waarden van de EU te bevorderen.

Uit de kwantitatieve beoordeling is gebleken dat optie 2 geen onevenredige belasting van de lidstaten met zich zou brengen. Ook de kosten voor de particuliere sector zouden binnen de perken blijven aangezien veel betrokken organisaties verondersteld worden al aan de bestaande beveiligingseisen te voldoen (voor de verwerking verantwoordelijke personen moeten namelijk technische en organisatorische maatregelen, inclusief NIB-maatregelen,

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

nemen om persoonsgegevens te beveiligen). Bestaande uitgaven voor beveiliging in de particuliere sector zijn overigens ook in aanmerking genomen.

Dit voorstel is in overeenstemming met de beginselen van het Handvest van de grondrechten van de Europese Unie, meer bepaald het recht op eerbiediging van het privéleven en communicatie, de bescherming van persoonsgegevens, de vrijheid van ondernemerschap, het recht op eigendom, het recht op een doeltreffende voorziening in rechte en het recht te worden gehoord. Deze richtlijn moet overeenkomstig deze rechten en beginselen ten uitvoer worden gelegd.

3. JURIDISCHE ELEMENTEN VAN HET VOORSTEL

3.1. Rechtsgrondslag

De Europese Unie is gemachtigd tot het vaststellen van de maatregelen die ertoe bestemd zijn de interne markt tot stand te brengen en de werking ervan te verzekeren, overeenkomstig de bepalingen ter zake van de Verdragen (artikel 26 van het Verdrag betreffende de werking van de Europese Unie – VWEU). Krachtens artikel 114 VWEU kan de EU maatregelen vaststellen "*inzake de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten* die de instelling en de werking van de interne markt betreffen".

Zoals hierboven reeds vermeld, spelen netwerk- en informatiesystemen een essentiële rol in het vergemakkelijken van grensoverschrijdend verkeer van goederen, diensten en personen. Zij zijn vaak met elkaar verbonden en het internet is van nature uit mondiaal georiënteerd. Vanwege deze intrinsiek internationale dimensie kan een verstoring in één lidstaat voelbaar worden in andere lidstaten en in de EU als geheel. Voor de vlotte werking van de interne markt is het daarom van het grootste belang dat netwerk- en informatiesystemen veerkrachtig en stabiel zijn.

De EU-wetgever heeft reeds erkend dat de NIB-regels moeten worden geharmoniseerd, wil men de ontwikkeling van de interne markt garanderen. Dit geldt met name voor de op artikel 114 VWEU gebaseerde Verordening (EG) nr. 460/2004 tot oprichting van ENISA[23].

De scheefgetrokken situatie die het gevolg is van verschillen in nationale capaciteit, beleid en beschermingsniveau tussen de lidstaten, belemmert de werking van de interne markt en rechtvaardigt een optreden van de EU.

3.2. Subsidiariteit

Het subsidiariteitsbeginsel rechtvaardigt een optreden van de EU op het gebied van NIB.

Gezien het grensoverschrijdende karakter van NIB zou, wanneer de EU niet optreedt, een situatie ontstaan waarin elke lidstaat alleen maatregelen neemt en geen rekening wordt gehouden met de verwevenheid van de netwerk- en informatiesystemen in de EU. Adequate coördinatie tussen de lidstaten moet garanderen dat NIB-risico's naar behoren worden beheerd in de grensoverschrijdende context waarin zij zich voordoen. Verschillen in de NIB-regelgeving vormen een belemmering voor bedrijven die hun activiteit tot meerdere landen willen uitbreiden, en staan het realiseren van wereldwijde schaalvoordelen in de weg.

Ten tweede moeten wettelijke verplichtingen op EU-niveau worden vastgesteld om een gelijk speelveld te creëren en lacunes in de wetgeving te dichten. De louter op vrijwilligheid gebaseerde aanpak die tot dusverre is gevolgd, heeft slechts een minderheid van lidstaten, elk

[23] Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging (PB L 77 van 13.3.2004, blz. 1).

met een hoog capaciteitsniveau, tot samenwerking gestimuleerd. De overige lidstaten kunnen in dit verband alleen over de streep worden gehaald als zij allemaal over het vereiste minimale capaciteitsniveau beschikken. Van overheidswege vastgestelde NIB-maatregelen moeten met elkaar in overeenstemming zijn en onderling worden gecoördineerd om de gevolgen van NIB-incidenten in te dijken en tot een minimum te beperken. In het kader van het netwerk zullen de bevoegde autoriteiten en de Commissie, middels het uitwisselen van beste praktijken en de continue betrokkenheid van ENISA, samenwerken om een samenhangende tenuitvoerlegging van de richtlijn in de EU te waarborgen. Bovendien kunnen gezamenlijke beleidsmaatregelen op het gebied van NIB een sterk positief effect hebben op de bescherming van de grondrechten, en met name het recht op bescherming van persoonsgegevens en van het privéleven. Optreden op EU-niveau zou de doeltreffendheid van bestaande nationale beleidslijnen ten goede komen en de ontwikkeling van dergelijke beleidslijnen vergemakkelijken.

Ook het evenredigheidsbeginsel kan worden aangevoerd als rechtvaardiging voor de voorgestelde maatregelen. De NIB-vereisten waaraan de lidstaten moeten voldoen, worden vastgesteld op het minimale niveau dat vereist is voor een adequate paraatheid en een op vertrouwen gebaseerde samenwerking. Dit biedt de lidstaten de mogelijkheid om rekening te houden met hun eigen specifieke situatie en zorgt ervoor dat de gemeenschappelijke EU-beginselen op een evenredige manier worden toegepast. Dankzij de ruime werkingssfeer kunnen de lidstaten de tenuitvoerlegging van de richtlijn afstemmen op de daadwerkelijk op nationaal niveau bestaande risico's die in de nationale NIB-strategie zijn omschreven. De vereisten voor de toepassing van risicobeheer hebben enkel betrekking op kritieke organisaties en verplichten tot het vaststellen van maatregelen die evenredig zijn aan de risico's. In het kader van de openbare raadpleging is benadrukt hoe belangrijk het is dat de beveiliging van deze kritieke organisaties wordt gewaarborgd. De rapportagevoorschriften betreffen uitsluitend incidenten met een aanzienlijke impact. Zoals hierboven reeds is vermeld, brengen de maatregelen geen onevenredige kosten met zich mee, aangezien een groot aantal van deze organisaties, in hun hoedanigheid van voor de verwerking van gegevens verantwoordelijke, op grond van de vigerende gegevensbeschermingsvoorschriften nu al moeten zorgen voor de beveiliging van de bescherming van persoonsgegevens.

Om te voorkomen dat kleinschalige exploitanten, met name het mkb, onevenredig zwaar worden belast, staan de vereisten in verhouding tot het risico voor het betrokken netwerk of informatiesysteem en moeten microbedrijven van de toepassing van deze vereisten worden vrijgesteld. De risico's moeten in de eerste plaats worden bepaald door de organisaties waarvoor deze verplichtingen gelden. Zij zullen moeten beslissen welke maatregelen dienen te worden vastgesteld om deze risico's te verkleinen.

Gezien het grensoverschrijdende karakter van NIB-incidenten en -risico's kunnen de vooropgestelde doelstellingen beter op EU-niveau worden bereikt dan door afzonderlijke lidstaten. De EU kan derhalve maatregelen treffen overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel. Overeenkomstig het evenredigheidsbeginsel gaat de voorgestelde richtlijn niet verder dan wat nodig is om de doelstellingen te verwezenlijken.

Om de doelstellingen te halen, dient de Commissie te worden gemachtigd om overeenkomstig artikel 290 VWEU gedelegeerde handelingen vast te stellen ter aanvulling of wijziging van bepaalde niet-essentiële onderdelen van het basisbesluit. Het voorstel van de Commissie streeft ook naar evenredigheid bij de tenuitvoerlegging van de verplichtingen waaraan particuliere en openbare exploitanten zich moeten houden.

Om uniforme voorwaarden voor de uitvoering van deze richtlijn te waarborgen, moet de Commissie ertoe worden gemachtigd uitvoeringshandelingen vast te stellen overeenkomstig artikel 291 VWEU.

Met name gezien de brede werkingssfeer van de voorgestelde richtlijn, gezien het feit dat deze richtlijn strikt gereglementeerde gebieden bestrijkt en gezien de uit hoofdstuk IV van deze richtlijn voortvloeiende wettelijke verplichtingen, moet de kennisgeving van de omzettingsmaatregelen vergezeld gaan van toelichtende stukken. Overeenkomstig de gezamenlijke politieke verklaring van de lidstaten en de Commissie over toelichtende stukken van 28 september 2011 hebben de lidstaten zich ertoe verbonden om in gerechtvaardigde gevallen de kennisgeving van hun omzettingsmaatregelen vergezeld te doen gaan van één of meer stukken waarin het verband tussen de onderdelen van een richtlijn en de overeenkomstige delen van de nationale omzettingsinstrumenten wordt toegelicht. Met betrekking tot deze richtlijn acht de wetgever de toezending van dergelijke stukken gerechtvaardigd.

4. GEVOLGEN VOOR DE BEGROTING

Zowel de samenwerking als de uitwisseling van informatie tussen de lidstaten moet worden ondersteund door een beveiligde infrastructuur. Dit voorstel zal slechts gevolgen voor de begroting hebben indien de lidstaten opteren voor de aanpassing van een bestaande infrastructuur (zoals sTESTA) en zij de Commissie opdragen dit ten uitvoer te leggen binnen het meerjarig financieel kader voor de periode 2014-2020. De eenmalige kosten worden geraamd op EUR 1 250 000 en zouden ten laste van de EU-begroting komen, met name onder post 09 03 02 (de interconnectie en interoperabiliteit van online nationale openbare diensten bevorderen, alsook de toegang tot dergelijke netwerken — Hoofdstuk 09 03 Connecting Europe Facility — telecommunicatienetwerken), mits in het kader van de financieringsfaciliteit voor Europese verbindingen voldoende middelen beschikbaar zijn. Bij wijze van alternatief kunnen de lidstaten de eenmalige kosten van de aanpassing van bestaande infrastructuur delen of beslissen nieuwe infrastructuur op te zetten en de kosten daarvan (naar raming ca. EUR 10 miljoen per jaar) te dragen.

2013/0027 (COD)

Voorstel voor een

RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD

houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van de wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité[1],

Na raadpleging van de Europese Toezichthouder voor gegevensbescherming,

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) Netwerk- en informatiesystemen en -diensten spelen een cruciale rol in de samenleving. De betrouwbaarheid en beveiliging ervan zijn essentieel voor de economische bedrijvigheid en het sociaal welzijn, en met name voor de werking van de eengemaakte markt.

(2) De omvang en frequentie van opzettelijke en accidentele beveiligingsincidenten neemt toe en vormt een grote bedreiging voor de werking van netwerken en informatiesystemen. Zulke incidenten kunnen de economische bedrijvigheid belemmeren, aanzienlijke financiële verliezen opleveren, het gebruikersvertrouwen ondermijnen en de economie van de Unie ernstige schade toebrengen.

(3) Als communicatiemiddel zonder grenzen spelen digitale informatiesystemen, en hoofdzakelijk het internet, een cruciale rol in het faciliteren van het grensoverschrijdende verkeer van goederen, diensten en personen. Vanwege dat transnationale karakter kan een ernstige verstoring van die systemen in een lidstaat ook andere lidstaten en de Unie als geheel treffen. De veerkracht en stabiliteit van netwerk- en informatiesystemen is daarom essentieel voor de soepele werking van de eengemaakte markt.

(4) Op het niveau van de Unie moet een samenwerkingsmechanisme worden opgezet dat informatie-uitwisseling en gecoördineerde opsporing en reactie met betrekking tot netwerk- en informatiebeveiliging ("NIB") mogelijk maakt. Opdat dat mechanisme doeltreffend en inclusief zou zijn, is het essentieel dat alle lidstaten over minimumcapaciteit en een strategie beschikken om op hun grondgebied een hoog niveau van NIB te waarborgen. Om een cultuur van risicobeheer te bevorderen en ervoor te zorgen dat de ernstigste incidenten worden gemeld, moeten ook voor overheden en exploitanten van kritieke informatie-infrastructuur minimumeisen inzake beveiliging gelden.

[1] PB C […] van […], blz.. […].

(5) Om in alle relevante incidenten en risico's te voorzien, moet deze richtlijn van toepassing zijn op alle netwerk- en informatiesystemen. De verplichtingen ten aanzien van overheden en marktdeelnemers mogen echter niet van toepassing zijn op ondernemingen die openbare communicatienetwerken of openbare elektronischecommunicatiediensten in de zin van Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronischecommunicatienetwerken en -diensten (kaderrichtlijn)[2] aanbieden, welke zijn onderworpen aan de in artikel 13 bis van die richtlijn vastgestelde specifieke veiligheids- en integriteitseisen, noch op aanbieders van vertrouwensdiensten.

(6) De bestaande capaciteit volstaat niet om een hoog niveau van NIB in de Unie te waarborgen. Omdat het niveau van paraatheid van de lidstaten sterk uiteenloopt, is de aanpak in de Unie gefragmenteerd. Dit leidt tot ongelijke niveaus van bescherming van consumenten en bedrijven en ondermijnt het algemene NIB-niveau in de Unie. Doordat er geen gemeenschappelijke minimumeisen ten aanzien van overheden en marktdeelnemers gelden, is het dan weer onmogelijk een overkoepelend en doeltreffend mechanisme voor samenwerking op het niveau van de Unie op te zetten.

(7) Om doeltreffend te reageren op de beveiligingsuitdagingen voor netwerk- en informatiesystemen is daarom een overkoepelende aanpak op het niveau van de Unie nodig die gemeenschappelijke minimumeisen inzake capaciteitsopbouw en planning, informatie-uitwisseling, coördinatie van maatregelen en gemeenschappelijke minimumeisen inzake beveiliging voor alle betrokken marktdeelnemers en overheden omvat.

(8) De bepalingen van deze richtlijn moeten de mogelijkheid onverlet laten dat elke lidstaat de nodige maatregelen neemt om voor de bescherming van zijn essentiële veiligheidsbelangen te zorgen, de openbare orde en de openbare veiligheid te garanderen en het onderzoek, de opsporing en de vervolging van misdrijven mogelijk te maken. Overeenkomstig artikel 346 VWEU mag geen enkele lidstaat verplicht worden inlichtingen te verstrekken waarvan de openbaarmaking naar zijn mening strijdig is met wezenlijke veiligheidsbelangen.

(9) Om een hoog gemeenschappelijk beveiligingsniveau van netwerk- en informatiesystemen te bereiken en te handhaven, moet elke lidstaat een nationale NIB-strategie hebben waarin de te verwezenlijken strategische doelstellingen en concrete beleidsmaatregelen zijn vastgesteld. Op nationaal niveau moeten aan essentiële eisen beantwoordende NIB-samenwerkingsplannen worden ontwikkeld om een niveau van reactiecapaciteit te bereiken dat in geval van incidenten doeltreffende en efficiënte samenwerking op nationaal niveau en op het niveau van de Unie mogelijk maakt.

(10) Om de doeltreffende uitvoering van de krachtens deze richtlijn vastgestelde bepalingen mogelijk te maken, moet in elke lidstaat een met de coördinatie van NIB-zaken belaste instantie worden opgericht of aangewezen die optreedt als contactpunt voor grensoverschrijdende samenwerking op het niveau van de Unie. Deze instanties moeten de nodige technische, financiële en personele middelen krijgen om de hun toegewezen taken op doeltreffende en efficiënte wijze te kunnen verrichten en aldus de doelstellingen van deze richtlijn te verwezenlijken.

(11) Alle lidstaten moeten zowel technisch als organisatorisch voldoende zijn toegerust voor het voorkomen en opsporen van en reageren op incidenten en risico's met

[2] PB L 108 van 24.4.2002, blz. 33.

betrekking tot netwerk- en informatiesystemen. Daarom moeten in alle lidstaten goed functionerende, aan essentiële eisen beantwoordende computercrisisteams (*Computer Emergency Response Teams* – CERT's) worden opgericht die voor doeltreffende en compatibele capaciteit voor de aanpak van incidenten en risico's moeten zorgen en doeltreffende samenwerking op het niveau van de Unie waarborgen.

(12) Voortbouwend op de aanzienlijke vooruitgang die in het Europees Forum voor de lidstaten (EFMS) is geboekt met betrekking tot het bevorderen van discussies en de uitwisseling van goede beleidspraktijken, waaronder de ontwikkeling van beginselen voor Europese cybercrisissamenwerking, moeten de lidstaten en de Commissie een netwerk vormen om permanente communicatie tot stand te brengen en samenwerking te bevorderen. Dit beveiligde en doeltreffende samenwerkingsmechanisme moet gestructureerde en gecoördineerde informatie-uitwisseling, opsporing en reactie op het niveau van de Unie mogelijk maken.

(13) Het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) moet de lidstaten en de Commissie met deskundigheid en advies bijstaan en de uitwisseling van beste praktijken faciliteren. Met name bij de toepassing van deze richtlijn moet de Commissie ENISA raadplegen. Om ervoor te zorgen dat de lidstaten en de Commissie doeltreffend en tijdig worden geïnformeerd, moeten binnen het samenwerkingsnetwerk vroegtijdige waarschuwingen over incidenten en risico's worden gegeven. Om capaciteit en kennis bij de lidstaten op te bouwen, moet het samenwerkingsnetwerk tevens dienstdoen als een instrument voor de uitwisseling van beste praktijken, dat de leden behulpzaam is bij het opbouwen van capaciteit en houvast biedt bij de organisatie van collegiale toetsingen en NIB-oefeningen.

(14) Er moet een beveiligde informatie-uitwisselingsstructuur worden opgezet om de uitwisseling van gevoelige en vertrouwelijke informatie binnen het netwerk mogelijk te maken. Onverminderd hun verplichting om incidenten en risico's met een uniale dimensie bij het samenwerkingsnetwerk te melden, mogen lidstaten alleen toegang tot vertrouwelijke informatie van andere lidstaten krijgen indien zij aantonen dat hun technische, financiële en personele middelen en processen, alsook hun communicatiestructuur, waarborgen dat hun deelname aan het netwerk doeltreffend, efficiënt en veilig is.

(15) Aangezien de meeste netwerk- en informatiesystemen particulier worden geëxploiteerd, is samenwerking tussen de publieke en private sector essentieel. Marktdeelnemers moeten worden aangemoedigd eigen informele samenwerkingsmechanismen op te zetten om NIB te waarborgen. Zij moeten ook met de publieke sector samenwerken en informatie en beste praktijken uitwisselen in ruil voor operationele steun bij incidenten.

(16) Om voor transparantie te zorgen en de EU-burgers en marktdeelnemers naar behoren te informeren, moeten de bevoegde autoriteiten een gemeenschappelijke website opzetten om niet-vertrouwelijke informatie over de incidenten en risico's bekend te maken.

(17) Wanneer informatie overeenkomstig uniale en nationale voorschriften inzake de vertrouwelijkheid van bedrijfsinformatie als vertrouwelijk wordt beschouwd, moet die vertrouwelijkheid worden gewaarborgd tijdens de activiteiten die noodzakelijk zijn ter verwezenlijking van de doelstellingen van deze verordening.

(18) Uitgaande van de nationale ervaringen inzake crisisbeheer en in samenwerking met ENISA, moeten de Commissie en de lidstaten een NIB-samenwerkingsplan van de

Unie opstellen waarin samenwerkingsmechanismen worden vastgesteld om risico's en incidenten aan te pakken. Met dat plan moet terdege rekening worden gehouden in de werking van het mechanisme voor vroegtijdige waarschuwing dat in het kader van het samenwerkingsnetwerk bestaat.

(19) Het geven van een vroegtijdige waarschuwing in het netwerk moet enkel worden voorgeschreven indien de omvang of ernst van het incident of risico van dien aard is of kan worden dat informatie over of coördinatie van de reactie op het niveau van de Unie vereist is. Vroegtijdige waarschuwingen moeten daarom worden beperkt tot mogelijke of daadwerkelijke incidenten of risico's die snel in omvang toenemen, de nationale reactiecapaciteit te boven gaan of meer dan een lidstaat treffen. Om een behoorlijke evaluatie mogelijk te maken, moet alle informatie die relevant is voor de beoordeling van het risico of incident, aan het samenwerkingsnetwerk worden meegedeeld.

(20) Zodra de bevoegde autoriteiten een vroegtijdige waarschuwing hebben ontvangen en beoordeeld, moeten zij een gecoördineerde reactie op grond van het NIB-samenwerkingsplan van de Unie overeenkomen. Zowel de bevoegde autoriteiten als de Commissie moeten worden geïnformeerd over de maatregelen die als gevolg van de gecoördineerde reactie op nationaal niveau zijn genomen.

(21) Gezien het mondiale karakter van NIB-problemen is er behoefte aan nauwere internationale samenwerking om beveiligingsnormen en informatie-uitwisseling te verbeteren en een gemeenschappelijke internationale aanpak van NIB-kwesties te bevorderen.

(22) De verantwoordelijkheid voor het waarborgen van NIB ligt voor een groot deel bij overheden en marktdeelnemers. Aan de hand van passende regelgevingseisen en sectorconvenanten moet een cultuur van risicobeheer worden bevorderd en ontwikkeld, die risicobeoordeling en de uitvoering van aan de risico's aangepaste beveiligingsmaatregelen behelst. Ook de totstandbrenging van een gelijk speelveld is essentieel om te waarborgen dat alle lidstaten doeltreffend samenwerken in het samenwerkingsnetwerk.

(23) Krachtens Richtlijn 2002/21/EG moeten ondernemingen die openbare elektronischecommunicatienetwerken of openbaar beschikbare elektronischecommunicatiediensten aanbieden passende maatregelen nemen om de integriteit en veiligheid daarvan te vrijwaren en zijn eisen vastgesteld voor de melding van inbreuken op de beveiliging en het verlies van integriteit. Krachtens Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)[3] moet een aanbieder van een openbaar beschikbare elektronischecommunicatiedienst passende technische en organisatorische maatregelen treffen om de beveiliging van zijn diensten te garanderen.

(24) Deze verplichtingen moeten van de elektronischecommunicatiesector worden uitgebreid naar andere belangrijke aanbieders van diensten van de informatiemaatschappij zoals gedefinieerd in Richtlijn 98/34/EG van het Europees Parlement en de Raad betreffende een informatieprocedure op het gebied van normen en technische voorschriften en regels betreffende de diensten van de

[3] PB L 201 van 31.7.2002, blz. 37.

informatiemaatschappij[4], die ten grondslag liggen aan stroomafwaartse diensten van de informatiemaatschappij of onlineactiviteiten zoals platforms voor elektronische handel, gateways voor internetbetalingen, sociaalnetwerksites, zoekmachines, cloudcomputingdiensten en internetwinkels die applicaties aanbieden. Verstoring van deze ondersteunende diensten van de informatiemaatschappij belemmert de aanbieding van andere diensten van de informatiemaatschappij die daarvan in belangrijke mate afhankelijk zijn. Softwareontwikkelaars en hardwarefabrikanten zijn geen aanbieders van diensten van de informatiemaatschappij en zijn daarom uitgesloten. De genoemde verplichtingen moeten ook worden uitgebreid naar overheden en exploitanten van kritieke infrastructuur die sterk afhankelijk zijn van informatie- en communicatietechnologie en essentieel zijn voor de instandhouding van vitale economische en maatschappelijke functies zoals de voorziening van elektriciteit en gas, vervoer, kredietinstellingen, effectenbeurzen en gezondheidszorg. Verstoring van deze netwerk- en informatiesystemen zou de eengemaakte markt aantasten.

(25) De technische en organisatorische maatregelen die aan overheden en marktdeelnemers worden opgelegd, mogen er niet toe nopen dat een bepaald commercieel informatie- en communicatietechnologieproduct op een bepaalde wijze moet worden ontworpen, ontwikkeld of vervaardigd.

(26) De overheden en marktdeelnemers moeten de beveiliging van de netwerken en systemen onder hun controle waarborgen. Het gaat daarbij voornamelijk om particuliere netwerken en systemen die door hun intern IT-personeel worden beheerd of waarvan de beveiliging is uitbesteed. De beveiligings- en meldingsverplichtingen moeten van toepassing zijn op de betrokken marktexploitanten en overheden, ongeacht of zij het onderhoud van hun netwerk- en informatiesystemen intern verrichten dan wel uitbesteden.

(27) Om te voorkomen dat aan kleine exploitanten en gebruikers onevenredige financiële en administratieve lasten worden opgelegd, moeten de eisen, rekening houdend met de meest recente technische mogelijkheden, evenredig zijn met het risico dat verbonden is met het netwerk- of informatiesysteem in kwestie. Deze eisen mogen niet van toepassing zijn op micro-ondernemingen.

(28) De bevoegde autoriteiten moeten de nodige aandacht besteden aan de instandhouding van informele en vertrouwde kanalen voor informatie-uitwisseling tussen marktdeelnemers en de publieke en private sector. Bij de bekendmaking van aan de bevoegde autoriteiten gemelde incidenten moet het belang van het publiek om te worden geïnformeerd over bedreigingen, worden afgewogen tegen mogelijke commerciële en imagoschade voor de overheden en marktdeelnemers die incidenten melden. Bij het nakomen van de meldingsverplichtingen moeten de bevoegde autoriteiten bijzondere aandacht besteden aan de noodzaak om informatie over de kwetsbare punten van producten strikt vertrouwelijk te houden tot er passende herstel- en beveiligingsmaatregelen zijn genomen.

(29) De bevoegde autoriteiten moeten over de nodige middelen beschikken om hun taken uit te voeren, met inbegrip van de bevoegdheid om van marktdeelnemers en overheden de nodige informatie te eisen om het beveiligingsniveau van netwerk- en informatiesystemen te beoordelen, alsook betrouwbare en complete gegevens over reële incidenten die een impact op de werking van netwerk- en informatieystemen hebben gehad.

[4] PB L 204 van 21.7.1998, blz. 37.

(30) In veel gevallen liggen criminele activiteiten aan de oorsprong van een incident. De criminele aard van incidenten kan worden verondersteld, zelfs indien daar in het begin nog niet voldoende bewijs voor is. Tegen die achtergrond moet een doeltreffende en alomvattende reactie op de dreiging van beveiligingsincidenten leiden tot passende samenwerking tussen bevoegde autoriteiten en wetshandhavingsinstanties. Om een veilige, beveiligde en veerkrachtige omgeving te bevorderen, moeten incidenten waarvan wordt vermoed dat ze van ernstig criminele aard zijn, systematisch aan wetshandhavingsautoriteiten worden gemeld. Of incidenten van ernstig criminele aard zijn, moet worden beoordeeld in het licht van de EU-wetgeving inzake cybercriminaliteit.

(31) In veel gevallen worden persoonsgegevens aangetast als gevolg van incidenten. Daarom moeten de bevoegde autoriteiten en de autoriteiten voor gegevensbeschermnig samenwerken en informatie over alle relevante zaken uitwisselen om inbreuken in verband met persoonsgegevens als gevolg van incidenten aan te pakken. De lidstaten moeten de verplichting om beveiligingsincidenten te melden, gestalte geven op een wijze die de administratieve lasten minimaliseert wanneer het beveiligingsincident ook een inbreuk in verband met persoonsgegevens vormt overeenkomstig de verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[5]. ENISA, dat in contact staat met de bevoegde autoriteiten en de autoriteiten voor gegevensbescherming, kan bijstand verlenen door informatie-uitwisselingsmechanismen en modellen te ontwikkelen zodat er geen twee meldingsmodellen nodig zijn. Dit eenvormige meldingsmodel zou de rapportage van incidenten die persoonsgegevens aantasten, faciliteren en zo de administratieve lasten voor bedrijven en overheden verlichten.

(32) De normalisatie van beveiligingseisen is een marktgestuurd proces. Met het oog op een eenvormige toepassing van beveiligingsnormen, moeten de lidstaten naleving van of afstemming op specifieke normen aanmoedigen om een hoog beveilgingsniveau op het niveau van de Unie te waarborgen. Daartoe kan het nodig zijn geharmoniseerde normen op te stellen, hetgeen moet gebeuren overeenkomstig Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad[6].

(33) De Commissie moet deze richtlijn op gezette tijden evalueren, met name om na te gaan of zij in het licht van de veranderende technologische omstandigheden of marktomstandigheden moeten worden gewijzigd.

(34) Teneinde de soepele werking van het samenwerkingsnetwerk mogelijk te maken, moet aan de Commissie de bevoegdheid worden overgedragen om overeenkomstig artikel 290 van het Verdrag betreffende de werking van de Europese Unie handelingen vast te stellen met het oog op het bepalen van de criteria die een lidstaat moet nakomen bij zijn deelname aan het beveiligde informatie-uitwisselingssysteem, alsmede met het oog op de verdere omschrijving van de gebeurtenissen die tot

[5] SEC(2012) 72 final.

[6] PB L 316 van 14.11.2012, blz. 12.

vroegtijdige waarschuwing leiden en de bepaling van de omstandigheden waarin marktdeelnemers en overheden verplicht zijn incidenten te melden.

(35) Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadpleging overgaat, onder meer op deskundigenniveau. De Commissie moet er bij de voorbereiding en opstelling van de gedelegeerde handelingen voor zorgen dat de desbetreffende documenten tijdig en op gepaste wijze gelijktijdig worden toegezonden aan het Europees Parlement en aan de Raad.

(36) Om uniforme voorwaarden voor de uitvoering van deze richtlijn te waarborgen, moeten aan de Commissie uitvoeringsbevoegdheden worden verleend met betrekking tot de samenwerking tussen de bevoegde autoriteiten en de Commissie in het samenwerkingsnetwerk, de toegang tot de beveiligde informatie-uitwisselingsinfrastructuur, het NIB-samenwerkingsplan van de Unie, de formaten en procedures om het publiek in te lichten over incidenten, en de voor NIB relevante normen en/of technische specificaties. Die bevoegdheden moeten worden uitgeoefend in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren[7].

(37) Bij de toepassing van deze richtlijn moet de Commissie waar passend contacten onderhouden met de relevante sectorale comités en de op EU-niveau opgerichte relevante organen, met name op het gebied van energie, vervoer en gezondheid.

(38) Informatie die door een bevoegde autoriteit overeenkomstig de uniale en nationale voorschriften inzake de vertrouwelijkheid van bedrijfsinformatie als vertrouwelijk wordt beschouwd, mag uitsluitend met de Commissie en andere bevoegde autoriteiten worden uitgewisseld wanneer die uitwisseling strikt noodzakelijk is voor de toepassing van deze richtlijn. De uitgewisselde informatie moet beperkt zijn tot hetgeen relevant is voor en evenredig met het doel van een dergelijke uitwisseling.

(39) Voor de uitwisseling van informatie over risico's en incidenten in het samenwerkingsnetwerk en de naleving van de voorschriften inzake het melden van incidenten aan de nationale bevoegde autoriteiten, kan het nodig zijn persoonsgegevens te verwerken. Zulke verwerking van persoonsgegevens is noodzakelijk ter verwezenlijking van de met deze richtlijn nagestreefde doelstellingen van algemeen belang en is dus gerechtvaardigd uit hoofde van artikel 7 van Richtlijn 95/46/EG. Zij vormt, met betrekking tot deze gerechtvaardigde doelen, geen onevenredige en onduldbare ingreep waardoor het recht op de door artikel 8 van het Handvest van grondrechten gewaarborgde bescherming van persoonsgegevens in zijn kern wordt aangetast. Waar zulks passend is, moet bij de toepassing van deze richtlijn Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie[8] van toepassing zijn. Wanneer door de instellingen en organen van de Unie gegevens worden verwerkt, is deze verwerking met het oog op de uitvoering van deze richtlijn onderworpen aan Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens.

---

7 PB L 55 van 28.2.2011, blz. 13.

8 PB L 145 van 31.5.2001, blz. 43.

(40) Aangezien de doelstellingen van deze richtlijn, namelijk het veiligstellen van een hoog niveau van NIB in de Unie, niet voldoende door de lidstaten alleen kunnen worden verwezenlijkt en derhalve, gezien de gevolgen van de maatregelen, beter op het niveau van de Unie kunnen worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze richtlijn niet verder dan nodig is om die doelstellingen te verwezenlijken.

(41) Deze richtlijn is in overeenstemming met de grondrechten en beginselen die door het Handvest van de grondrechten van de Europese Unie worden erkend, met name het recht op eerbiediging van het privéleven en communicatie, de vrijheid van ondernemerschap, het recht op eigendom, het recht op een doeltreffende voorziening in rechte en het recht te worden gehoord. Deze richtlijn moet overeenkomstig deze rechten en beginselen ten uitvoer worden gelegd,

HEBBEN DE VOLGENDE RICHTLIJN VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp en toepassingsgebied

1. Bij deze richtlijn worden maatregelen vastgesteld om in de Unie een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging (hierna "NIB" genoemd) te waarborgen.

2. Daartoe wordt bij deze richtlijn in het volgende voorzien:

(a) de vaststelling van verplichtingen voor alle lidstaten met betrekking tot de preventie en behandeling van en de reactie op risico's en incidenten met betrekking tot netwerken en informatiesystemen;

(b) de oprichting van een mechanisme voor samenwerking tussen de lidstaten met het oog op een uniforme toepassing van deze richtlijn in de Unie en, waar nodig, een gecoördineerde en doeltreffende behandeling van en reactie op risico's en incidenten met betrekking tot netwerken en informatiesystemen;

(c) de vaststelling van beveiligingseisen voor marktdeelnemers en overheden.

3. De beveiligingseisen van artikel 14 zijn niet van toepassing op ondernemingen die openbare communicatienetwerken of openbare elektronischecommunicatiediensten in de zin van Richtlijn 2002/21/EG aanbieden, welke aan de specifieke veiligheids- en integriteitseisen van de artikelen 13 bis en 13 ter van die richtlijn zijn onderworpen, noch op verleners van vertrouwensdiensten.

4. Deze richtlijn laat de EU-wetgeving inzake cybercriminaliteit en Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren[9], onverlet.

[9] PB L 345 van 23.12.2008, blz. 75.

5. Deze richtlijn laat Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[10] en Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie alsmede de verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[11], eveneens onverlet.

6. Voor de uitwisseling van informatie in het samenwerkingsnetwerk krachtens hoofdstuk III en de melding van NIB-incidenten krachtens artikel 14 kan de verwerking van persoonsgegevens vereist zijn. Deze verwerking, die noodzakelijk is ter verwezenlijking van de met deze richtlijn nagestreefde doelstellingen van algemeen belang, wordt door de lidstaten toegestaan uit hoofde van artikel 7 van Richtlijn 95/46/EG en Richtlijn 2002/58/EG, zoals in de nationale wetgeving ten uitvoer gelegd.

Artikel 2

Minimumharmonisatie

Onverminderd de krachtens het recht van de Unie op hen rustende verplichtingen worden de lidstaten er niet van weerhouden bepalingen die een hoger niveau van beveiliging waarborgen, aan te nemen of te handhaven.

Artikel 3

Definities

Voor de toepassing van deze richtlijn wordt verstaan onder:

(1) "netwerk- en informatiesysteem":

(a) een elektronischecommunicatienetwerk in de zin van Richtlijn 2002/21/EG; en

(b) een apparaat of groep van onderling verbonden of bij elkaar behorende apparaten, waarvan een of meer, overeenkomstig een programma, computergegevens automatisch verwerkt of verwerken; alsook

(c) computergegevens die met onder a) en b) bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan.

(2) "beveiliging": het vermogen van een netwerk- en informatiesysteem om met een bepaald niveau van betrouwbaarheid bestand te zijn tegen accidentele gebeurtenissen of opzettelijke handelingen die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen of verzonden gegevens of de daaraan gerelateerde diensten die via dat netwerk- en informatiesysteem worden aangeboden of toegankelijk zijn, in gevaar brengen;

(3) "risico": elke omstandigheid of gebeurtenis met een mogelijk schadelijk effect op de beveiliging;

[10] PB L 281 van 23.11.1995, blz. 31.
[11] SEC(2012) 72 final.

(4) "incident": elke omstandigheid of gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging;

(5) "dienst van de informatiemaatschappij": een dienst in de zin van artikel 1, punt 2, van Richtlijn 98/34/EG;

(6) "NIB-samenwerkingsplan": een plan waarin het kader voor organisatorische taken, verantwoordelijkheden en procedures is vastgesteld om de werking van netwerken en informatiesystemen te handhaven of te herstellen wanneer deze door een risico of incident worden getroffen;

(7) "incidentenbehandeling": alle procedures ter ondersteuning van de analyse en beheersing van en reactie op een incident;

(8) "marktdeelnemer":

(a) een aanbieder van diensten van de informatiemaatschappij die de verlening van andere diensten van de informatiemaatschappij mogelijk maken; een niet-exhaustieve lijst hiervan is opgenomen in bijlage II;

(b) een exploitant van kritische infrastructuur die essentieel is voor de handhaving van vitale economische en maatschappelijke activiteiten op het gebied van energie, vervoer, bankieren, effectenbeurzen en gezondheid; een niet-exhaustieve lijst hiervan is opgenomen in bijlage II;

(9) "norm": een norm als bedoeld in Verordening (EU) nr. 1025/2012;

(10) "specificatie": een specificatie als bedoeld in Verordening (EU) nr. 1025/2012;

(11) "aanbieder van vertrouwensdiensten": een natuurlijke of rechtspersoon die elektronische diensten aanbiedt bestaande uit het aanmaken, verifiëren, valideren, hanteren en bewaren van elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, elektronische documenten, elektronische bezorgingsdiensten, website-authenticatie en elektronische certificaten, met inbegrip van certificaten voor elektronische handtekeningen en voor elektronische zegels.

HOOFDSTUK II

NATIONALE KADERS VOOR NETWERK- EN INFORMATIEBEVEILIGING

Artikel 4

Beginsel

Overeenkomstig deze richtlijn waarborgen de lidstaten een hoog beveiligingsniveau van de netwerk- en informatiesystemen op hun grondgebied.

Artikel 5

Nationale NIB-strategie en nationaal NIB-samenwerkingsplan

1. Elke lidstaat stelt een nationale NIB-strategie vast waarin de strategische doelstellingen en de concrete beleids- en regelgevingsmaatregelen ter waarborging van een hoog niveau van netwerk- en informatiebeveiliging worden omschreven. De nationale NIB-strategie voorziet met name in het volgende:

(a) de bepaling van de doelstellingen en prioriteiten van de strategie op basis van een actuele risico- en incidentenanalyse.

(b) een governancekader ter verwezenlijking van de strategische doelstellingen en prioriteiten, met inbegrip van een duidelijke bepaling van de taken en verantwoordelijkheden van de overheidsorganen en de andere betrokken actoren;

(c) de aanwijzing van de algemene maatregelen inzake paraatheid, reactie en herstel, met inbegrip van mechanismen voor samenwerking tussen de publieke en de private sector.

(d) een vermelding van de scholings-, bewustmakings- en opleidingsprogramma's;

(e) plannen voor onderzoek en ontwikkeling en een beschrijving van de wijze waarop deze plannen de aangewezen prioriteiten weerspiegelen.

2. De nationale NIB-strategie omvat een nationaal NIB-samenwerkingsplan waarin ten minste het volgende is opgenomen:

(a) een risicobeoordelingsplan om risico's te vast te stellen en de impact van mogelijke incidenten te beoordelen;

(b) de omschrijving van de taken en verantwoordelijkheden van de verscheidene actoren die bij de uitvoering van het plan betrokken zijn;

(c) de omschrijving van samenwerkings- en communicatieprocessen die preventie, opsporing, reactie en herstel waarborgen en aan het alarmniveau zijn aangepast.

(d) een stappenplan voor NIB-oefeningen en -opleiding om het plan te versterken, valideren en testen. Praktijkervaringen moeten worden gedocumenteerd en in nieuwe aanpassingen van het plan worden verwerkt.

3. De nationale NIB-strategie en het nationale NIB-samenwerkingsplan worden binnen een maand na de vaststelling ervan aan de Commissie toegezonden.

Artikel 6

Nationale autoriteit voor de beveiliging van netwerk- en informatiesystemen

1. Elke lidstaat wijst een voor de beveiliging van netwerk- en informatiesystemen bevoegde nationale autoriteit (de "bevoegde autoriteit") aan.

2. De bevoegde autoriteiten monitoren de toepassing van deze richtlijn op nationaal niveau en dragen bij aan de consistente toepassing ervan in de Unie.

3. De lidstaten zorgen ervoor dat de bevoegde autoriteiten over de nodige technische, financiële en personele middelen beschikken om de hun toegewezen taken op doeltreffende en efficiënte wijze te kunnen verrichten en aldus de doelstellingen van deze richtlijn te verwezenlijken. De lidstaten zorgen ervoor dat de bevoegde autoriteiten op doeltreffende, efficiënte en veilige wijze samenwerken middels het in artikel 8 bedoelde netwerk.

4. De lidstaten zorgen ervoor dat de bevoegde autoriteiten de meldingen van incidenten van overheden en marktdeelnemers ontvangen overeenkomstig artikel 14, lid 2, en dat hun de in artikel 15 bedoelde uitvoerings- en handhavingsbevoegdheden worden verleend.

5. Indien nodig raadplegen de bevoegde autoriteiten de betrokken nationale wetshandhavingsinstanties en gegevensbeschermingsautoriteiten en werken zij daarmee samen.

6. Elke lidstaat stelt de Commissie onverwijld in kennis van de aanstelling van de bevoegde autoriteit, van haar taken, en van elke latere wijziging daarvan. Elke lidstaat maakt zijn aanwijzing van de bevoegde autoriteit openbaar.

Artikel 7

Computercrisisteams

1. Elke lidstaat zet een computercrisisteam ("Computer Emergency Response Team", hierna "CERT") op dat verantwoordelijk is voor de behandeling van incidenten en risico's, volgens een welomschreven proces dat voldoet aan de eisen van bijlage I.A, punt 1). Een CERT mag worden opgericht binnen de bevoegde autoriteit.

2. De lidstaten zorgen ervoor dat CERT's over de nodige technische, financiële en personele middelen beschikken om hun in bijlage I, punt 2, vastgestelde taken doeltreffend uit te voeren.

3. De lidstaten zorgen ervoor dat CERT's gebruikmaken van een beveiligde en veerkrachtige communicatie- en informatiestructuur op nationaal niveau, die compatibel en interoperabel is met het in artikel 9 bedoelde beveiligde informatie-uitwisselingssysteem.

4. De lidstaten informeren de Commissie over de middelen en het mandaat alsook over de incidentenbehandelingsprocedure van de CERT's.

5. Het CERT oefent zijn taken uit onder toezicht van de bevoegde autoriteit, die regelmatig de adequaatheid van de middelen, het mandaat en de doeltreffendheid van de incidentenbehandelingsprocedure ervan evalueert.

HOOFDSTUK III

SAMENWERKING TUSSEN BEVOEGDE AUTORITEITEN

Artikel 8

Samenwerkingsnetwerk

1. De bevoegde autoriteiten en de Commissie vormen een netwerk ("samenwerkingsnetwerk") om samen op te treden tegen risico's en incidenten met betrekking tot netwerk- en informatiesystemen.

2. Het samenwerkingsnetwerk brengt permanente communicatie tussen de Commissie en de bevoegde autoriteiten tot stand. Het Europees Agentschap voor netwerk- en informatiebeveiliging ("ENISA") staat het samenwerkingsnetwerk op verzoek bij met zijn deskundigheid en advies.

3. Binnen het samenwerkingsnetwerk doen de bevoegde autoriteiten het volgende:

   (a) zij verspreiden vroegtijdige waarschuwingen over risico's en incidenten overeenkomstig artikel 10;

   (b) zij zorgen voor een gecoördineerde reactie overeenkomstig artikel 11;

   (c) zij maken regelmatig niet-vertrouwelijke informatie over vroegtijdige waarschuwingen en gecoördineerde reacties die op dat moment worden verspreid of aan de gang zijn, bekend op een gemeenschappelijke website.

   (d) zij bespreken en beoordelen gezamenlijk, op verzoek van een lidstaat of van de Commissie, een of meer in artikel 5 bedoelde nationale NIB-strategieën en

nationale NIB-samenwerkingsplannen, binnen het toepassingsgebied van deze richtlijn.

(e) zij bespreken en beoordelen gezamenlijk, op verzoek van een lidstaat of van de Commissie, de doeltreffendheid van de CERT's, met name wanneer er NIB-oefeningen worden verricht op het niveau van de Unie;

(f) zij werken samen met en wisselen informatie over alle relevante kwesties uit met het Europees Centrum voor de bestrijding van cybercriminaliteit van Europol, en met andere relevante Europese instanties, met name op het gebied van gegevensbescherming, energie, vervoer, bankieren, effectenbeurzen en gezondheid;

(g) zij wisselen onderling en met de Commissie beste praktijken uit en verlenen elkaar bijstand bij het opbouwen van capaciteit op het gebied van NIB;

(h) zij organiseren regelmatig collegiale toetsingen met betrekking tot capaciteit en paraatheid;

(i) zij organiseren NIB-oefeningen op het niveau van de Unie en nemen indien passend deel aan internationale NIB-oefeningen.

4. De Commissie stelt, door middel van uitvoeringshandelingen, de nodige maatregelen vast om de in de leden 2 en 3 bedoelde samenwerking tussen de bevoegde autoriteiten en de Commissie te faciliteren. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 19, lid 2, bedoelde raadplegingsprocedure.

Artikel 9

Beveiligd informatie-uitwisselingssysteem

1. De uitwisseling van gevoelige en vertrouwelijke informatie binnen het samenwerkingsnetwerk moet plaatsvinden via een beveiligde infrastructuur.

2. De Commissie is bevoegd overeenkomstig artikel 18 gedelegeerde handelingen vast te stellen met betrekking tot de bepaling van de criteria die een lidstaat moet nakomen om aan het beveiligde informatie-uitwisselingsnetwerk te mogen deelnemen, wat betreft:

(a) de beschikbaarheid van beveiligde en veerkrachtige communicatie- en informatie-infrastructuur op nationaal niveau, die overeenkomstig artikel 7, lid 3, compatibel en interoperabel is met de beveiligde infrastructuur van het samenwerkingsnetwerk; en

(b) de aanwezigheid krachtens artikel 6, lid 3, artikel 7, lid 2, en artikel 7, lid 3, van de nodige technische, financiële en personele middelen en processen voor hun bevoegde autoriteit en CERT, om op doeltreffende, efficiënte en veilige wijze aan het beveiligde informatie-uitwisselingssysteem te kunnen deelnemen.

3. De Commissie stelt, door middel van uitvoeringshandelingen, besluiten inzake de toegang van de lidstaten tot deze beveiligde infrastructuur vast, krachtens de in de leden 2 en 3 bedoelde criteria. Die uitvoeringshandelingen worden volgens de in artikel 19, lid 3, bedoelde onderzoeksprocedure vastgesteld.

Artikel 10

Vroegtijdige waarschuwingen

1. De bevoegde autoriteiten of de Commissie geven binnen het samenwerkingsnetwerk vroegtijdige waarschuwingen over risico's en incidenten die aan ten minste een van de volgende voorwaarden voldoen:

   (a) zij nemen snel in omvang toe of kunnen snel in omvang toenemen;

   (b) zij gaan de nationale reactiecapaciteit te boven of kunnen die te boven gaan;

   (c) zij treffen meer dan een lidstaat of kunnen meer dan een lidstaat treffen.

2. De bevoegde autoriteiten en de Commissie doen de vroegtijdige waarschuwingen vergezeld gaan van alle relevante informatie waarover zij beschikken die nuttig kan zijn voor de beoordeling van het risico of incident.

3. De Commissie kan op verzoek van een lidstaat of op eigen initiatief een lidstaat verzoeken relevante informatie te verstrekken over een specifiek risico of incident.

4. Wanneer wordt vermoed dat het risico of incident dat het voorwerp van een vroegtijdige waarschuwing vormt, van criminele aard is, stellen de bevoegde autoriteiten of de Commissie het Europees Centrum voor de bestrijding van cybercriminaliteit van Europol in kennis.

5. De Commissie is bevoegd overeenkomstig artikel 18 gedelegeerde handelingen vast te stellen met betrekking tot de verdere omschrijving van de risico's en incidenten die aanleiding geven tot de in lid 1 bedoelde vroegtijdige waarschuwingen.

Artikel 11

Gecoördineerde reactie

1. Na een in artikel 10 bedoelde vroegtijdige waarschuwing komen de bevoegde autoriteiten, na de relevante informatie te hebben beoordeeld, een gecoördineerde reactie overeen overeenkomstig het in artikel 12 bedoelde NIB-plan van de Unie.

2. De diverse maatregelen die als gevolg van de gecoördineerde actie op nationaal niveau worden vastgesteld, worden aan het samenwerkingsnetwerk meegedeeld.

Artikel 12

NIB-samenwerkingsplan van de Unie

1. De Commissie is bevoegd, middels uitvoeringshandelingen, een NIB-samenwerkingsplan van de Unie vast te stellen. Die uitvoeringshandelingen worden volgens de in artikel 19, lid 3, bedoelde onderzoeksprocedure vastgesteld.

2. Het NIB-samenwerkingsplan van de Unie voorziet in het volgende:

   (a) voor de toepassing van artikel 10:

      – een bepaling van het formaat en de procedures voor de vergaring en de uitwisseling van compatibele en vergelijkbare informatie over risico's en incidenten door de bevoegde autoriteiten;

      – een bepaling van de procedures en de criteria voor de beoordeling van de risico's en incidenten door het samenwerkingsnetwerk;

(b) de procedures die moeten worden gevolgd voor de gecoördineerde reacties krachtens artikel 11, met inbegrip van de vaststelling van taken en verantwoordelijkheden en samenwerkingsprocedures;

(c) een stappenplan voor NIB-oefeningen en -opleiding om het plan te versterken, te valideren en te testen;

(d) een programma voor de overdracht van kennis tussen de lidstaten met betrekking tot capaciteitsopbouw en intercollegiaal leren;

(e) een programma voor bewustmaking en opleiding tussen de lidstaten.

3. Het NIB-samenwerkingsplan van de Unie wordt uiterlijk een jaar na de inwerkingtreding van deze richtlijn vastgesteld en wordt regelmatig getoetst.

Artikel 13

Internationale samenwerking

Onverminderd de mogelijkheid van het samenwerkingsnetwerk om op informele basis internationaal samen te werken, kan de Unie internationale overeenkomsten met derde landen of internationale organisaties sluiten waarbij hun deelname aan bepaalde activiteiten van het samenweringsnetwerk mogelijk wordt gemaakt en georganiseerd. Zulke overeenkomsten houden rekening met de noodzaak om afdoende bescherming te waarborgen van de persoonsgegevens die in het samenwerkingsnetwerk circuleren.

HOOFDSTUK IV

BEVEILIGING VAN DE NETWERKEN EN OVERHEDEN EN MARKTDEELNEMERS

Artikel 14

Beveiligingseisen en melding van incidenten

1. De lidstaten zorgen ervoor dat overheden en marktdeelnemers passende technische en organisatorische maatregelen nemen ter beheersing van de risico's voor de beveiliging van de netwerken en informatiesystemen die zij controleren en bij hun activiteiten gebruiken. Deze maatregelen zorgen, rekening houdend met de meest recente technische mogelijkheden, voor een beveiligingsniveau dat is afgestemd op de risico's die zich voordoen. Overheden en marktdeelnemers nemen met name maatregelen om de impact te voorkomen en te minimaliseren van incidenten met betrekking tot hun netwerk- en informatiesysteem op de door hen verleende kerndiensten en aldus te zorgen voor de continuïteit van de op die netwerken en informatiesystemen gebaseerde diensten.

2. De lidstaten zorgen ervoor dat overheden en marktdeelnemers incidenten met een aanzienlijke impact op de beveiliging van de door hen verleende kerndiensten aan de bevoegde autoriteiten melden.

3. De eisen van de leden 1 en 2 zijn van toepassing op alle marktdeelnemers die diensten verlenen in de Europese Unie.

4. De bevoegde autoriteit kan het publiek informeren of overheden en marktdeelnemers daartoe verplichten wanneer zij oordeelt dat openbaarmaking van het incident in het algemeen belang is. Eenmaal per jaar dient de bevoegde autoriteit bij het

samenwerkingsnetwerk een samenvattend verslag in over de meldingen die zij heeft ontvangen en de maatregelen die overeenkomstig dit lid zijn genomen.

5. De Commissie is bevoegd overeenkomstig artikel 18 gedelegeerde handeling vast te stellen met betrekking tot de omschrijving van de omstandigheden waarin overheden en marktdeelnemers incidenten moeten melden.

6. Onverminderd elke krachtens lid 5 vastgestelde gedelegeerde handeling kunnen de bevoegde autoriteiten richtsnoeren vaststellen en, zo nodig, instructies geven met betrekking tot de omstandigheden waarin overheden en marktdeelnemers incidenten moeten melden.

7. De Commissie is bevoegd om, door middel van gedelegeerde handelingen, de formaten en procedures die gelden voor de toepassing van lid 2 vast te stellen. Die uitvoeringshandelingen worden volgens de in artikel 19, lid 3, bedoelde onderzoeksprocedure vastgesteld.

8. De leden 1 en 2 zijn niet van toepassing op micro-ondernemingen zoals gedefinieerd in Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen[12].

Artikel 15

Uitvoering en handhaving

1. De lidstaten zorgen ervoor dat de bevoegde autoriteiten de nodige bevoegdheden hebben om niet-naleving van de krachtens artikel 14 op overheden of marktdeelnemers rustende verplichtingen en de effecten daarvan op de beveiliging van netwerken en informatiesystemen te onderzoeken.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten de bevoegdheid hebben om marktnemers en overheden ertoe te verplichten:

   (a) de informatie te verschaffen die nodig is om de beveiliging van hun netwerken en informatiesystemen te beoordelen, met inbegrip van gedocumenteerde beleidsmaatregelen op het gebied van beveiliging;

   (b) een door een gekwalificeerde onafhankelijke instantie of nationale autoriteit uitgevoerde beveiligingsaudit te ondergaan en de resultaten daarvan ter beschikking te stellen van de bevoegde autoriteit.

3. De lidstaten zorgen ervoor dat de bevoegde autoriteiten de bevoegdheid hebben om marktdeelnemers en overheden bindende instructies te geven.

4. De bevoegde autoriteiten melden de autoriteiten voor wetshandhaving incidenten waarvan wordt vermoed dat zij van ernstig criminele aard zijn.

5. De bevoegde autoriteiten werken nauw samen met de autoriteiten voor gegevensbescherming om incidenten aan te pakken die inbreuken in verband met persoonsgegevens tot gevolg hebben.

6. De lidstaten zorgen ervoor dat uit hoofde van dit hoofdstuk aan overheden en marktdeelnemers opgelegde verplichtingen aan rechterlijke toetsing kunnen worden onderworpen.

[12] PB L 124 van 20.5.2003, blz. 36.

Artikel 16

Normalisatie

1. Met het oog op de geharmoniseerde uitvoering van artikel 14, lid 1, moedigen de lidstaten het gebruik van normen en/of specificaties voor netwerk- en informatiebeveiliging aan.

2. De Commissie stelt, door middel van uitvoeringshandelingen, een lijst op van de in lid 1 bedoelde normen. De lijst wordt bekendgemaakt in het *Publicatieblad van de Europese Unie*.

HOOFDSTUK V

SLOTBEPALINGEN

Artikel 17

Sancties

1. De lidstaten stellen regels vast voor sancties op overtredingen op nationale bepalingen die ingevolge deze richtlijn zijn vastgesteld, en nemen alle nodige maatregelen om ervoor te zorgen dat zij worden uitgevoerd. De sancties moeten doeltreffend, evenredig en afschrikkend zijn. De lidstaten stellen de Commissie uiterlijk op de omzettingsdatum van deze richtlijn van deze bepalingen in kennis en delen haar eventuele latere wijzigingen onverwijld mee.

2. De lidstaten zorgen ervoor dat wanneer een beveiligingsincident betrekking heeft op persoonsgegevens, de voorgeschreven sancties in overeenstemming zijn met de sancties waarin wordt voorzien in de verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[13].

Artikel 18

Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.

2. De bevoegdheid om de in artikel 9, lid 2, artikel 10, lid 5, en artikel 14, lid 5, bedoelde gedelegeerde handelingen vast te stellen, wordt aan de Commissie verleend. De Commissie stelt uiterlijk negen maanden vóór het einde van de termijn van 5 jaar een verslag op over de bevoegdheidsdelegatie. De bevoegdheidsdelegatie wordt stilzwijgend met termijnen van dezelfde duur verlengd, tenzij het Europees Parlement of de Raad zich uiterlijk drie maanden voor het einde van elke termijn tegen deze verlenging verzet.

3. Het Europees Parlement of de Raad kan de in artikel 9, lid 2, artikel 10, lid 5, en artikel 14, lid 5, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheden. Het wordt van kracht op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie* of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

[13] SEC(2012) 72 final.

4. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.

5. Een overeenkomstig artikel 9, lid 2, artikel 10, lid 5, en artikel 14, lid 5, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement of de Raad binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad daartegen geen bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad vóór het verstrijken van de termijn van twee maanden de Commissie hebben medegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee maanden verlengd.

Artikel 19

Comitéprocedure

1. De Commissie wordt bijgestaan door een comité (het comité Netwerk- en informatiebeveiliging). Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.

2. Wanneer naar dit lid wordt verwezen, is artikel 4 van Verordening (EU) nr. 182/2011 van toepassing.

3. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

Artikel 20

Evaluatie

De Commissie evalueert de werking van deze richtlijn en brengt verslag uit aan het Europees Parlement en de Raad. Het eerste verslag wordt uiterlijk drie jaar na de in artikel 21 bedoelde omzettingsdatum ingediend. Daartoe kan de Commissie de lidstaten verzoeken onverwijld informatie te verstrekken.

Artikel 21

Omzetting

1. De lidstaten dienen uiterlijk [anderhalf jaar na de aanneming] de nodige wettelijke en bestuursrechtelijke bepalingen vast te stellen en bekend te maken om aan deze richtlijn te voldoen. Zij delen de Commissie de tekst van die bepalingen onverwijld mede.

   Zij passen deze bepalingen toe met ingang van [anderhalf jaar na de aanneming].

   Wanneer de lidstaten deze bepalingen aannemen, wordt in de bepalingen zelf of bij de officiële bekendmaking daarvan naar deze richtlijn verwezen. De regels voor deze verwijzing worden vastgesteld door de lidstaten.

2. De lidstaten delen de Commissie de tekst mee van de voornaamste bepalingen van intern recht die zij vaststellen op het door deze richtlijn bestreken gebied.

Artikel 22

Inwerkingtreding

Deze richtlijn treedt in werking op de [twintigste] dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Artikel 23

Geadresseerden

Deze richtlijn is gericht tot de lidstaten.

Gedaan te Brussel,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*

BIJLAGE 1

Voorschriften en taken voor het computercrisisteam (CERT)

De voorschriften en taken voor het CERT moeten adequaat en duidelijk worden gedefinieerd en worden ondersteund door nationale beleids- en/of regelgevingsmaatregelen. Deze dienen de volgende elementen te omvatten:

(1) voorschriften voor het CERT:

(a) het CERT garandeert een hoge mate van beschikbaarheid van zijn communicatiediensten door zwakke punten (*single points of failure*) te voorkomen, en kan langs diverse kanalen worden bereikt of contact opnemen. Bovendien moeten de communicatiekanalen duidelijk worden gespecificeerd en bekend zijn bij de CERT-gebruikers (*constituency*) en de samenwerkingspartners;

(b) het CERT zorgt voor de tenuitvoerlegging en het beheer van beveiligingsmaatregelen om de vertrouwelijkheid, integriteit, beschikbaarheid en authenticiteit van de informatie die het ontvangt en behandelt te waarborgen;

(c) de kantoren van het CERT en de ondersteunende informatiesystemen moeten zich op beveiligde locaties bevinden;

(d) er wordt een kwaliteitszorgsysteem ingevoerd om de prestatie van het CERT te volgen en een gestaag proces van verbetering te garanderen. Dit systeem moet zijn gebaseerd op duidelijk omschreven metrieken, zoals formele dienstniveaus en essentiële prestatie-indicatoren;

(e) bedrijfscontinuïteit:

– het CERT wordt, met het oog op vlotte overdrachten, uitgerust met een adequaat systeem voor het beheren en routeren van verzoeken,

– het CERT krijgt voldoende personeel om een volcontinue beschikbaarheid te garanderen,

– de continuïteit van de infrastructuur die het werk van het CERT ondersteunt, wordt gewaarborgd. Hiertoe wordt voorzien in redundante systemen en reservewerkruimten teneinde een permanente toegang tot de communicatiemiddelen te garanderen;

(2) taken van het CERT:

(a) de taken van het CERT behelzen ten minste het volgende:

– monitoren van incidenten op nationaal niveau,

– ten bate van de betrokken belanghebbende partijen zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten,

– reageren op incidenten,

– zorgen voor een dynamische risico- en incidentanalyse en situatiekennis,

– het publiek bewust maken van de met onlineactiviteiten verbonden risico's,

– het organiseren van campagnes over NIB;

(b) het CERT legt op samenwerking gerichte contacten met de particuliere sector;

(c) ter bevordering van de samenwerking stimuleert het CERT de vaststelling en het gebruik van gemeenschappelijke of gestandaardiseerde praktijken op het gebied van:

- procedures voor de behandeling van incidenten en risico's,
- systemen voor de classificatie van incidenten, risico's en informatie,
- indelingssystemen voor metrieken,
- formaten voor uitwisseling van informatie over risico's, incidenten en naamconventies voor systemen.

BIJLAGE II

Lijst van marktdeelnemers

Zoals bedoeld in artikel 3, lid 8, onder a):

1. Platforms voor elektronische handel

2. Gateways voor internetbetalingen

3. Sociaalnetwerksites

4. Zoekmachines

5. Cloudcomputingdiensten

6. Internetwinkels die applicaties aanbieden

Zoals bedoeld in artikel 3, lid 8, onder b):

1. Energie

- elektriciteits- en gasleveranciers,
- exploitanten en aan de eindconsument leverende retailers van elektriciteits- en/of gasdistributiesystemen,
- exploitanten van aardgastransmissiesystemen, exploitanten van aardgasopslag en LNG-exploitanten,
- exploitanten van elektriciteitstransmissiesystemen,
- oliepijpleidingen en olieopslag,
- exploitanten die actief zijn op de elektriciteits- en de gasmarkt,
- exploitanten van voorzieningen voor de productie, raffinage en behandeling van olie en aardgas

2. Vervoer

- luchtvaartmaatschappijen (voor vracht en passagiers),
- bedrijven voor maritiem vervoer (kust- en zeevervoer van passagiers en vracht),
- spoorwegbedrijven (infrastructuurbeheerders, geïntegreerde bedrijven en exploitanten van spoorvervoer),
- luchthavens,
- havens,
- exploitanten op het gebied van verkeersbeheer en -controle,
- ondersteunende logistieke diensten: a) opslag , b) vrachtafhandeling en c) andere transportondersteunende activiteiten

3. Bankwezen: kredietinstellingen in de zin van artikel 4, punt 1, van Richtlijn 2006/48/EG.

4. Infrastructuur voor de financiële markt: beurzen en als centrale tegenpartij fungerende clearinginstellingen.

5. Gezondheidszorg: zorginstellingen (waaronder ziekenhuizen en privéklinieken) en andere zorgverleners.

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

1.2. Betrokken beleidsterrein(en) in de ABM/ABB-structuur

1.3. Aard van het voorstel/initiatief

1.4. Doelstellingen

1.5. Motivering van het voorstel/initiatief

1.6. Duur en financiële gevolgen

1.7. Beheersvorm(en)

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

2.2. Beheers- en controlesysteem

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarig financieel kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

3.2.2. Geraamde gevolgen voor de beleidskredieten

3.2.3. Geraamde gevolgen voor de administratieve kredieten

3.2.4. Verenigbaarheid met het huidig meerjarig financieel kader

3.2.5. Bijdrage van derden aan de financiering

3.3. Geraamde gevolgen voor de ontvangsten

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Voorstel voor een Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen.

1.2. Betrokken beleidsterrein(en) in de ABM/ABB-structuur[37]

- 09 - Communicatienetwerken, inhoud en technologie

1.3. Aard van het voorstel/initiatief

☒ Het voorstel/initiatief betreft **een nieuwe actie**

☐ Het voorstel/initiatief betreft **een nieuwe actie na een proefproject/een voorbereidende actie**[38]

☐ Het voorstel/initiatief betreft **de verlenging van een bestaande actie**

☐ Het voorstel/initiatief betreft **een actie die wordt omgebogen naar een nieuwe actie**

1.4. Doelstellingen

1.4.1. Met het voorstel/initiatief beoogde strategische meerjarendoelstelling(en) van de Commissie

Het oogmerk van de voorgestelde richtlijn is een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging (NIB) in de EU te waarborgen.

1.4.2. Specifieke doelstellingen en betrokken ABM/ABB-activiteit(en)

In het voorstel zijn maatregelen vastgesteld om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen.

De specifieke doelstellingen zijn:

1. Een minimumniveau voor NIB in de lidstaten bepalen en zo het algemene paraatheids- en reactieniveau verhogen.

2. De samenwerking binnen de EU op het gebied van NIB verbeteren teneinde grensoverschrijdende incidenten en dreigingen efficiënt te bestrijden. Er zal een beveiligde informatie-uitwisselingsinfrastructuur worden opgezet die de uitwisseling van gevoelige en vertrouwelijke informatie tussen de bevoegde autoriteiten mogelijk maakt.

3. Een cultuur van risicobeheer creëren en de uitwisseling van informatie tussen de particuliere en de openbare sector verbeteren.

Betrokken ABM/ABB-activiteit(en)

De richtlijn is van toepassing op entiteiten (bedrijven en organisaties, met inbegrip van enkele kmo's) in een aantal sectoren (energie, vervoer, kredietinstellingen en beurzen, gezondheidszorg en facilitatoren van essentiële internetdiensten) en op overheden. In de richtlijn zijn ook verbanden met wetshandhaving en gegevensbescherming aan de orde, net als NIB-aspecten van externe betrekkingen.

- 09 - Communicatienetwerken, inhoud en technologie

[37] ABM: Activity Based Management – ABB: Activity Based Budgeting.

[38] In de zin van artikel 49, lid 6, onder a) of b), van het Financieel Reglement.

- 02 - Ondernemingen

- 32 - Energie

- 06 - Mobiliteit en vervoer

- 17 - Gezondheidszorg en consumentenbescherming

- 18 - Binnenlandse zaken

- 19 - Externe betrekkingen

- 33 - Justitie

- 12 - Interne markt

1.4.3. Verwachte resulta(a)t(en) en gevolg(en)

Vermeld de gevolgen die het voorstel/initiatief zou moeten hebben op de begunstigden/doelgroepen.

Consumenten, ondernemingen en overheden in de EU zouden aanzienlijk beter tegen NIB-incidenten, -dreigingen en -risico's worden beschermd.

Nadere gegevens zijn te vinden onder punt 8.2 (Impact van optie 2 - Regelgeving) van het werkdocument van de diensten van de Commissie met de effectbeoordeling, dat bij dit wetgevingsvoorstel is gevoegd.

1.4.4. Resultaat- en effectindicatoren

Vermeld de indicatoren aan de hand waarvan kan worden nagegaan in hoeverre het voorstel/initiatief is uitgevoerd.

De indicatoren voor toezicht en evaluatie zijn te vinden onder punt 10 van de effectbeoordeling.

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoeften waarin op korte of lange termijn moet worden voorzien

Elke lidstaat dient te beschikken over:

- een nationale NIB-strategie;

- een NIB-samenwerkingsplan;

- een voor NIB bevoegde nationale autoriteit, en

- een computercrisisteam (Computer Emergency Response Team – CERT).

Op EU-niveau moeten de lidstaten samenwerken via een netwerk.

Overheden en essentiële particuliere spelers worden ertoe verplicht NIB-risico's te beheren en incidenten met een aanzienlijke impact te rapporteren bij de bevoegde autoriteiten.

1.5.2. Toegevoegde waarde van de deelname van de EU

Gezien het grensoverschrijdende karakter van NIB vormen verschillen in de desbetreffende wetgevings- en beleidslijnen een belemmering voor bedrijven die hun activiteit tot meerdere landen willen uitbreiden en staan zij het realiseren van wereldwijde schaalvoordelen in de weg. Wanneer de EU niet optreedt, zou een situatie ontstaan waarin elke lidstaat alleen maatregelen neemt en geen rekening wordt gehouden met de verwevenheid van de netwerk- en informatiesystemen.

De vooropgestelde doelstellingen kunnen beter op EU-niveau worden bereikt dan door de afzonderlijke lidstaten.

1.5.3. Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan

Het voorstel vloeit voort uit de analyse dat wettelijke verplichtingen vereist zijn om een gelijk speelveld te creëren en lacunes in de wetgeving te dichten. De louter op vrijwilligheid gebaseerde aanpak die tot dusverre is gevolgd, heeft slechts een minderheid van lidstaten, elk met een hoog capaciteitsniveau, tot samenwerking gestimuleerd.

1.5.4. Samenhang en eventuele synergie met andere relevante instrumenten

Het voorstel is volledig in overeenstemming met de Digitale agenda voor Europa en bijgevolg ook met de Europa 2020-strategie. Het sluit aan bij en vormt een aanvulling op het EU-regelgevingskader inzake elektronische communicatie, de EU-richtlijn over Europese kritieke infrastructuur en de EU-richtlijn inzake gegevensbescherming.

Dit voorstel wordt gepresenteerd samen met de mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid over een Europese strategie voor cyberbeveiliging, en maakt een essentieel onderdeel daarvan uit.

1.6. Duur en financiële gevolgen

– ☐ Voorstel/initiatief met een beperkte geldigheidsduur

– ☐ Voorstel/initiatief van kracht vanaf [DD/MM]JJJJ tot en met [DD/MM]JJJJ

– ☐ Financiële gevolgen vanaf JJJJ tot en met JJJJ

– ☒ Voorstel/initiatief met een onbeperkte geldigheidsduur

– De omzettingsperiode van 18 maanden gaat onmiddellijk na de vaststelling (naar schatting in 2015) van start. Met de tenuitvoerlegging van de richtlijn zal echter al na de vaststelling worden begonnen, onder meer door de beveiligde infrastructuur die de samenwerking tussen de lidstaten moet ondersteunen, op te zetten.

– gevolgd door een volledige uitvoering.

1.7. Beheersvormen[39]

– ☒ Direct gecentraliseerd beheer door de Commissie

– ☒ Indirect gecentraliseerd beheer door uitvoeringstaken te delegeren aan:

– ☐uitvoerende Agentschappen

– ☒ door de Unie opgerichte organen[40]

– ☐ nationale publiekrechtelijke organen of organen met een openbaredienstverleningstaak

– ☐ personen aan wie de uitvoering van specifieke acties in het kader van titel V van het Verdrag betreffende de Europese Unie is toevertrouwd en die worden genoemd in het betrokken basisbesluit in de zin van artikel 49 van het Financieel Reglement

– ☐ Gedeeld beheer met lidstaten

– ☐ Gedecentraliseerd beheer met derde landen

– ☐ Gezamenlijk beheer met internationale organisaties, met inbegrip van het Europees Ruimteagentschap

Verstrek, indien meer dan een beheersvorm is aangekruist, extra informatie onder "Opmerkingen".

Opmerkingen
ENISA, een door de Gemeenschappen in het leven geroepen agentschap, kan de lidstaten en de Commissie bijstaan bij de tenuitvoerlegging van de richtlijn, en wel op basis van zijn mandaat en middels de herverdeling van de middelen die binnen het meerjarig financieel kader 2014-2020 zijn geoormerkt voor dit agentschap.

[39] Nadere gegevens over de beheersvormen en verwijzingen naar het Financieel Reglement zijn beschikbaar op BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] In de zin van artikel 185 van het Financieel Reglement.

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Vermeld frequentie en voorwaarden.

Op gezette tijden evalueert de Commissie de werking van deze richtlijn en brengt zij daarover verslag uit aan het Europees Parlement en de Raad.

De Commissie zal tevens nagaan of de lidstaten de richtlijn correct omzetten.

Het voorstel betreffende de financieringsfaciliteit voor Europese verbindingen voorziet ook in de mogelijkheid de wijze waarop projecten zijn uitgevoerd en het effect van de uitvoering daarvan te evalueren, teneinde te beoordelen of de beoogde doelstellingen, onder meer inzake milieubescherming, zijn bereikt.

2.2. Beheers- en controlesysteem

2.2.1. Geconstateerd risico

- de uitvoering van het project kan vertraging oplopen bij de aanleg van de beveiligde infrastructuur.

2.2.2. Controlemiddelen

In de overeenkomsten en besluiten tot uitvoering van de acties in het kader van de financieringsfaciliteit voor Europese verbindingen zal worden voorzien in toezicht en financiële controle door de Commissie of een door de Commissie daartoe gemachtigde vertegenwoordiger, in audits door de Rekenkamer en in controles ter plaatse door het Europees Bureau voor fraudebestrijding (OLAF).

2.2.3. Kosten en baten van controles en waarschijnlijk niveau van niet-naleving

Risicogebaseerde controles vooraf en achteraf en de mogelijkheid van audits ter plaatse moeten ervoor zorgen dat de kosten van controles redelijk blijven.

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

Vermeld de bestaande en geplande preventie- en beschermingsmaatregelen.

De Commissie neemt passende maatregelen om ervoor te zorgen dat bij de uitvoering van de uit hoofde van deze richtlijn gefinancierde actie de financiële belangen van de Unie met de toepassing van preventieve maatregelen tegen fraude, corruptie en andere onwettige activiteiten worden beschermd door middel van doeltreffende controles en, indien onregelmatigheden worden ontdekt, door middel van terugvordering van de ten onrechte betaalde bedragen en, voor zover van toepassing, door middel van doeltreffende, evenredige en afschrikkende sancties.

De Commissie of haar vertegenwoordigers en de Rekenkamer hebben de bevoegdheid om audits, op basis van documenten of ter plaatse, uit te voeren bij alle begunstigden, contractanten en subcontractanten die uit hoofde van het programma middelen van de Unie hebben ontvangen.

Het Europees Bureau voor fraudebestrijding (OLAF) kan overeenkomstig de procedures van Verordening (Euratom, EG) nr. 2185/96 controles en verificaties ter plaatse bij de direct of indirect bij de financiering betrokken economische subjecten uitvoeren om vast te stellen of er sprake is van fraude, corruptie of andere onwettige activiteiten in verband met een subsidieovereenkomst of -besluit of een contract

betreffende financiering door de Unie, waardoor de financiële belangen van de Unie zijn geschaad.

Onverminderd de voorgaande alinea's verlenen de uit deze verordening voortvloeiende samenwerkingsovereenkomsten met derde landen en internationale organisaties, subsidieovereenkomsten en -besluiten en contracten de Commissie, de Rekenkamer en OLAF uitdrukkelijk de bevoegdheid om dergelijke audits en controles en verificaties ter plaatse uit te voeren.

De financieringsfaciliteit voor Europese verbindingen voorziet in de mogelijkheid om als basis voor subsidie- en aanbestedingscontracten gebruik te maken van standaardmodellen waarin de algemeen geldende fraudebestrijdingsmaatregelen worden vastgesteld.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarig financieel kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

- Bestaande begrotingsonderdelen

In volgorde van de rubrieken van het meerjarig financieel kader en de begrotingsonderdelen

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Soort uitgave	Bijdrage			
	Nummer [Omschrijving……...……]	GK/NGK (41)	van EVA-landen[42]	van kandidaat-lidstaten[43]	van derde landen	in de zin van artikel 18, lid 1, onder a bis), van het Financieel Reglement
	09 03 02 De interconnectie en interoperabiliteit van nationale online-overheidsdiensten bevorderen, alsook de toegang tot dergelijke netwerken.	GK	NEEN	NEEN	NEEN	NEEN

- Te creëren nieuwe begrotingsonderdelen (niet van toepassing)

In volgorde van de rubrieken van het meerjarig financieel kader en de begrotingsonderdelen

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Soort uitgave	Bijdrage			
	Nummer [Omschrijving…..……..]	GK/NGK	van EVA-landen	van kandidaat-lidstaten	van derde landen	in de zin van artikel 18, lid 1, onder a bis), van het Financieel Reglement
	[XX.YY.YY.YY]		JA/NEEN	JA/NEEN	JA/NEEN	JA/NEEN

41 GK = gesplitste kredieten/NGK = niet-gesplitste kredieten.

42 EVA: Europese Vrijhandelsassociatie.

43 Kandidaat-lidstaten en, in voorkomend geval, potentiële kandidaat-lidstaten van de Westelijke Balkan.

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

in miljoenen euro's (tot op 3 decimalen)

Rubriek van het meerjarig financieel kader	1	Slimme en inclusieve groei

DG: <…….>			2015* [44]	Jaar **2016**	Jaar **2017**	Jaar **2018**	Daaropvolgende jaren (2019-2021) en later			**TOTAAL**
• Beleidskredieten										
09 03 02	Vastleggingen	(1)	1,250**	0,000						**1,250**
	Betalingen	(2)	0,750	0,250	0,250					**1,250**
Uit het budget van specifieke programma's gefinancierde administratieve kredieten[45]			**0.000**							**0,000**
Nummer begrotingsonderdeel		(3)	**0,000**							**0,000**
TOTAAL kredieten voor DG <…….>	Vastleggingen	=1+1a +3	1,250	0,000						**1,250**
	Betalingen	=2+2a +3	0,750	0,250	0,250					**1,250**

• TOTAAL beleidskredieten	Vastleggingen	(4)	1,250	0,000						**1,250**
	Betalingen	(5)	0,750	0,250	0,250					**1,250**
• TOTAAL uit het budget van specifieke programma's		(6)	**0,000**							

[44] Het jaar N is het jaar waarin met de uitvoering van het voorstel/initiatief wordt begonnen.

[45] Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek door derden, eigen onderzoek.

gefinancierde administratieve kredieten										
TOTAAL kredieten van RUBRIEK 1 van het meerjarig financieel kader	Vastleggingen	=4+ 6	1,250	0,000						**1,250**
	Betalingen	=5+ 6	0,750	0,250	0,250					**1,250**

* Het precieze tijdschema hangt af van de datum waarop het wetgevende gezag het voorstel vaststelt (i.e. als de richtlijn in 2014 wordt goedgekeurd, wordt in 2015 met de aanpassing van de bestaande infrastructuur begonnen; zo niet, een jaar later).

** Als de lidstaten ervoor opteren bestaande infrastructuur te gebruiken en de eenmalige aanpassingskosten ten laste van de EU-begroting te brengen, zoals wordt toegelicht in de punten 1.4.3 en 1.7, worden de kosten om een netwerk zo aan te passen dat het de samenwerking tussen de lidstaten overeenkomstig hoofdstuk III van de richtlijn (vroegtijdige waarschuwingen, gecoördineerde reactie, enz.) kan ondersteunen, geraamd op EUR 1 250 000. Dit bedrag gaat dat in de effectbeoordeling (ca. EUR 1 miljoen) iets te boven aangezien het is gebaseerd op een nauwkeuriger raming van de voor een dergelijke infrastructuur benodigde bouwstenen. Het JRC, dat ervaring heeft met de ontwikkeling van vergelijkbare systemen voor andere sectoren, zoals volksgezondheid, heeft een raming gemaakt van de benodigde bouwstenen en de desbetreffende kosten daarvan en is tot het volgende resultaat gekomen: een systeem voor snelle waarschuwing en melding met betrekking tot NIB (EUR 275 000), een informatie-uitwisselingsplatform (EUR 400 000), een systeem voor vroegtijdige waarschuwing en reactie (EUR 275 000) en een situatiecentrum (EUR 300 000), alles samen voor in totaal EUR 1 250 000. Een nader uitgewerkt uitvoeringsplan zal naar verwachting worden voorgelegd in de studie die in het kader van het specifieke contract SMART 2012/0010 zal worden verricht naar de haalbaarheid en de voorbereiding van de tenuitvoerlegging van een Europees systeem voor vroegtijdige waarschuwing en reactie met betrekking tot cyberaanvallen en -verstoringen.

Wanneer het voorstel/initiatief gevolgen heeft voor meerdere rubrieken:

• TOTAAL beleidskredieten	Vastleggingen	(4)	0,000	0,000						
	Betalingen	(5)	0,000	0,000						
• TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten		(6)	**0.000**	**0,000**						
TOTAAL kredieten van de RUBRIEKEN 1 tot en met 4 van het meerjarig financieel kader (Referentiebedrag)	Vastleggingen	=4+ 6	1,250	0,000						1,250
	Betalingen	=5+ 6	0,750	0,250	0,250					1,250

Rubriek van het meerjarig financieel kader	**5**	"Administratieve uitgaven"

in miljoenen euro's (tot op 3 decimalen)

		Jaar **2015**	Jaar **2016**	Jaar **2017**	Jaar **2018**	Daaropvolgende jaren (2019-2021) en later			**TOTAAL**
DG: CNECT									
• Personele middelen		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Andere administratieve uitgaven		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
TOTAAL DG CNECT	Kredieten	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

TOTAAL kredieten voor RUBRIEK 5 van het meerjarig financieel kader	(totaal vastleggingen = totaal betalingen)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5.430**

in miljoenen euro's (tot op 3 decimalen)

		Jaar **2015**[46]	Jaar **2016**	Jaar **2017**	Jaar **2018**	Daaropvolgende jaren (2019-2021) en later			**TOTAAL**
TOTAAL kredieten van de RUBRIEKEN 1 tot en met 5 van het meerjarig financieel kader	Vastleggingen	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6.680**
	Betalingen	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6.680**

[46] Het jaar N is het jaar waarin met de uitvoering van het voorstel/initiatief wordt begonnen.

3.2.2. Geraamde gevolgen voor de beleidskredieten

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☑ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

– Vastleggingskredieten (miljoen EUR, tot op 3 decimalen)

Vermeld doelstellingen en outputs ⇩			Jaar **2015***		Jaar **2016**		Jaar **2017**		Jaar **2018**		Daaropvolgende jaren (2019-2021) en later				**TOTAAL**	
			OUTPUTS													
	Soort output[47]	Gem. kosten	Aantal outputs	Kosten	Aantal outputs	Kosten	Aantal outputs	Kosten	Aantal outputs	Kosten	Aantal outputs	Kosten	Aantal outputs	Kosten	Totaal aantal outputs	Totaal kosten
SPECIFIEKE DOELSTELLING NR. 2[48] Beveiligde infrastructuur voor informatie-uitwisseling																
- Output	Aan-passing infra-structuur															
Subtotaal voor specifieke doelstelling nr. 2			1	1,250**											1	1,250
TOTALE KOSTEN				1,250												1,250

47 Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen, enz.).

48 Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…".

* Het precieze tijdschema hangt af van de datum waarop het wetgevende gezag het voorstel vaststelt (i.e. als de richtlijn in 2014 wordt goedgekeurd, wordt in 2015 met de aanpassing van de bestaande infrastructuur begonnen; zo niet, een jaar later).

** Zie punt 3.2.1.

3.2.3. Geraamde gevolgen voor de administratieve kredieten

3.2.3.1. Samenvatting

– ☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

– ☑ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

in miljoenen euro's (tot op 3 decimalen)

	Jaar **2015**[49]	Jaar **2016**	Jaar **2017**	Jaar **2018**	Daaropvolgende jaren (2019-2021) en later			**TOTAAL**
RUBRIEK 5 van het meerjarig financieel kader								
Personele middelen	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Andere administratieve uitgaven	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Subtotaal RUBRIEK 5 van het meerjarig financieel kader	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
Buiten RUBRIEK 5[50] **van het meerjarig financieel kader**								
Personele middelen	0,000	0,000						**0,000**
Andere administratieve uitgaven								
Subtotaal buiten RUBRIEK 5 van het meerjarig financieel kader	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
TOTAAL	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

In de benodigde administratieve kredieten zal worden voorzien door de kredieten van DG CNECT die reeds voor het beheer van deze actie zijn toegewezen en/of in het DG zijn herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de bestaande budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

49 Het jaar N is het jaar waarin met de uitvoering van het voorstel/initiatief wordt begonnen.

50 Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek door derden, eigen onderzoek.

ENISA, het Europees Agentschap voor netwerk- en informatiebeveiliging, kan de lidstaten en de Commissie bijstaan bij de tenuitvoerlegging van de richtlijn, en wel op basis van zijn mandaat en middels de herverdeling van de middelen waarin het meerjarig financieel kader 2014-2020 voor dit agentschap voorziet, i.e. zonder dat daarvoor aanvullende begrotingsmiddelen of personele middelen worden toegewezen.

3.2.3.2. Geraamde personeelsbehoeften

– ☐ Voor het voorstel/initiatief zijn geen personele middelen nodig

– ☑ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven:

In beginsel zou geen extra personeel nodig zijn. De behoefte aan personele middelen zal zeer beperkt blijven en worden gedekt door personeelsleden van het DG die het beheer van de actie al tot taak hebben gekregen.

Raming in een geheel getal (of met hoogstens 1 decimaal)

	Jaar **2015**	Jaar **2016**	Jaar **2017**	Jaar **2018**	Daaropvolgende jaren (2019-2021) en later		
• Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)							
09 01 01 01 (zetel en vertegenwoordigingen van de Commissie)	4	4	4	4	4	4	4
XX 01 01 02 (delegaties)							
XX 01 05 01 (onderzoek door derden)							
10 01 05 01 (eigen onderzoek)							
• Extern personeel (in voltijdequivalenten: VTE's)[51]							
09 01 02 01 (CA, END, INT van de "totale financiële middelen")	1	1	1	1	1	1	1
XX 01 02 02 (CA, INT, JED, LA en SNE in de delegaties)							
XX 01 04 ***jj***[52] - zetel[53]							
XX 01 04 ***jj***[52] - delegaties							
XX 01 05 02 (CA, INT, SNE – onderzoek door derden)							
10 01 05 02 (CA, INT, SNE – eigen onderzoek)							
Ander begrotingsonderdeel (te vermelden)							
TOTAAL	**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX is het beleidsterrein of de begrotingstitel.

De benodigde personele middelen zullen worden gefinancierd uit de middelen die reeds voor het beheer van deze actie zijn toegewezen en/of binnen DG CNECT zijn herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen..

51 CA = Agent Contractuel (arbeidscontractant); INT = Intérimaire (uitzendkracht); JED = Jeune Expert en Délégation (jonge deskundige in delegaties); LA = Local Agent (plaatselijk functionaris); SNE = Seconded National Expert (gedetacheerd nationaal deskundige).

52 Submaximum voor extern personeel uit beleidskredieten (vroegere "BA"-onderdelen).

53 Vooral voor structuurfondsen, Europees Landbouwfonds voor Plattelandsontwikkeling (ELFPO) en Europees Visserijfonds (EVF).

ENISA, het Europees Agentschap voor netwerk- en informatiebeveiliging, kan de lidstaten en de Commissie bijstaan bij de tenuitvoerlegging van de richtlijn, en wel op basis van zijn mandaat en middels de herverdeling van de middelen waarin het meerjarig financieel kader 2014-2020 voor dit agentschap voorziet, i.e. zonder dat daarvoor aanvullende begrotingsmiddelen of personele middelen worden toegewezen.

Beschrijving van de uit te voeren taken

Ambtenaren en tijdelijk personeel	- Voorbereiding van gedelegeerde handelingen overeenkomstig artikel 14, lid 3 - Voorbereiding van uitvoeringshandelingen overeenkomstig artikel 8, artikel 9, lid 2, artikel 12, artikel 14, lid 5, en artikel 16 - Bijdrage tot de samenwerking via het netwerk, zowel op beleids- als op operationeel niveau - Deelname aan internationale besprekingen en eventueel sluiting van internationale overeenkomsten
Extern personeel	Waar nodig ondersteuning bij de hierboven genoemde taken

3.2.4. Verenigbaarheid met het huidig meerjarig financieel kader

– ☑ Het voorstel/initiatief is verenigbaar met het huidige meerjarig financieel kader

– ☐ Het voorstel/initiatief vergt herprogrammering van de betrokken rubriek van het meerjarig financieel kader.

Het voorstel zal de geraamde gevolgen voor de beleidsuitgaven hebben indien de lidstaten ervoor kiezen bestaande infrastructuur aan te passen en zij de Commissie opdragen deze aanpassing binnen het meerjarig financieel kader 2014-2020 ten uitvoer te leggen. De betrokken eenmalige kosten komen ten laste financieringsfaciliteit voor Europese verbindingen, mits deze over voldoende middelen beschikt. Bij wijze van alternatief kunnen de lidstaten de kosten die hetzij met het aanpassen van bestaande infrastructuur hetzij met het opzetten van nieuwe infrastructuur gepaard gaan, delen.

– ☐ Het voorstel/initiatief vergt toepassing van het flexibiliteitsinstrument of herziening van het meerjarig financieel kader[54].

Niet van toepassing.

3.2.5. Bijdrage van derden aan de financiering

– Het voorstel/initiatief voorziet niet in medefinanciering door derden

3.3. Geraamde gevolgen voor de ontvangsten

– ☑ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten.

[54] Zie de punten 19 en 24 van het Interinstitutioneel Akkoord.