EUROPESE COMMISSIE

Brussel, 30.9.2010
COM(2010) 521 definitief

2010/0275 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

Inzake het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA)

{SEC(2010) 1126}
{SEC(2010) 1127}

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

1.1. Beleidsachtergrond

Het Europees Agentschap voor netwerk- en informatiebeveiliging (het ENISA) is in maart 2004 bij Verordening (EG) nr. 460/2004[1] opgericht voor een eerste periode van 5 jaar, en heeft als hoofddoel *"te zorgen voor een hoog en doeltreffend niveau van netwerk- en informatiebeveiliging in de Gemeenschap en (…) een cultuur van netwerk- en informatiebeveiliging ten behoeve van de burgers, consumenten, bedrijven en publieke organen in de Europese Unie tot stand te brengen en op die manier bij te dragen tot de goede werking van de interne markt"*. Het mandaat van het ENISA is bij Verordening (EG) nr. 1007/2008[2] verlengd tot maart 2012.

De verlenging van het mandaat van het ENISA in 2008 heeft ook een debat op gang gebracht over de algemene richting van de Europese inspanningen op het gebied van netwerk- en informatiebeveiliging; de Commissie heeft een bijdrage geleverd tot dit debat door een openbare raadpleging op te starten over de mogelijke doelstellingen van een versterkt beleid voor netwerk- en informatiebeveiliging op het niveau van de Unie. Deze openbare raadpleging, die plaatsvond van november 2008 tot januari 2009, leverde bijna 600 reacties op[3].

Op 30 maart 2009 heeft de Commissie een mededeling betreffende de bescherming van kritieke informatie-infrastructuur vastgesteld[4], waarin met name aandacht wordt besteed aan de bescherming van Europa tegen cyberaanvallen en -verstoringen door de paraatheid, beveiliging en veerkracht te verbeteren; deze mededeling bevat ook een actieplan waarin het ENISA wordt opgeroepen om een rol te spelen, met name ter ondersteuning van de lidstaten. Tijdens de besprekingen in het kader van de ministeriële conferentie betreffende de bescherming van kritieke informatie-infrastructuur, die op 27 en 28 april 2009 plaatsvond in de Estse hoofdstad Tallinn, kon het actieplan op brede steun rekenen[5]. In de conclusies die het voorzitterschap van de Europese Unie uit deze conferentie heeft getrokken, wordt benadrukt dat het belangrijk is de operationele steun voor het ENISA op te drijven; volgens deze conclusies is het ENISA een waardevol instrument om de gezamenlijke inspanningen in de hele Unie op dit gebied te versterken en moet het mandaat van het Agentschap worden herbekeken en anders geformuleerd, zodat het beter is afgestemd op de prioriteiten en

---

1 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).

2 Verordening (EG) nr. 1007/2008 van het Europees Parlement en de Raad van 24 september 2008 tot wijziging van 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, ten aanzien van de looptijd van het Agentschap (PB L 293 van 31.10.2008, blz. 1).

3 Het samenvattend verslag van de resultaten van de openbare raadpleging 'Op weg naar een versterkt beleid inzake netwerk- en informatiebeveiliging in Europa' is als bijlage 11 bij de effectbeoordeling bij dit voorstel gevoegd.

4 COM(2009) 149 van 30.3.2009.

5 Discussienota: http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf
Conclusies van het voorzitterschap:
http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf.

behoeften van de EU, een flexibeler responscapaciteit kan worden opgebouwd, vaardigheden en bekwaamheden kunnen worden ontwikkeld en de operationele efficiëntie en algemene impact van het Agentschap kunnen worden versterkt, teneinde ervoor te zorgen dat het Agentschap een permanente aanwinst wordt voor alle lidstaten en voor de Europese Unie in haar geheel.

Na de besprekingen in de Raad Telecommunicatie van 11 juni 2009, waar de lidstaten, gezien het belang van netwerk- en informatiebeveiliging, hun steun hebben uitgesproken voor een uitbreiding van het mandaat en een verhoging van de middelen van het ENISA, werd het debat afgesloten onder het Zweedse voorzitterschap van de Unie. In de resolutie van de Raad van 18 december 2009 over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging[6] worden de rol en het potentieel van het ENISA erkend, alsook de behoefte om het ENISA *'verder te ontwikkelen tot een doeltreffend orgaan'*. Volgens deze resolutie moet ook aandacht worden geschonken aan het moderniseren en versterken van het ENISA, zodat het de Commissie en de lidstaten kan helpen bij het overbruggen van de kloof tussen technologie en beleid en het centrum van deskundigheid kan worden in EU-aangelegenheden op het gebied van netwerk- en informatiebeveiliging.

1.2. Algemene context

Informatie- en communicatietechnologieën (ICT) vormen de ruggengraat van de Europese economie en samenleving. ICT zijn kwetsbaar voor bedreigingen die niet stoppen aan nationale grenzen en die veranderd zijn ten gevolge van technologische en marktontwikkelingen. Aangezien ICT een mondiale dimensie hebben en nauw met elkaar en met andere infrastructuren zijn verweven, kan de beveiliging en veerkracht ervan niet worden gewaarborgd door een louter nationale en niet-gecoördineerde aanpak. Tegelijk evolueren de uitdagingen met betrekking tot netwerk- en informatiebeveiliging zeer snel. Netwerk- en informatiesystemen moeten effectief worden beveiligd tegen alle soorten verstoringen en defecten, inclusief aanvallen door mensen.

Beleidsmaatregelen op het gebied van netwerk- en informatiebeveiliging spelen een centrale rol in de Digitale Agenda voor Europa[7] (DAE), een vlaggenschipinitiatief van de EU 2020-strategie, om het potentieel van ICT te exploiteren en te bevorderen en om dit potentieel te vertalen in duurzame groei en innovatie. De benutting van ICT stimuleren en het vertrouwen in de informatiemaatschappij bevorderen, zijn sleutelprioriteiten van de DAE.

Het ENISA is oorspronkelijk opgericht om een hoog en effectief niveau van netwerk- en informatiebeveiliging in de Unie te garanderen. Uit de ervaring die is opgedaan met het Agentschap en de uitdagingen en bedreigingen blijkt dat het mandaat van het Agentschap moet worden gemoderniseerd, zodat het beter aansluit bij de behoeften van de Europese Unie; daarbij moet aandacht worden besteed aan de volgende punten:

- de uiteenlopende nationale benaderingen om het hoofd te bieden aan de veranderende uitdagingen;

- het gebrek aan coöperatieve modellen bij de tenuitvoerlegging van beleid op het gebied van netwerk- en informatiebeveiliging;

---

[6] Resolutie van de Raad van 18 december 2009 over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging (PB C 321 van 29.12.2009, blz. 1), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:NL:PDF.

[7] COM(2010) 245 van 19.5.2010.

- onvoldoende paraatheid, ook ten gevolge van de beperkte Europese capaciteit voor vroegtijdige waarschuwing en respons;

- gebrek aan betrouwbare Europese gegevens en beperkte kennis over veranderende problemen;

- laag bewustzijn van risico's en uitdagingen met betrekking tot netwerk- en informatiebeveiliging;

- de uitdaging om aspecten van netwerk- en informatiebeveiliging efficiënter te integreren in beleidsmaatregelen ter bestrijding van cybercriminaliteit.

1.3. Beleidsdoelstellingen

Het algemene doel van de voorgestelde verordening is ervoor te zorgen dat de Unie, de lidstaten en belanghebbenden de nodige bekwaamheid en paraatheid ontwikkelen om problemen op het gebied van netwerk- en informatiebeveiliging te voorkomen, op te sporen en aan te pakken. Dit helpt om vertrouwen op te bouwen, hetgeen de basis vormt voor de ontwikkeling van de informatiemaatschappij, om de concurrentiekracht van het Europese bedrijfsleven te verbeteren en om het effectief functioneren van de interne markt te garanderen.

1.4. Bestaande bepalingen op het door het voorstel bestreken gebied

Dit voorstel is een aanvulling op de regelgevende en niet-regelgevende beleidsinitiatieven inzake netwerk- en informatiebeveiliging die op het niveau van de Unie zijn genomen om de beveiliging en veerkracht van ICT te verbeteren:

- Het actieplan dat is opgestart door de Mededeling over de bescherming van kritieke communicatie- en informatie-infrastructuur voorziet in de oprichting van:

    (1) een Europees forum voor de lidstaten, dat tot doel heeft overleg en uitwisseling van goede beleidspraktijken te bevorderen, teneinde beleidsdoelstellingen en prioriteiten inzake beveiliging en veerkracht van ICT-infrastructuur te delen; dit forum heeft ook rechtstreeks baat bij de werkzaamheden en de ondersteuning van het Agentschap;

    (2) een Europees publiek-privaat partnerschap voor veerkracht (EP3R), een flexibel Europawijd governancekader voor de veerkracht van ICT-infrastructuur, dat de samenwerking tussen de publieke en de private sector stimuleert op het gebied van beveiligings- en veerkrachtsdoelstellingen, basisvereisten en goede beleidspraktijken en -maatregelen.

- Het Stockholmprogramma, dat op 11 december 2009 door de Europese Raad is vastgesteld, bevordert beleidsmaatregelen die netwerkbeveiliging beogen en die snellere reactie op cyberaanvallen in de Unie mogelijk maken.

- Deze initiatieven dragen ertoe bij dat de Digitale Agenda voor Europa zijn effect bereikt. Beleidsmaatregelen op het gebied van netwerk- en informatiebeveiliging spelen een centrale rol in het deel van de strategie dat het versterken van het vertrouwen in de beveiliging van de informatiemaatschappij beoogt. Ze ondersteunen ook de steunmaatregelen en het beleid van de Commissie inzake de bescherming van de privacy

(met name 'privacy by design') en persoonsgegevens (herziening van het kader), het CPC-netwerk, identiteitsbeheer en het actieplan voor een veiliger internet.

1.5. Ontwikkelingen in het huidige beleid inzake netwerk- en informatiebeveiliging, met betrekking tot het voorstel

Diverse actuele ontwikkelingen in het beleid inzake netwerk- en informatiebeveiliging, met name die welke zijn aangekondigd in de Digitale Agenda voor Europa, hebben baat bij de ondersteuning en deskundigheid van het ENISA. Enkele hiervan zijn:

- Versterking van de samenwerking op het gebied van het beleid inzake netwerk- en informatiebeveiliging door de activiteiten in het **Europees Forum voor de lidstaten** te intensiveren; met de steun van het ENISA zal dit helpen om:

  – manieren te vinden om een effectief Europees netwerk tot stand te brengen via grensoverschrijdende samenwerking tussen nationale/gouvernementele computercalamiteitenteams (CERT's);

  – langetermijndoelstellingen en prioriteiten voor grootschalige pan-Europese oefeningen met betrekking tot incidenten op het gebied van netwerk- en informatiebeveiliging te identificeren;

  – de minimumeisen voor overheidsaanbestedingen op te trekken om de beveiliging en veerkracht van publieke systemen en netwerken te bevorderen;

  – economische en regelgevende stimulansen voor beveiliging en veerkracht te identificeren;

  – de gezondheidstoestand van netwerk- en informatiebeveiliging in Europa te beoordelen.

- Versterking van de samenwerking en partnerschappen tussen de publieke en private sector door het **Europees publiek-privaat partnerschap voor veerkracht (EP3R)** te ondersteunen. Het ENISA speelt een steeds belangrijker rol bij het faciliteren van EP3R-vergaderingen en –activiteiten. De volgende stappen met betrekking tot EP3R zijn:

  – De bespreking van innoverende maatregelen en instrumenten om de beveiliging en veerkracht te verbeteren, zoals:

  (1) basisvereisten inzake beveiliging en veerkracht, met name op het gebied van overheidsaanbestedingen voor ICT-producten of –diensten, teneinde een gelijk speelveld te creëren en tegelijk een passend niveau van paraatheid en preventie te garanderen;

  (2) problemen met betrekking tot de aansprakelijkheid van marktdeelnemers onderzoeken, bijvoorbeeld als deze minimumbeveiligingseisen vaststellen;

  (3) economische stimulansen voor de ontwikkeling en opname van risicobeheerpraktijken, beveiligingsprocessen en producten;

  (4) regelingen voor risicobeoordeling en –beheer, teneinde belangrijke incidenten te beoordelen en te beheren op basis van onderling begrip;

(5) samenwerking tussen de private en de publieke sector bij grootschalige incidenten;

(6) de organisatie van een **topontmoeting tussen bedrijven** met betrekking tot economische hinderpalen en stimulansen voor beveiliging en veerkracht.

- De beveiligingseisen van het regelgevingspakket inzake elektronische communicatie in de praktijk brengen; hiervoor is de deskundigheid en bijstand van het ENISA vereist, teneinde:

  – de lidstaten en de Commissie te steunen, rekening houdende met de standpunten van de private sector, bij het vaststellen van een kader van regels en procedures voor de tenuitvoerlegging van de bepalingen inzake aanmelding van inbreuken op de beveiliging (vastgesteld in artikel 13, onder a), van de herziene kaderrichtlijn);

  – een jaarlijks forum voor nationale organen die bevoegd zijn voor netwerk- en informatiebeveiliging/nationale regelgevende autoriteiten en belanghebbenden uit de private sector te organiseren, teneinde ervaringen en goede praktijken met betrekking tot de toepassing van regelgevende maatregelen op het gebied van netwerk- en informatiebeveiliging uit te wisselen.

- **EU-wijde beveiligingsoefeningen ter voorbereiding op cyberaanvallen** faciliteren, met de steun van de Commissie en de bijdrage van het ENISA, teneinde deze oefeningen in een latere fase op internationale schaal uit te breiden.

- **Computercalamiteitenteams (CERT) oprichten voor de EU-instellingen**. In het kader van kernactie 6 van de Digitale Agenda voor Europa zal de Commissie 'maatregelen voorleggen voor een versterkt netwerk- en informatiebeveiligingsbeleid op hoog niveau, met inbegrip van […] maatregelen ter verhoging van de reactiesnelheid bij cyberaanvallen, inclusief een CERT voor de EU-instellingen'[8]. Hiertoe moeten de Commissie en de andere instellingen van de Unie een computercalamiteitenteam analyseren en oprichten, waarvoor het ENISA de technische ondersteuning en deskundigheid kan leveren.

- De lidstaten mobiliseren en ondersteunen bij het voltooien en, waar nodig, oprichten van **nationale/gouvernementele CERT's teneinde een goed functionerend netwerk van CERT's op te richten dat heel Europa bestrijkt**. Deze activiteit zal ook bijdragen tot de verdere ontwikkeling van een Europees informatie-uitwisselings- en waarschuwingssysteem (EISAS) voor burgers en het mkb; dit systeem moet tegen eind 2012 worden uitgebouwd met nationale middelen en capaciteiten.

- Het **bewustzijn** van uitdagingen met betrekking tot netwerk- en informatiebeveiliging **vergroten**:

  – de Commissie zal met het ENISA samenwerken om een eerste ontwerp van richtsnoeren voor de bevordering van normen, goede praktijken en een

[8] In de resolutie van de Raad van 18 december 2009 over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging is bepaald dat: *'De strategische effecten, risico's en vooruitzichten voor het instellen van CERT's voor de EU-instellingen moeten worden verkend en er moet worden nagedacht over de mogelijke toekomstige rol van het ENISA op dit gebied'.*

risicobeheerscultuur op het gebied van netwerk- en informatiebeveiliging op te stellen.

– het ENISA zal, samen met de lidstaten, de '**Europese maand van de netwerk- en informatiebeveiliging voor iedereen**' organiseren, met onder meer een nationale/Europese cyberbeveiligingswedstrijd.

1.6. Samenhang met andere beleidsmaatregelen en doelstellingen van de Unie

Het voorstel spoort met de bestaande beleidsmaatregelen en doelstellingen van de Europese Unie en ligt volledig in de lijn van de doelstelling om bij te dragen tot de vlotte werking van de interne markt via het verbeteren van de paraatheid en respons op de uitdagingen op het gebied van netwerk- en informatiebeveiliging.

2. RESULTAAT VAN DE RAADPLEGINGEN EN DE EFFECTBEOORDELING

2.1. Raadpleging van belanghebbende partijen

Dit beleidsinitiatief is het resultaat van een brede discussie op basis van een inclusieve benadering, waarbij de beginselen van participatie, openheid, toerekenbaarheid, effectiviteit en coherentie in acht zijn genomen. Het brede proces dat heeft plaatsgevonden, omvatte een evaluatie van het Agentschap in 2006/2007, gevolgd door aanbevelingen van de raad van bestuur van het ENISA, twee openbare raadplegingen (in 2007 en 2008-2009) en een aantal workshops over kwesties die verband houden met netwerk- en informatiebeveiliging.

De eerste openbare raadpleging vond plaats naar aanleiding van de tussentijdse evaluatie van het ENISA door de Commissie. Ze liep van 13 juni tot en met 7 september 2007 en had in de eerste plaats betrekking op de toekomst van het Agentschap; in totaal werden 44 online-reacties en twee schriftelijke reacties ingediend. Deze reacties waren afkomstig van uiteenlopende belanghebbenden en belangstellenden, inclusief ministeries van lidstaten, regelgevingsorganen, bedrijven en consumentenverenigingen, universitaire instellingen en individuele burgers.

De reacties hadden vooral betrekking op een aantal interessante problemen met betrekking tot de ontwikkeling van het bedreigingsscenario, de behoefte om de verordening te verduidelijken en meer flexibiliteit in de verordening in te bouwen zodat het ENISA zich kan aanpassen aan de uitdagingen, het belang te zorgen voor een effectieve interactie met belanghebbenden en de kans op een beperkte verhoging van de middelen.

De tweede openbare raadpleging, die plaatsvond van 7 november 2008 tot en met 9 januari 2009, had als doel de prioritaire doelstellingen voor een versterkt beleid inzake netwerk- en informatiebeveiliging op Europees niveau te identificeren, alsook de middelen om die doelstellingen te verwezenlijken. De autoriteiten van de lidstaten, universitaire/onderzoeksinstellingen, brancheverenigingen, private bedrijven en andere belanghebbenden, zoals gegevensbeschermingsorganisaties en consultants, en privépersonen hebben bijna 600 reacties ingediend.

Een grote meerderheid van de respondenten[9] steunde de uitbreiding van het mandaat van het Agentschap en was voorstander van een uitbreiding van de rol die het Agentschap speelt in de activiteiten met betrekking tot netwerk- en informatiebeveiliging op Europees niveau, en van een verhoging van de middelen van het Agentschap. Als sleutelprioriteiten werden de behoefte aan een meer gecoördineerde benadering van cyberbedreigingen in Europa, transnationale samenwerking om te reageren op grootschalige cyberaanvallen, het opbouwen van vertrouwen en verbeterde informatie-uitwisseling tussen belanghebbenden vermeld.

In september 2009 ging een effectbeoordeling van het voorstel van start, gebaseerd op een voorbereidende studie van een externe contractant. Hierbij waren diverse belanghebbenden en deskundigen betrokken. Onder meer netwerk- en informatiebeveiligingsorganen van lidstaten, nationale regelgevende autoriteiten, telecomoperatoren, internet service providers en verenigingen van aanverwante branches, consumentenverenigingen, ICT-fabrikanten, computercalamiteitenteams (CERT's), academici en gebruikers uit de bedrijfswereld dienden een bijdrage in. Ter ondersteuning van de uitvoering van de effectbeoordeling is een interdepartementale stuurgroep opgezet met vertegenwoordigers van de betrokken directoraten-generaal van de Europese Commissie.

2.2. Effectbeoordeling

Det instandhouding van een agentschap werd als een passende oplossing beschouwd voor het verwezenlijken van de Europese beleidsdoelstellingen[10]. Na een voorafgaande screening zijn vijf beleidsopties geselecteerd voor verdere analyse:

- Optie 1 – Geen beleid;
- Optie 2 – Het huidige beleid ongewijzigd voortzetten, d.w.z. met een vergelijkbaar mandaat en hetzelfde niveau van middelen;
- Optie 3 – De taken van het ENISA uitbreiden, waarbij ordehandhavingsautoriteiten en privacybeschermingsautoriteiten als volwaardige belanghebbenden worden toegevoegd;
- Optie 4 – De bestrijding van cyberaanvallen en de respons op cyberincidenten toevoegen aan de taken van het Agentschap;
- Optie 5 – De ondersteuning van gerechtelijke en politieautoriteiten bij de bestrijding van cybercriminaliteit toevoegen aan de taken van het Agentschap.

Op basis van een vergelijkende kosten-batenanalyse werd besloten dat optie 3 de meest kosteneffectieve en efficiënte wijze was om de beleidsdoelstellingen te verwezenlijken.

Optie 3 voorziet in een uitbreiding van de rol van het ENISA met de volgende taken:

- de uitbouw en instandhouding van een verbindingsnetwerk tussen belanghebbenden en een kennisnetwerk, zodat het ENISA op de hoogte blijft van het reilen en zeilen op het gebied van netwerk- en informatiebeveiliging in Europa;

[9] Zie bijlage XI bij de effectbeoordeling.
[10] Zie bijlage IV bij de effectbeoordeling.

- dienst doen als ondersteuningscentrum voor netwerk- en informatiebeveiliging met het oog op de ontwikkeling en toepassing van het beleid (met name met betrekking tot e-privacy, e-sign, e-ID en aanbestedingsnormen voor netwerk- en informatiebeveiliging);
- het EU-beleid inzake de bescherming van kritieke informatie-infrastructuur en de veerkracht van die infrastructuur ondersteunen (oefeningen, EP3R, Europees informatie-uitwisselings- en waarschuwingssysteem enz.);
- het opzetten van een EU-kader voor het verzamelen van gegevens met betrekking tot netwerk- en informatiebeveiliging, inclusief het ontwikkelen van methoden en praktijken voor wettelijke rapportering en uitwisseling;
- het bestuderen van de economische aspecten van netwerk- en informatiebeveiliging;
- het stimuleren van samenwerking met derde landen en internationale organisaties om een gemeenschappelijke mondiale benadering van netwerk- en informatiebeveiliging te bevorderen en om ervoor te zorgen dat internationale activiteiten op hoog niveau in Europa hun effect niet missen;
- het uitvoeren van niet-operationele taken met betrekking tot aspecten van netwerk- en informatiebeveiliging die verband houden met ordehandhaving en gerechtelijke samenwerking op het gebied van cybercriminaliteit.

3. JURIDISCHE ELEMENTEN VAN HET VOORSTEL

3.1. Samenvatting van de voorgestelde maatregel(en)

Het doel van de voorgestelde verordening is het Europees Agentschap voor netwerk- en informatiebeveiliging (het ENISA) te versterken en te moderniseren, en een nieuw mandaat voor een periode van vijf jaar vast te stellen.

Het voorstel bevat enkele belangrijke wijzigingen in vergelijking met de oorspronkelijke verordening:

(1) **Grotere flexibiliteit, aanpasbaarheid en groter vermogen om te focussen**. De taken worden geactualiseerd en ruimer geherformuleerd, teneinde de werkingssfeer van de activiteiten van het Agentschap te verruimen; de taken zijn voldoende afgelijnd om de middelen te kunnen beschrijven waarmee de doelstellingen moeten worden bereikt. Hierdoor wordt de opdracht van het Agentschap scherper omlijnd, is het Agentschap beter in staat zijn doelstellingen te verwezenlijken, en worden de taken van het Agentschap ter ondersteuning van de tenuitvoerlegging van het beleid van de Unie versterkt.

(2) **Betere afstemming van het Agentschap op het beleid en de regelgevingsprocedures van de Unie**. De Europese instellingen en organen kunnen een beroep doen op het Agentschap voor bijstand en advies. Dit ligt in de lijn van de politieke en regelgevende ontwikkelingen: de Raad is begonnen met zich rechtstreeks tot het Agentschap te richten in resoluties, en het EP en de Raad hebben taken in verband met netwerk- en informatiebeveiliging aan het Agentschap toegewezen, als onderdeel van het regelgevingskader inzake elektronische communicatie.

(3) **Raakvlak met de strijd tegen cybercriminaliteit**. Bij het verwezenlijken van zijn doelstellingen houdt het Agentschap rekening met de strijd tegen cybercriminaliteit.

Ordehandhavings- en privacybeschermingsautoriteiten worden volwaardige belanghebbenden van het Agentschap, met name in de permanente groep van belanghebbenden.

(4) **Versterkte governancestructuur**. Het voorstel versterkt de toezichthoudende rol van de raad van bestuur van het Agentschap, waarin de lidstaten en de Commissie zijn vertegenwoordigd. De raad van bestuur kan bijvoorbeeld algemene richtsnoeren opstellen inzake personeelszaken, hetgeen voorheen tot de exclusieve bevoegdheid van de uitvoerend directeur behoorde. De raad van bestuur kan ook werkgroepen oprichten om hem bij te staan bij het uitvoeren van zijn taken, ook wat het toezicht op de toepassing van zijn beslissingen betreft.

(5) **Stroomlijning van procedures**. Procedures die nodeloos lastig bleken te zijn, worden vereenvoudigd. Voorbeelden: (a) vereenvoudigde procedure voor de interne regels van de raad van bestuur, (b) het advies over het werkprogramma van het ENISA wordt verstrekt door de diensten van de Commissie in plaats van via een besluit van de Commissie. De raad van bestuur krijgt ook voldoende middelen voor het geval hij uitvoerende besluiten moet nemen en toepassen (bijv. als een personeelslid een klacht indient tegen de uitvoerend directeur of de raad van bestuur zelf).

(6) **Geleidelijke verhoging van de middelen**. Om te beantwoorden aan de versterkte Europese prioriteiten en de steeds groter wordende uitdagingen moeten de financiële middelen en het personeelsbestand van het Agentschap tussen 2012 en 2016 geleidelijk worden verhoogd, onverminderd het voorstel van de Commissie voor het volgende meerjarig financieel kader. Op basis van het voorstel van de Commissie voor de verordening waarbij het meerjarig financieel kader voor de periode na 2013 wordt vastgesteld, en rekening houdende met de conclusies van de effectbeoordeling, zal de Commissie een gewijzigd financieel memorandum presenteren.

(7) **De optie om de ambtstermijn van de uitvoerend directeur te verlengen**. De raad van bestuur kan de ambtstermijn van de uitvoerend directeur met drie jaar verlengen.

3.2. Rechtsgrondslag

Dit voorstel is gebaseerd op artikel 114 van het Verdrag betreffende de werking van de Europese Unie[11] (VWEU).

Volgens een arrest van het Europees Hof van Justitie[12] moest vóór de inwerkingtreding van het Verdrag van Lissabon **artikel 95 van het EG-Verdrag** als passende rechtsgrondslag worden beschouwd voor de oprichting van een orgaan dat als doel heeft een hoog en effectief niveau van netwerk- en informatiebeveiliging in de Unie te garanderen. De auteurs van het Verdrag hebben in artikel 95 de uitdrukking 'maatregelen inzake de onderlinge aanpassing' gebruikt om de wetgevende macht van de Unie de mogelijkheid te bieden passende maatregelen te kiezen om het gewenste resultaat te bereiken. Het verbeteren van de beveiliging en veerkracht van ICT-infrastructuur is dus een belangrijk element dat bijdraagt tot de vlotte werking van de interne markt.

---

[11] PB C 115 van 9.5.2008, blz. 94.

[12] EHvJ, 2.5.2006, C-217/04, *Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland tegen Europees Parlement en Raad van de Europese Unie.*

Onder het Verdrag van Lissabon wordt in **artikel 114 van het VWEU**[13] - in bijna identieke bewoordingen - de bevoegdheid voor de interne markt beschreven. Om de hierboven uiteengezette redenen blijft dit de toepasselijke rechtsgrondslag voor het vaststellen van maatregelen ter verbetering van de netwerk- en informatiebeveiliging. De bevoegdheid voor de interne markt is nu een gedeelde bevoegdheid van de Unie en de lidstaten (artikel 4, lid 2, onder a), van het VWEU). Dit betekent dat de Unie en de lidstaten (bindende) maatregelen kunnen vaststellen en dat de lidstaten optreden als de Unie haar bevoegdheid niet uitoefent of heeft besloten haar bevoegdheid niet meer uit te oefenen (artikel 2, lid 2, van het VWEU).

Maatregelen die onder de bevoegdheid voor de interne markt vallen, worden vastgesteld volgens de gewone wetgevingsprocedure (artikelen 289 en 294 van het VWEU), die vergelijkbaar[14] is met de vroegere medebeslissingsprocedure (artikel 251 van het EG-Verdrag).

Met het Verdrag van Lissabon is ook het vroegere onderscheid tussen de pijlers verdwenen. Het voorkomen en bestrijden van misdaad is een gedeelde bevoegdheid van de Unie geworden. Dit heeft het ENISA de kans gegeven om een rol te spelen als platform voor aspecten van de bestrijding van cybercriminaliteit die verband houden met netwerk- en informatiebeveiliging en om standpunten en goede praktijken met betrekking tot cyberbeveiligings-, ordehandhavings- en privacybeschermingsautoriteiten uit te wisselen.

3.3. Subsidiariteitsbeginsel

Het voorstel is in overeenstemming met het subsidiariteitsbeginsel: het beleid inzake netwerk- en informatiebeveiliging vereist een coöperatieve aanpak en de doelstellingen van het voorstel kunnen niet door individuele lidstaten worden verwezenlijkt.

Een strategie waarbij de Unie niet tussenbeide komt in het nationale beleid inzake netwerk- en informatiebeveiliging zou tot gevolg hebben dat deze taak wordt overgelaten aan de lidstaten en dat geen rekening wordt gehouden met de onderlinge verwevenheid van de bestaande informatiesystemen. Een maatregel die zorgt voor een passende mate van coördinatie tussen de lidstaten om te garanderen dat risico's op het gebied van netwerk- en informatiebeveiliging goed kunnen worden beheerd in de grensoverschrijdende context waarin ze zich voordoen, is dan ook in overeenstemming met het subsidiariteitsbeginsel. Bovendien verbeteren Europese maatregelen de effectiviteit van bestaande nationale beleidsmaatregelen en zorgen ze dus voor toegevoegde waarde.

Bovendien zal een gezamenlijk en coöperatief beleid inzake netwerk- en informatiebeveiliging een positief effect hebben op de bescherming van de grondrechten, en met name het recht op de bescherming van persoonsgegevens en privacy. De behoefte aan gegevensbescherming is op dit ogenblik van cruciaal belang aangezien Europese burgers steeds vaker hun gegevens toevertrouwen aan complexe informatiesystemen, ofwel uit vrije wil ofwel omdat ze daartoe genoodzaakt zijn, zonder daarom noodzakelijk de bijbehorende risico's inzake gegevensbescherming correct te kunnen inschatten. In het geval van incidenten zullen zij dus niet altijd passende maatregelen kunnen nemen; het is bovendien niet zeker dat de lidstaten internationale incidenten effectief kunnen oplossen zonder Europese coördinatie op het gebied van netwerk- en informatiebeveiliging.

---

13 Cf. supra.

14 Het verschil zit hem met name in het feit dat de gewone wetgevingsprocedure andere meerderheden vereist in de Raad en het EP.

3.4. Evenredigheidsbeginsel

Dit voorstel beantwoordt aan het evenredigheidsbeginsel aangezien het niet verder gaat dan nodig is om de doelstellingen ervan te verwezenlijken.

3.5. Keuze van instrumenten

Voorgesteld instrument: een verordening, die rechtstreeks toepasselijk is in alle lidstaten.

4. GEVOLGEN VOOR DE BEGROTING

Het voorstel heeft gevolgen voor de begroting van de Unie.

Aangezien wordt vastgesteld dat extra taken aan het nieuwe mandaat van het ENISA moeten worden toegevoegd, wordt verwacht dat het Agentschap de middelen krijgt om deze taken uit te voeren. Uit de evaluatie van het Agentschap, het uitgebreide raadplegingsproces met belanghebbenden op alle niveaus en de effectbeoordeling blijkt dat er algemene eensgezindheid bestaat over het feit dat de grootte van het Agentschap niet beantwoordt aan zijn kritische massa en dat een verhoging van de middelen noodzakelijk is. De gevolgen en effecten van een verhoging van het personeelsbestand en de begroting van het Agentschap worden geanalyseerd in de effectbeoordeling bij het voorstel.

De EU-financiering na 2013 zal worden onderzocht in de context van een bespreking van alle voorstellen voor de periode na 2013 in de hele Commissie.

5. AANVULLENDE OPMERKINGEN

5.1. Duur

De verordening heeft betrekking op een periode van vijf jaar.

5.2. Evaluatieclausule

De verordening voorziet in een evaluatie van het Agentschap, die betrekking heeft op de periode sinds de vorige evaluatie in 2007. In de evaluatie wordt beoordeeld hoe effectief het Agentschap tewerk gaat bij het verwezenlijken van de in de verordening uiteengezette doelstellingen, of het nog steeds een effectief instrument is en of de looptijd van het Agentschap moet worden verlengd. Op basis van de bevindingen dient de raad van bestuur bij de Commissie aanbevelingen in met het oog op wijzigingen in deze verordening, het Agentschap en zijn werkmethoden. Om de Commissie in staat te stellen tijdig een voorstel voor een verlenging van het mandaat op te stellen, moet de evaluatie zijn afgerond tegen het einde van het tweede jaar van het in de verordening vastgelegde mandaat.

5.3. Voorlopige maatregel

De Commissie is zich ervan bewust dat in het kader van de wetgevingsprocedure met betrekking tot het voorstel lange besprekingen kunnen plaatsvinden in het Europees Parlement en de Raad, met het risico op een juridisch vacuüm als het nieuwe mandaat van het Agentschap niet wordt goedgekeurd vóór het huidige mandaat verstrijkt. Daarom doet de Commissie, samen met dit voorstel, ook een voorstel voor een verordening tot verlenging van

het huidige mandaat van het Agentschap met 18 maanden, zodat er voldoende tijd is voor de nodige discussies en procedures.

2010/0275 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

Inzake het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA)

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,

Gezien het advies van het Europees Economisch en Sociaal Comité[15],

Gezien het advies van het Comité van de Regio's[16],

Na toezending van het voorstel aan de nationale parlementen,

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) Elektronische communicatie, infrastructuur en diensten zijn essentiële factoren in de economische en maatschappelijke ontwikkeling. Zij spelen een cruciale rol in de maatschappij en zijn uitgegroeid tot alomtegenwoordige voorzieningen, zoals elektriciteit en water. De verstoring van deze voorzieningen kan gevoelige economische schade veroorzaken; het is dan ook belangrijk maatregelen te nemen om de bescherming en veerkracht van deze voorzieningen te verbeteren, zodat de continuïteit van kritieke diensten gegarandeerd is. De uitdagingen voor de beveiliging van elektronische communicatie, infrastructuur en diensten, en met name de integriteit en beschikbaarheid ervan, worden steeds groter. Dit is van steeds groter belang voor de maatschappij, niet in het minst omdat problemen ten gevolge van de complexiteit van systemen, ongevallen, fouten en aanvallen gevolgen kunnen hebben voor de fysieke infrastructuur waarmee diensten worden verleend die van kritiek belang zijn voor het welzijn van de Europese burgers.

(2) De bedreigingen veranderen voortdurend en veiligheidsincidenten kunnen het vertrouwen van de gebruikers schaden. Ernstige verstoringen van de elektronische communicatie, infrastructuur en diensten kunnen grote economische en sociale gevolgen hebben, maar ook dagelijkse veiligheidsinbreuken, problemen en storingen kunnen het vertrouwen van het publiek in technologie, netwerken en diensten ondermijnen.

---

15 PB C , , blz. .

16 PB C , , blz. .

(3) Een regelmatige beoordeling van de staat van netwerk- en informatiebeveiliging in Europa, op basis van betrouwbare Europese gegevens, is dan ook belangrijk voor de beleidmakers, het bedrijfsleven en de gebruikers.

(4) De vertegenwoordigers van de lidstaten, in de Europese Raad bijeen op 13 december 2003, hebben besloten dat het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), dat moet worden opgericht op basis van het door de Commissie ingediende voorstel, wordt gevestigd in een door de Griekse regering aan te wijzen stad in Griekenland.

(5) In 2004 hebben het Europees Parlement en de Raad Verordening (EG) nr. 460/2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging[17] vastgesteld teneinde bij te dragen tot een hoog niveau van netwerk- en informatiebeveiliging in de Unie en tot de ontwikkeling van een cultuur van netwerk- en informatiebeveiliging ten bate van burgers, consumenten, ondernemingen en overheidsadministraties. In 2008 hebben het Europees Parlement en de Raad Verordening (EG) nr. 1007/2008[18] vastgesteld, waarbij het mandaat van het Agentschap wordt verlengd tot maart 2012.

(6) Sinds de oprichting van het Agentschap zijn de uitdagingen voor netwerk- en informatiebeveiliging veranderd ten gevolge van technologische, commerciële en sociaaleconomische ontwikkelingen, en zijn ze het voorwerp geweest van verdere beschouwing en debat. In reactie op de veranderende uitdagingen heeft de Unie haar prioriteiten voor het netwerk- en informatiebeveiligingsbeleid bijgewerkt in een aantal documenten, waaronder de mededeling van de Commissie uit 2006 *Een strategie voor een veilige informatiemaatschappij – Dialoog, partnerschap en empowerment*[19], de resolutie van de Raad uit 2007 inzake een strategie voor een veilige informatiemaatschappij[20], de mededeling uit 2009 *Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht*[21], de conclusies van het voorzitterschap van de ministeriële conferentie over de bescherming van kritieke informatie-infrastructuur, de resolutie van de Raad uit 2009 over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging en de Digitale Agenda voor Europa[22]. De behoefte is erkend om het Agentschap te moderniseren en te versterken, teneinde met succes bij te dragen tot de inspanningen van de Europese instellingen en de lidstaten om een Europese capaciteit op te bouwen waarmee het hoofd kan worden geboden aan uitdagingen met betrekking tot netwerk- en informatiebeveiliging. Recentelijk heeft de Commissie de Digitale Agenda voor Europa[23] vastgesteld, een vlaggenschipinitiatief van de Europa 2020-strategie. Deze uitgebreide agenda heeft tot doel het potentieel van ICT te benutten en te bevorderen teneinde dit potentieel te vertalen in duurzame groei en innovatie. Het vertrouwen in de informatiemaatschappij stimuleren, is een van

---

17 PB L 77 van 13.3.2004 blz. 1.

18 PB L 293 van 31.10.2008, blz. 1.

19 COM(2006) 251 van 31.5.2006.

20 Resolutie van de Raad van 22 maart 2007 inzake een strategie voor een veilige informatiemaatschappij (PB C 68 van 24.3.2007, blz. 1).

21 COM(2009) 149 van 30.3.2009.

22 Resolutie van de Raad van 18 december 2009 over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging (PB C 321 van 29.12.2009, blz. 1).

23 COM(2010) 245 van 19.5.2010.

de hoofddoelstellingen van deze uitgebreide agenda, waarin een aantal acties van de Commissie op dit gebied zijn aangekondigd, inclusief het onderhavige voorstel.

(7) Maatregelen op de interne markt op het gebied van de beveiliging van elektronische communicatie en, meer in het algemeen, netwerk- en informatiebeveiliging vereisen verschillende vormen van technische en organisatorische toepassingen door de lidstaten en de Commissie. De heterogene toepassing van deze eisen kan tot inefficiëntie leiden en belemmeringen creëren voor de interne markt. Daarom moet op Europees niveau een centrum van deskundigheid worden opgericht dat begeleiding en advies verstrekt en, indien gevraagd, bijstand met betrekking tot kwesties die verband houden met netwerk- en informatiebeveiliging; zowel de lidstaten als de Europese instellingen moeten een beroep kunnen doen op dit centrum. Het Agentschap kan op deze behoeften inspelen door een hoog niveau van deskundigheid te ontwikkelen en in stand te houden en door de lidstaten, de Commissie en het bedrijfsleven te helpen voldoen aan de juridische en regelgevende eisen met betrekking tot netwerk- en informatiebeveiliging; hierdoor draagt het Agentschap ook bij tot de vlotte werking van de interne markt.

(8) Het Agentschap moet de taken uitvoeren die hem zijn toegewezen in de huidige EU-wetgeving op het gebied van elektronische communicatie en, in het algemeen, bijdragen tot een verbetering van het niveau van de beveiliging van elektronische communicatie door, onder meer, deskundigheid ter beschikking te stellen, advies te verstrekken en de uitwisseling van goede praktijken te bevorderen.

(9) Bij Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en –diensten[24] is voorts vereist dat aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten passende maatregelen nemen om hun integriteit en beveiliging in stand te houden, en zijn eisen vastgesteld voor de melding van inbreuken op de beveiliging en het verlies van integriteit. Desgevallend moet het Agentschap ook op de hoogte worden gebracht door de nationale regelgevende autoriteiten, die ook een samenvattend jaarverslag over de ontvangen meldingen en de ondernomen acties bij de Commissie en het Agentschap moeten indienen. In Richtlijn 2002/21/EG wordt het Agentschap ook opgeroepen om bij te dragen tot de harmonisering van passende technische en organisatorische beveiligingsmaatregelen door adviezen op te stellen.

(10) Volgens Richtl?n 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonl?ke levenssfeer in de sector elektronische communicatie (richtl?n betreffende privacy en elektronische communicatie)[25] moeten aanbieders van openbare elektronische communicatiediensten passende technische en organisatorische maatregelen nemen om de beveiliging van hun diensten te garanderen en moet het vertrouwelijke karakter van de communicatie en het bijbehorende gegevensverkeer worden gegarandeerd. Richtlijn 2002/58/EG bevat ook eisen waaraan aanbieders van elektronische communicatiediensten moeten voldoen met betrekking tot de informatieverstrekking en aanmelding van inbreuken op de bescherming van persoonsgegevens. Volgens deze richtlijn moet de Commissie het Agentschap ook

[24] PB L 108 van 24.4.2002 blz. 33.
[25] PB L 201 van 31.7.2002 blz. 37.

raadplegen over alle technische tenuitvoerleggingsmaatregelen die volgens de omstandigheden moeten worden vastgesteld of over het formaat en de procedures die van toepassing zijn op de eisen inzake informatieverstrekking en aanmelding. 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[26] verplicht de lidstaten ervoor te zorgen dat de controlerende instantie passende technische en organisatorische maatregelen treft om persoonsgegevens te beveiligen tegen vernietiging, hetzij accidenteel, hetzij onrechtmatig, tegen accidenteel verlies, vervalsing, ongeautoriseerde verspreiding of toegang, met name als de verwerking betrekking heeft op de verzending van gegevens over een netwerk, en tegen enige andere vorm van onwettige verwerking.

(11) Het Agentschap moet bijdragen tot een hoog niveau van netwerk- en informatiebeveiliging in de Unie en tot de ontwikkeling van een cultuur van netwerk- en informatiebeveiliging ten behoeve van de burgers, consumenten, bedrijven en organisaties uit de publieke sector in de Europese Unie, en aldus bijdragen tot de goede werking van de interne markt.

(12) In een reeks taken moet worden aangegeven hoe het Agentschap zijn doelstellingen moet verwezenlijken en toch de nodige flexibiliteit in zijn werking behouden. De taken die het Agentschap moet uitvoeren, moeten onder meer betrekking hebben op het verzamelen van passende informatie en gegevens die nodig zijn om de risico's voor de beveiliging en veerkracht van de elektronische communicatie, infrastructuur en diensten te analyseren en om, samen met de lidstaten, de staat van de netwerk- en informatiebeveiliging in Europa te beoordelen. Het Agentschap moet zorgen voor coördinatie met de lidstaten en voor verbeterde samenwerking tussen belanghebbenden in Europa, met name door bevoegde nationale organen en deskundigen op het gebied van netwerk- en informatiebeveiliging uit de privésector te betrekken bij zijn activiteiten. Het Agentschap moet de Commissie en de lidstaten helpen met het bedrijfsleven te overleggen om beveiligingsproblemen in hardware- en softwareproducten op te lossen, en draagt aldus bij tot een coöperatieve benadering van netwerk- en informatiebeveiliging.

(13) Het Agentschap moet als referentiepunt fungeren en vertrouwen scheppen door zijn onafhankelijkheid, de kwaliteit van zijn advies en informatie, de transparantie van zijn procedures en werkmethoden, en de toewijding bij de uitvoering van zijn taken. Het Agentschap dient voort te bouwen op inspanningen in de lidstaten en de EU en derhalve zijn taken uit te voeren in volledige samenwerking met de lidstaten. Het dient open te staan voor contacten met het bedrijfsleven en andere belanghebbenden. Bovendien moet het Agentschap voortbouwen op de input van en de samenwerking met de privésector, die een belangrijke rol speelt in de beveiliging van elektronische communicatie, infrastructuur en diensten.

(14) De Commissie heeft een Europees publiek-privaat partnerschap voor veerkracht opgericht dat dienst doet als flexibel Europawijd governancekader voor de veerkracht van ICT-infrastructuur, waarin het Agentschap een faciliterende rol moet spelen door publieke en private belanghebbenden uit te sector samen te brengen om te overleggen

[26] PB L 281 van 23.11.1995 blz. 31.

over prioriteiten van het openbaar beleid en de economische en marktdimensie van uitdagingen en maatregelen voor de veerkracht van ICT-infrastructuur en om na te gaan welke verantwoordelijkheid de belanghebbenden dragen.

(15) Het Agentschap moet, op verzoek van de Commissie of op eigen initiatief, advies verstrekken aan de Commissie door middel van adviezen en technische en sociaaleconomische analyses, teneinde de Commissie te helpen bij het ontwikkelen van beleid op het gebied van netwerk- en informatiebeveiliging. Wanneer lidstaten of Europese instellingen en organen daarom verzoeken, moet het Agentschap hen ook bijstaan in hun inspanningen om beleid en bekwaamheid op het gebied van netwerk- en informatiebeveiliging te ontwikkelen.

(16) Het Agentschap moet ertoe bijdragen dat de lidstaten en de Europese instellingen grensoverschrijdende bekwaamheid en paraatheid ontwikkelen om problemen op het gebied van netwerk- en informatiebeveiliging te voorkomen, op te sporen en te beperken; om dit doel te verwezenlijken, moet het Agentschap de samenwerking tussen de lidstaten onderling en tussen de lidstaten en de Commissie bevorderen. daartoe moet het Agentschap de lidstaten actief ondersteunen in hun niet-aflatende inspanningen om hun responscapaciteit te verbeteren en nationale en Europese oefeningen op het gebied van beveiligingsincidenten te organiseren en uit te voeren.

(17) De verwerking van persoonsgegevens bij de toepassing van de onderhavige verordening is geregeld bij Richtlijn 95/46/EG.

(18) Om de uitdagingen op het gebied van netwerk- en informatiebeveiliging beter te begrijpen, moet het Agentschap actuele en ontluikende risico's analyseren. Daartoe moet het Agentschap, in samenwerking met lidstaten en, voor zover van toepassing, statistische organen, relevante informatie verzamelen. Bovendien moet het Agentschap de lidstaten en de Europese instellingen en organen bijstaan in hun inspanningen om gegevens met betrekking tot netwerk- en informatiebeveiliging te verzamelen, te analyseren en te verspreiden.

(19) Bij het uitvoeren van toezichtsactiviteiten in de Unie moet het Agentschap de samenwerking tussen de Unie en de lidstaten bij het beoordelen van de toestand van de netwerk- en informatiebeveiliging in Europa bevorderen en bijdragen tot beoordelingsactiviteiten in samenwerking met de lidstaten.

(20) Het Agentschap moet de samenwerking tussen de bevoegde overheidsorganen van de lidstaten bevorderen, met name door de opstelling en uitwisseling van goede praktijken en normen voor opleidingsprogramma's en bewustmakingsregelingen te ondersteunen. Meer informatie-uitwisseling tussen de lidstaten kan bijdragen tot dergelijke acties. Het Agentschap moet ook de samenwerking tussen publieke en private belanghebbenden op EU-niveau ondersteunen, onder meer door informatie-uitwisseling, bewustmakingscampagnes en opleidings- en trainingsprogramma's te bevorderen.

(21) Efficiënte beveiligingsvoorschriften zijn gebaseerd op goed ontwikkelde methoden voor risicoanalyse, zowel in de openbare als in de particuliere sector. Methoden en procedures voor risicoanalyse worden op verschillende niveaus ingezet zonder dat er een gemeenschappelijke praktijk bestaat voor de efficiënte toepassing ervan. Door goede praktijken voor risicoanalyse en voor interoperabele oplossingen voor

risicobeheersing binnen overheids- en particuliere organisaties te stimuleren en te ontwikkelen, kan het beveiligingsniveau van netwerken en informatiesystemen in Europa worden verbeterd. Daartoe moet het Agentschap de samenwerking tussen publieke en private belanghebbenden op EU-niveau bevorderen door hun inspanningen te ondersteunen met betrekking tot de ontwikkeling en oppak van normen voor risicobeheer en meetbare beveiliging van elektronische producten, systemen, netwerken en diensten.

(22) Het Agentschap dient bij zijn werkzaamheden gebruik te maken van de lopende activiteiten op het gebied van onderzoek, ontwikkeling en technologie-evaluatie, en met name van de verschillende onderzoeksinitiatieven van de Europese Unie.

(23) Voor zover dat nodig en nuttig is voor de uitvoering van zijn mandaat, doelstellingen en taken, moet het Agentschap ervaringen en algemene informatie uitwisselen met op grond van de EU-wetgeving ingestelde organen en agentschappen die zich met netwerk- en informatiebeveiliging bezighouden.

(24) In zijn contacten met ordehandhavingsorganen over beveiligingsaspecten van cybercriminaliteit respecteert het Agentschap bestaande informatiekanalen en gevestigde netwerken zoals de contactpunten die vermeld zijn in de voorgestelde richtlijn van het Europees Parlement en de Raad over aanvallen op informatiesystemen, waarbij Kaderbesluit 2005/222/JHA wordt ingetrokken, of de Europol-hoofden van de 'High Tech Crime Units Task Force'.

(25) Om te garanderen dat zijn doelstellingen volledig worden verwezenlijkt, moet het Agentschap contacten met ordehandhavingsorganen en privacybeschermingsautoriteiten onderhouden om de nadruk te leggen op en oplossingen te vinden voor de aspecten van cybercriminaliteit die betrekking hebben op netwerk- en informatiebeveiliging. Vertegenwoordigers van deze autoriteiten moeten volwaardige belanghebbenden van het Agentschap worden en moeten vertegenwoordigd zijn in de permanente groep van belanghebbenden van het Agentschap.

(26) Problemen op het gebied van netwerk- en informatiebeveiliging zijn wereldwijde problemen. Er is dan ook behoefte aan nauwere internationale samenwerking om de beveiligingsnormen en de informatie-uitwisseling te verbeteren en om een gemeenschappelijke wereldwijde aanpak van problemen op het gebied van netwerk- en informatiebeveiliging te stimuleren. Daartoe moet het Agentschap de samenwerking met derde landen en internationale organisaties ondersteunen, voor zover van toepassing samen met de Europese dienst voor extern optreden.

(27) De uitoefening van de taken van het Agentschap laat de bevoegdheden van de volgende instanties onverlet en mag hun bevoegdheden en taken niet uithollen, belemmeren of overlappen: de nationale regelgevende autoriteiten, zoals vermeld in de richtlijnen inzake elektronische communicatienetwerken en –diensten, de Europese Groep van regelgevende instanties voor elektronische communicatienetwerken en -diensten, opgericht bij Verordening 1211/2009[27] van het Europees Parlement en de Raad, het Comité voor communicatie, zoals vermeld in Richtlijn 2002/21/EG, de Europese normalisatie-instanties, de nationale normalisatie-instanties en het permanent

[27] PB L 337 van 18.12.2009, blz. 1.

comité, zoals vermeld in Richtlijn 98/34/EG van het Europees Parlement en de Raad van 22 juni 1998 betreffende een informatieprocedure op het gebied van normen en technische voorschriften en regels betreffende de diensten van de informatiemaatschappij[28] en de toezichthoudende autoriteiten van de lidstaten op het gebied van de bescherming van de persoonlijke levenssfeer in verband met de verwerking van persoonsgegevens en het vrije verkeer van dergelijke gegevens.

(28) Om de effectiviteit van het Agentschap te garanderen, moeten de lidstaten en de Commissie vertegenwoordigd zijn in de raad van bestuur, die de algemene richting van de werkzaamheden van het Agentschap vaststelt en garandeert dat het Agentschap zijn taken overeenkomstig deze verordening uitvoert. De raad van bestuur dient de noodzakelijke bevoegdheden te krijgen voor het vaststellen van de begroting, de controle op de uitvoering ervan, het vaststellen van passende financiële regels, het opstellen van transparante werkprocedures voor besluitvorming door het Agentschap, het goedkeuren van het werkprogramma van het Agentschap, het vaststellen van zijn eigen reglement van orde en van het huishoudelijk reglement van het Agentschap en de benoeming en de ambtsontheffing van de uitvoerend directeur. De raad van bestuur kan ook werkgroepen oprichten om hem bij te staan bij het uitvoeren van zijn taken, bijvoorbeeld bij het opstellen van besluiten op het toezicht op de tenuitvoerlegging ervan.

(29) Voor een goede werking van het Agentschap is het noodzakelijk dat de uitvoerend directeur wordt benoemd op grond van zowel verdiensten en aantoonbare administratieve en bestuurskundige vaardigheden, als van bekwaamheid en ervaring die relevant is voor netwerk- en informatiebeveiliging. Daarnaast dient hij zijn taken op volledig onafhankelijke wijze ten aanzien van de organisatie van de interne werking van het Agentschap uit te voeren. Daartoe moet de uitvoerend directeur een voorstel voor het werkprogramma van het Agentschap voorbereiden, na overleg met de diensten van de Commissie, en alle nodige stappen ondernemen om de goede uitvoering van het werkprogramma van het Agentschap te garanderen. Hij moet elk jaar een ontwerp van het algemeen verslag opstellen, dat moet worden voorgelegd aan de raad van bestuur, een ontwerpverklaring van de geraamde inkomsten en uitgaven van het Agentschap opstellen en de begroting ten uitvoer leggen.

(30) De uitvoerend directeur moet over de mogelijkheid beschikken om adhoc-werkgroepen op te richten voor specifieke kwesties, met name van wetenschappelijke, technische, juridische of sociaaleconomische aard. Bij het oprichten van dergelijke adhoc-werkgroepen moet de uitvoerend directeur input vragen van en gebruik maken van de relevante externe deskundigheid die nodig is om het Agentschap in staat te stellen toegang te krijgen tot de meest actuele informatie die beschikbaar is over beveiligingsuitdagingen ten gevolge van de ontwikkelende informatiemaatschappij. Het Agentschap moet erop toezien dat de leden van de adhoc-werkgroepen overeenkomstig de hoogste normen inzake deskundigheid worden geselecteerd, ermee rekening houdende dat, afhankelijk van de specifieke kwestie, een passend evenwicht moet worden bereikt tussen de overheidsinstanties van de lidstaten, de private sector, inclusief het bedrijfsleven, de gebruikers en universitaire deskundigen op het gebied van netwerk- en informatiebeveiliging. Indien nodig kan het Agentschap op adhoc-basis individuele deskundigen die erkenning genieten op het desbetreffende gebied

[28] PB L 204 van 21.7.1998 blz. 37.

uitnodigen om deel te nemen aan de werkzaamheden van de werkgroepen. Hun kosten dienen door het Agentschap te worden vergoed overeenkomstig zijn huishoudelijk reglement en overeenkomstig het vigerende Financieel Reglement.

(31) Het Agentschap moet beschikken over een permanente groep van belanghebbenden, die optreedt als adviserend orgaan, om te zorgen voor regelmatig overleg met de private sector, consumentenverenigingen en andere relevante belanghebbenden. Deze permanente groep van belanghebbenden, die wordt opgericht op voorstel van de uitvoerend directeur, dient zijn werkzaamheden toe te spitsen op aangelegenheden die voor alle belanghebbenden relevant zijn en deze onder de aandacht van het Agentschap te brengen. De uitvoerend directeur kan, indien nodig en overeenkomstig de vergaderagenda, vertegenwoordigers van het Europees Parlement en van andere instanties uitnodigen om deel te nemen aan de vergaderingen van de groep.

(32) Het Agentschap werkt volgens, respectievelijk, (i) het subsidiariteitsbeginsel, waardoor een passende graad van coördinatie tussen de lidstaten inzake kwesties die verband houden met netwerk- en informatiebeveiliging wordt gegarandeerd en de effectiviteit van het nationale beleid wordt verbeterd, hetgeen een toegevoegde waarde oplevert voor de lidstaten, en (ii) het evenredigheidsbeginsel, d.w.z. dat niet verder wordt gegaan dan wat noodzakelijk is om de doelstellingen van deze verordening te verwezenlijken.

(33) Het Agentschap moet de EU-wetgeving inzake publieke toegang tot documenten toepassen, zoals uiteengezet in Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad[29] en inzake de bescherming van natuurl?ke personen in verband met de verwerking van persoonsgegevens, zoals uiteengezet in Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurl?ke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vr?e verkeer van die gegevens[30].

(34) In het kader van zijn werkingssfeer en zijn doelstellingen en bij de vervulling van zijn taken dient het Agentschap in het bijzonder de bepalingen na te leven die van toepassing zijn op de Europese instellingen, alsmede de nationale wetgeving inzake de behandeling van gevoelige documenten. De raad van bestuur heeft de bevoegdheid een beslissing te nemen waarbij het Agentschap de toelating krijgt om gerubriceerde informatie te verwerken.

(35) Om de volledige autonomie en onafhankelijkheid van het Agentschap te waarborgen, wordt het noodzakelijk geacht aan het Agentschap een eigen begroting toe te kennen die hoofdzakelijk wordt gefinancierd uit een bijdrage van de Unie en bijdragen van derde landen die deelnemen aan de werkzaamheden van het Agentschap. De lidstaat van vestiging of om het even welke andere lidstaat mag een vrijwillige bijdrage

---

29 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 (PB L 145 van 31.5.2001, blz. 43).

30 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 bescherming van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1).

leveren tot de inkomsten van het Agentschap. De EU-begrotingsprocedure blijft echter van toepassing op eventuele subsidies die ten laste van de algemene begroting van de Europese Unie komen. Bovendien dient de controle van de rekeningen te worden uitgevoerd door de Rekenkamer.

(36) Het Agentschap is de opvolger van het ENISA, dat is opgericht bij Verordening (EG) nr. 460/2004. In het kader van het besluit van de vertegenwoordigers van de lidstaten, bijeen in de Europese raad van 13 december 2003, moet de lidstaat van vestiging de huidige praktische regelingen in stand houden en ontwikkelen teneinde de vlotte en efficiënte werking van het Agentschap te garanderen, met name wat betreft de samenwerking met en de bijstand aan de Commissie, de lidstaten en hun bevoegde organen, andere EU-instellingen en organen en publieke en private belanghebbenden in heel Europa.

(37) Het Agentschap dient voor een beperkte periode te worden opgericht. Bovendien moeten de werkmethoden en de effectiviteit van het Agentschap bij het verwezenlijken van zijn doelstellingen worden beoordeeld om te bepalen of de doelstellingen van het Agentschap nog steeds geldig zijn en, op basis daarvan, of de looptijd van de activiteiten van het Agentschap moet worden verlengd,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD :

HOOFDSTUK 1 WERKINGSSFEER, DOELSTELLINGEN EN TAKEN

Artikel 1

Onderwerp en toepassingsgebied

1. Bij deze verordening wordt een Europees Agentschap voor netwerk- en informatiebeveiliging opgericht (hierna "het Agentschap" genoemd), dat als doel heeft bij te dragen tot een hoog en doeltreffend niveau van netwerk- en informatiebeveiliging in de Unie, het bewustzijn van netwerk- en informatiebeveiliging te vergroten en een cultuur van netwerk- en informatiebeveiliging ten behoeve van de burgers, consumenten, bedrijven en publieke organen in de Unie tot stand te brengen en op die manier bij te dragen tot de goede werking van de interne markt.

2. De doelstellingen en taken van het Agentschap doen geen afbreuk aan de bevoegdheden van de lidstaten inzake netwerk- en informatiebeveiliging en laten in ieder geval de activiteiten op het gebied van openbare veiligheid, defensie, staatsveiligheid (inclusief de economische welvaart van de staat indien de vraagstukken verband houden met de staatsveiligheid) en activiteiten van de staat op het gebied van het strafrecht onverlet.

3. In deze verordening wordt onder *"netwerk- en informatiebeveiliging"* verstaan: het vermogen van een netwerk of informatiesysteem om met een gegeven niveau van betrouwbaarheid bestand te zijn tegen toevallige gebeurtenissen of onwettige of kwaadaardige acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen of verzonden gegevens en de daaraan gerelateerde diensten die via deze netwerken en systemen worden aangeboden of toegankelijk zijn, in gevaar brengen;

Artikel 2
Doelstellingen

1. Het Agentschap verleent bijstand aan de Commissie en de lidstaten om te voldoen aan de wet- en regelgevende eisen inzake netwerk- en informatiebeveiliging in de huidige en toekomstige wetgeving van de Unie, en draagt op die manier bij tot de goede werking van de interne markt.

2. Het Agentschap zorgt ervoor dat de Unie en de lidstaten over de nodige bekwaamheid en paraatheid beschikken om problemen en incidenten op het gebied van netwerk- en informatiebeveiliging te voorkomen, op te sporen en aan te pakken.

3. Het Agentschap zorgt voor de ontwikkeling en instandhouding van deskundigheid van hoog niveau en gebruikt deze deskundigheid om brede samenwerking tussen actoren uit de publieke en de private sector te stimuleren.

Artikel 3
Taken

1. Om het in artikel 1 uiteengezette doel te kunnen verwezenlijken, voert het Agentschap de volgende taken uit:

a) de Commissie, op verzoek of op eigen initiatief, bijstaan bij de ontwikkeling van beleid inzake netwerk- en informatiebeveiliging door de Commissie advies, standpunten, technische en sociaaleconomische analyses te verstrekken en voorbereidende werkzaamheden uit te voeren voor de ontwikkeling en actualisering van de EU-wetgeving op het gebied van netwerk- en informatiebeveiliging;

b) de samenwerking vergemakkelijken tussen de lidstaten onderling en tussen de lidstaten en de Commissie bij het leveren van inspanningen om incidenten op het gebied van netwerk- en informatiebeveiliging te voorkomen, op te sporen en aan te pakken;

c) de lidstaten en de Europese instellingen en organen bijstaan in hun inspanningen om gegevens met betrekking tot netwerk- en informatiebeveiliging te verzamelen, te analyseren en te verspreiden;

d) in samenwerking met de lidstaten en de Europese instellingen regelmatig de toestand van de netwerk- en informatiebeveiliging in Europa beoordelen;

e) samenwerking tussen bevoegde openbare organen in Europa ondersteunen, en met name hun inspanningen om goede praktijken en normen te ontwikkelen en uit te wisselen;

f) de Unie en de lidstaten bijstaan bij het aanmoedigen van het gebruik van risicobeheer en goede praktijken en normen voor elektronische producten, systemen en diensten;

g) samenwerking tussen publieke en private belanghebbenden op EU-niveau ondersteunen, onder meer door informatie-uitwisseling en bewustmaking te bevorderen, en hun inspanningen faciliteren om normen voor risicobeheer en voor de beveiliging van elektronische producten, netwerken en diensten te ontwikkelen en toe te passen;

h) overleg en uitwisseling van goede praktijken tussen publieke en private belanghebbenden op het gebied van netwerk- en informatiebeveiliging aanmoedigen, inclusief aspecten van de strijd tegen cybercriminaliteit; de Commissie bijstand verlenen op het gebied van beleidsontwikkelingen die verband houden met aspecten van netwerk- en informatiebeveiliging in de strijd tegen cybercriminaliteit;

i) de lidstaten en Europese instellingen en organen, op verzoek, bijstaan in hun inspanningen om detectie-, analyse- en responscapaciteit op het gebied van netwerk- en informatiebeveiliging te ontwikkelen;

j) de dialoog en samenwerking tussen de Unie en derde landen en internationale organisaties ondersteunen, voor zover van toepassing in samenwerking met de Europese dienst voor extern optreden, teneinde internationale samenwerking en een gemeenschappelijke mondiale aanpak van problemen op het gebied van netwerk- en informatiebeveiliging te bevorderen;

k) taken uitvoeren waarmee het Agentschap is belast krachtens wetgevingsbesluiten van de Unie.

HOOFDSTUK 2 ORGANISATIE

Artikel 4
Organen van het Agentschap

Het Agentschap bestaat uit:

a) een raad van bestuur,

b) een uitvoerend directeur en het personeel, en

c) een permanente groep van belanghebbenden.

Artikel 5
Raad van bestuur

1. De raad van bestuur bepaalt de algemene richting van de werkzaamheden van het Agentschap en ziet erop toe dat de werkzaamheden van het Agentschap in overeenstemming zijn met de in deze verordening vastgestelde regels en beginselen. De raad van bestuur zorgt ook voor samenhang tussen de werkzaamheden van het Agentschap en de activiteiten op het niveau van de lidstaten en de Unie.

2. De raad van bestuur stelt zijn reglement van orde vast, in overleg met de relevante diensten van de Commissie.

3. De raad van bestuur stelt het huishoudelijk reglement van het Agentschap vast, in overleg met de relevante diensten van de Commissie. Dit huishoudelijk reglement wordt openbaar gemaakt.

4. De raad van bestuur benoemt de uitvoerend directeur overeenkomstig artikel 10, lid 2, en kan hem uit zijn ambt ontheffen. De raad van bestuur treedt op als tuchtraad ten aanzien van de uitvoerend directeur.

5. De raad van bestuur stelt, overeenkomstig artikel 13, lid 3, het werkprogramma van het Agentschap vast, en, overeenkomstig artikel 14, lid 2, het algemeen verslag van de activiteiten van het Agentschap voor het voorgaande jaar.

6. De raad van bestuur stelt de financiële regels vast die van toepassing zijn op het Agentschap. Deze financiële regels mogen niet afwijken van Verordening (EG, Euratom) nr. 2343/2002 van de Commissie van 19 november 2002 houdende de financiële kaderregeling van de organen, bedoeld in artikel 185 van Verordening (EG, Euratom) nr. 1605/2002 van de Raad houdende het Financieel Reglement van toepassing op de algemene begroting van de Europese Gemeenschappen[31], tenzij de specifieke noden van het Agentschap zulks vereisen en de Commissie hierin vooraf heeft toegestemd.

7. De raad van bestuur stelt in overleg met de Commissie de nodige uitvoeringsmaatregelen vast volgens de regelingen van artikel 110 van het Statuut van de ambtenaren van de Europese Gemeenschappen.

8. De raad van bestuur kan werkorganen instellen, samengesteld uit leden van de raad van bestuur, om hem bij te staan bij de uitoefening van zijn functies, waaronder de voorbereiding van zijn besluiten en het toezicht op de uitvoering ervan.

9. De raad van bestuur kan het meerjarig personeelsbeleidsplan vaststellen, na overleg met de diensten van de Commissie en na de begrotingautoriteit in kennis te hebben gesteld.

Artikel 6

Samenstelling van de raad van bestuur

1. De raad van bestuur bestaat uit één vertegenwoordiger per lidstaat, drie door de Commissie benoemde vertegenwoordigers, alsmede drie door de Commissie benoemde vertegenwoordigers zonder stemrecht, die ieder één van de volgende groepen vertegenwoordigen:

a) de ict-industrie,

b) consumentenorganisaties,

c) universitaire deskundigen inzake netwerk- en informatiebeveiliging.

2. De leden van de raad van bestuur en hun plaatsvervangers worden benoemd op basis van hun relevante ervaring en deskundigheid op het gebied van netwerk- en informatiebeveiliging.

3. De ambtstermijn van de vertegenwoordigers van de in lid 1, onder a), b) en c), vermelde groepen bedraagt vier jaar. Deze ambtstermijn kan eenmaal worden verlengd. Als een vertegenwoordiger niet langer deel wenst uit te maken van een belangengroep, stelt de Commissie een plaatsvervanger aan.

[31] PB L 357 van 31.12.2002, blz. 72.

Artikel 7
Voorzitter van de raad van bestuur

De raad van bestuur kiest uit zijn midden een voorzitter en een vicevoorzitter voor een periode van drie jaar, die kan worden hernieuwd. De vicevoorzitter vervangt ambtshalve de voorzitter wanneer deze is verhinderd zijn taken te verrichten.

Artikel 8
Vergaderingen

1. De voorzitter roept de raad van bestuur in vergadering bijeen.

2. De raad van bestuur belegt tweemaal per jaar een gewone vergadering. Op verzoek van de voorzitter of van ten minste een derde van zijn stemgerechtigde leden belegt de raad van bestuur ook buitengewone vergaderingen.

3. De uitvoerend directeur neemt zonder stemrecht deel aan de vergaderingen van de raad van bestuur.

Artikel 9
Stemming

1. De besluiten van de raad van bestuur worden genomen met een meerderheid van alle stemgerechtigde leden.

2. Voor de vaststelling van het reglement van orde van het Agentschap, het huishoudelijk reglement, de begroting, het jaarlijkse werkprogramma, alsmede voor de benoeming, termijnverlenging en ambtsontheffing van de uitvoerend directeur is een tweederde meerderheid van alle stemgerechtigde leden van de raad van bestuur vereist.

Artikel 10
Uitvoerend directeur

1. Het Agentschap wordt geleid door de uitvoerend directeur, die onafhankelijk is in de uitvoering van zijn taken.

2. De uitvoerend directeur kan door de raad van bestuur uit zijn functie worden ontheven. De uitvoerend directeur wordt benoemd voor een ambtstermijn van vijf jaar op basis van een door de Commissie opgestelde kandidatenlijst, op grond van verdiensten en bewezen administratieve en bestuurlijke vaardigheden, alsmede specifieke bevoegdheid en ervaring. Vóór de benoeming kan de door de raad van bestuur gekozen kandidaat worden verzocht een verklaring voor de bevoegde commissie van het Europees Parlement af te leggen en vragen van de commissieleden te beantwoorden.

3. In de loop van de negen maanden voordat deze periode afloopt, verricht de Commissie een evaluatie. Daarbij kijkt de Commissie onder meer naar:

– de prestaties van de uitvoerend directeur;

– de taken en verplichtingen van het Agentschap in de volgende jaren.

4. De raad van bestuur kan op voorstel van de Commissie en rekening houdende met het evaluatieverslag de ambtstermijn van de uitvoerend directeur met ten hoogste drie jaar verlengen, maar alleen indien zulks op grond van de taken en verplichtingen van het Agentschap kan worden verantwoord.

5. De raad van bestuur stelt het Europees Parlement in kennis van zijn voornemen om de ambtstermijn van de directeur te verlengen. In de maand die voorafgaat aan de verlenging van zijn of haar ambtstermijn kan de uitvoerend directeur worden gevraagd een verklaring voor de bevoegde commissie van het Europees Parlement af te leggen en vragen van de commissieleden te beantwoorden.

6. Indien de ambtstermijn niet wordt verlengd, blijft de uitvoerend directeur in functie totdat er een opvolger is aangewezen.

7. De uitvoerend directeur is belast met:

a) het dagelijks beheer van het Agentschap;

b) de uitvoering van het werkprogramma en de besluiten van de raad van bestuur;

c) de taakuitoefening van het Agentschap conform de behoeften van de afnemers, met name wat betreft de doeltreffendheid van de verleende diensten;

d) alle specifieke personeelskwesties, waarbij erop moet worden toegezien dat de algemene richtsnoeren en beslissingen van de raad van bestuur in acht worden genomen;

e) de totstandbrenging en instandhouding van contacten met de Europese instellingen en organen;

f) het leggen en onderhouden van contacten met het bedrijfsleven en consumentenorganisaties om een regelmatige dialoog met de belanghebbenden te waarborgen;

g) andere taken waarmee hij/zij krachtens deze verordening is belast.

8. Indien dit noodzakelijk is en binnen de doelstellingen en taken van het Agentschap valt, kan de uitvoerend directeur adhoc-werkgroepen oprichten, samengesteld uit deskundigen. De raad van bestuur wordt daarvan van tevoren in kennis gesteld. De procedures betreffende met name de samenstelling, de benoeming van de deskundigen door de uitvoerend directeur en de werkwijze van de adhoc-werkgroepen worden in het huishoudelijk reglement van het Agentschap vastgesteld.

9. Indien nodig stelt de uitvoerend directeur ondersteunend administratief personeel en andere middelen ter beschikking van de raad van bestuur.

Artikel 11

Permanente groep van belanghebbenden

1. De raad van bestuur richt, op voorstel van de uitvoerend directeur, een permanente groep van belanghebbenden op, samengesteld uit deskundigen die de relevante belanghebbenden

vertegenwoordigen, zoals de ict-industrie, consumentenorganisaties, universitaire deskundigen op het gebied van netwerk- en informatiebeveiliging en ordehandhavings- en privacybeschermingsautoriteiten.

2. De procedures betreffende met name het aantal, de samenstelling en de benoeming van de leden door de raad van bestuur, op voorstel van de uitvoerend directeur, en de werking van de groep worden in het huishoudelijk reglement van het Agentschap gespecificeerd en worden gepubliceerd.

3. De groep wordt voorgezeten door de uitvoerend directeur.

4. De ambtstermijn van de leden van de groep bedraagt tweeënhalf jaar. Leden van de raad van bestuur kunnen geen lid zijn van de groep. Personeelsleden van de Commissie mogen de vergaderingen van de groep bijwonen en aan de werkzaamheden van de groep deelnemen.

5. De groep adviseert het Agentschap over de uitvoering van zijn activiteiten. De groep adviseert met name de uitvoerend directeur met betrekking tot het opstellen van een voorstel voor het werkprogramma van het Agentschap en met betrekking tot de communicatie met de relevante belanghebbenden over alle kwesties met betrekking tot het werkprogramma.

HOOFDSTUK 3 WERKING

Artikel 12
Werkprogramma

1. Het Agentschap voert zijn werkzaamheden uit overeenkomstig zijn werkprogramma, dat alle geplande activiteiten van het Agentschap bevat. Het werkprogramma belet het Agentschap niet om onvoorziene activiteiten op zich te nemen die binnen zijn doelstellingen en taken en binnen de gegeven budgettaire grenzen vallen. De uitvoerend directeur stelt de raad van bestuur in kennis van activiteiten van het Agentschap die niet in het werkprogramma zijn opgenomen.

2. De uitvoerend directeur is verantwoordelijk voor het opstellen van het ontwerpwerkprogramma van het Agentschap, na overleg met de diensten van de Commissie. Vóór 15 maart van elk jaar dient de uitvoerend directeur het ontwerpwerkprogramma voor het volgende jaar in bij de raad van bestuur.

3. De raad van bestuur stelt jaarlijks vóór 30 november het werkprogramma van het Agentschap voor het komende jaar vast, in overleg met de diensten van de Commissie. Het werkprogramma bevat ook een meerjarenvisie. De raad van bestuur ziet erop toe dat het werkprogramma aansluit bij de doelstellingen van het Agentschap, alsook bij de wetgevings- en beleidsprioriteiten van de Unie op het gebied van netwerk- en informatiebeveiliging.

4. Het werkprogramma wordt georganiseerd overeenkomstig het beginsel van activiteitsgestuurd management (Activity-Based Management, ABM). Het werkprogramma spoort met de raming van de inkomsten en uitgaven van het Agentschap en met de begroting van het Agentschap voor het betreffende financiële jaar.

5. De uitvoerend directeur zendt het werkprogramma, nadat dit door de raad van bestuur is aangenomen, naar het Europees Parlement, de Raad, de Commissie en de lidstaten en draagt zorg voor de publicatie ervan.

Artikel 13
Algemeen verslag

1. De uitvoerend directeur dient elk jaar een ontwerp van het algemeen verslag over alle werkzaamheden van het Agentschap tijdens het voorgaande jaar in bij de raad van bestuur.

2. De raad van bestuur stelt jaarlijks vóór 31 maart het algemeen verslag over de werkzaamheden van het Agentschap tijdens het voorgaande jaar vast.

3. De uitvoerend directeur zendt het algemeen verslag van het Agentschap, nadat dit door de raad van bestuur is aangenomen, toe aan het Europees Parlement, de Raad, de Commissie, de Rekenkamer, het Europees Economisch en Sociaal Comité en het Comité van de Regio's en draagt zorg voor de publicatie ervan.

Artikel 14
Verzoeken aan het Agentschap

1. Verzoeken om adviezen en bijstand die binnen de doelstellingen en taken van het Agentschap vallen, dienen aan de uitvoerend directeur te worden gericht, vergezeld van achtergrondinformatie waarin het te behandelen probleem wordt uitgelegd. De uitvoerend directeur stelt de raad van bestuur in kennis van de ontvangen verzoeken en, te zijner tijd, van de follow-up die aan die verzoeken is gegeven. Indien het Agentschap een verzoek weigert, dient zulks te worden gemotiveerd.

2. De in lid 1 genoemde verzoeken kunnen worden ingediend door:

a) het Europees Parlement,

b) de Raad,

c) de Commissie,

d) elke bevoegde instantie die door de lidstaten is aangewezen, zoals een nationale regelgevende instantie volgens de definitie van Richtlijn 2002/21/EG, artikel 2.

3. De praktische regelingen voor de toepassing van de leden 1 en 2, in het bijzonder met betrekking tot de indiening, de vaststelling van prioriteiten, de follow-up en het op de hoogte brengen van de raad van bestuur over de bij het Agentschap ingediende verzoeken, worden door de raad van bestuur vastgesteld in het huishoudelijk reglement van het Agentschap.

Artikel 15
Belangenverklaring

1. De uitvoerend directeur en de door de lidstaten op tijdelijke basis gedetacheerde ambtenaren leggen een schriftelijke verklaring af over hun verplichtingen en een schriftelijke

verklaring over hun belangen waaruit blijkt dat zij geen directe of indirecte belangen hebben die als nadelig voor hun onafhankelijkheid kunnen worden beschouwd.

2. Externe deskundigen die deelnemen aan adhoc-werkgroepen leggen op elke vergadering een verklaring af over belangen die met betrekking tot de agendapunten als nadelig voor hun onafhankelijkheid worden beschouwd, en nemen niet deel aan de bespreking van die punten.

Artikel 16
Transparantie

1. Het Agentschap garandeert dat het zijn activiteiten uitvoert met een hoog niveau van transparantie, overeenkomstig de artikelen 13 en 14.

2. Het Agentschap zorgt ervoor dat het publiek en alle belanghebbenden van objectieve, betrouwbare en gemakkelijk toegankelijke informatie worden voorzien, in het bijzonder en waar passend met betrekking tot de resultaten van zijn werkzaamheden. Tevens maakt het de belangenverklaringen van de uitvoerend directeur en de door de lidstaten op een tijdelijke basis gedetacheerde ambtenaren openbaar, alsmede de belangenverklaringen die deskundigen met betrekking tot agendapunten op de vergaderingen van de adhoc-werkgroepen hebben afgelegd.

3. De raad van bestuur kan op voorstel van de uitvoerend directeur belanghebbenden toestemming geven om de uitvoering van activiteiten van het Agentschap als waarnemer bij te wonen.

4. Het Agentschap legt in zijn huishoudelijk reglement de praktische regelingen voor de toepassing van de in de leden 1 en 2 bedoelde transparantiebepalingen vast.

Artikel 17
Vertrouwelijkheid

1. Onverminderd artikel 14, onthult het Agentschap aan derden geen verwerkte of ontvangen informatie waarvoor om vertrouwelijke behandeling is gevraagd.

2. De leden van de raad van bestuur, de uitvoerend directeur, de leden van de permanente groep van belanghebbenden, de externe deskundigen die deelnemen aan adhoc-werkgroepen en de personeelsleden van het Agentschap, met inbegrip van de door de lidstaten op een tijdelijke basis gedetacheerde ambtenaren, zijn ook na het beëindigen van hun functie gebonden aan de geheimhoudingsplicht uit hoofde van artikel 339 van het Verdrag.

3. Het Agentschap legt in zijn huishoudelijk reglement de praktische regelingen voor de toepassing van de in de leden 1 en 2 bedoelde vertrouwelijkheidsregels vast.

4. De raad van bestuur kan beslissen het Agentschap toestemming te geven om gerubriceerde informatie te verwerken In dat geval stelt de raad van bestuur, in overleg met de relevante diensten van de Commissie, interne regels vast waarbij de beveiligingsbeginselen van Besluit 2001/844/EG, EGKS, Euratom van de Commissie van 29 november 2001 tot w?ziging van

haar reglement van orde worden toegepast[32]. Dit geldt onder meer voor de bepalingen betreffende de uitwisseling, de verwerking en de opslag van gerubriceerde gegevens.

Artikel 18
Toegang tot documenten

1. Verordening (EG) nr. 1049/2001 is van toepassing op de documenten die in het bezit zijn van het Agentschap.

2. De raad van bestuur stelt binnen zes maanden na de oprichting van het Agentschap regelingen voor de uitvoering van Verordening (EG) nr. 1049/2001 vast.

3. Tegen besluiten van het Agentschap uit hoofde van artikel 8 van Verordening (EG) nr. 1049/2001 kan een klacht bij de ombudsman worden ingediend of een beroep bij het Hof van Justitie van de Europese Unie worden ingesteld, op grond van respectievelijk artikel 228 en artikel 263 van het Verdrag.

HOOFDSTUK 4 FINANCIËLE BEPALINGEN

Artikel 19
Vaststelling van de begroting

1. Het Agentschap wordt gefinancierd door een bijdrage uit de begroting van de Europese Unie en bijdragen van derde landen die deelnemen aan de werkzaamheden van het Agentschap, zoals bepaald in artikel 29, en bijdragen van de lidstaten.

2. De uitgaven van het Agentschap hebben betrekking op het personeel, administratieve en technische ondersteuning, infrastructuur, werkingskosten en uitgaven die voortvloeien uit contracten met derden.

3. De uitvoerend directeur stelt jaarlijks, uiterlijk op 1 maart, een ontwerpraming op van de ontvangsten en uitgaven van het Agentschap voor het volgende begrotingsjaar en zendt die, tezamen met een ontwerpoverzicht van de personeelsformatie, aan de raad van bestuur.

4. De ontvangsten en uitgaven moeten in evenwicht zijn.

5. De raad van bestuur stelt jaarlijks de raming van de ontvangsten en uitgaven van het Agentschap voor het volgende begrotingsjaar vast op basis van een door de uitvoerend directeur opgestelde ontwerpraming van de ontvangsten en uitgaven.

6. Deze raming wordt, samen met het ontwerpoverzicht van de personeelsformatie en het ontwerpwerkprogramma, uiterlijk op 31 maart door de raad van bestuur voorgelegd aan de Commissie en de staten waarmee de Europese Unie overeenkomstig artikel 24 een overeenkomst heeft gesloten.

[32] PB L 317 van 3.12.2001 blz. 1.

7. De raming wordt samen met het ontwerp van de algemene begroting van de Europese Unie door de Commissie aan het Europees Parlement en de Raad (hierna beide "de begrotingsautoriteit" genoemd) toegezonden.

8. Op basis van deze raming voert de Commissie in het ontwerp van algemene begroting van de Europese Unie, dat zij overeenkomstig artikel 314 van het Verdrag bij de begrotingsautoriteit indient, de ramingen op die zij nodig acht voor het overzicht van de personeelsformatie en voor de subsidie ten laste van de algemene begroting.

9. De begrotingsautoriteit keurt de kredieten voor de subsidie aan het Agentschap goed.

10. De begrotingsautoriteit stelt de personeelsformatie van het Agentschap vast.

11. De raad van bestuur stelt, samen met het werkprogramma, de begroting van het Agentschap vast. De begroting wordt definitief na de definitieve vaststelling van de algemene begroting van de Europese Unie. Voor zover van toepassing past de raad van bestuur de begroting en het werkprogramma van het Agentschap aan in overeenstemming met de algemene begroting van de Europese Unie. De raad van bestuur zendt de begroting onverwijld toe aan de Commissie en de begrotingsautoriteit.

Artikel 20
Fraudebestrijding

1. Met het oog op de bestrijding van fraude, corruptie en andere illegale handelingen is Verordening (EG) nr. 1073/1999 van het Europees Parlement en de Raad van 25 mei 1999 betreffende onderzoeken door het Europees Bureau voor fraudebestrijding (OLAF)[33] onbeperkt van toepassing.

2. Het Agentschap treedt toe tot het Interinstitutioneel akkoord van 25 mei 1999 tussen het Europees Parlement, de Raad van de Europese Unie en de Commissie van de Europese Gemeenschappen betreffende de interne onderzoeken verricht door het Europees Bureau voor fraudebestrijding (OLAF)[34] en treft onverwijld passende voorzieningen die op alle werknemers van het Agentschap van toepassing zijn.

Artikel 21
Tenuitvoerlegging van de begroting

1. De uitvoerend directeur voert de begroting van het Agentschap uit.

2. De interne controleur van de Commissie heeft ten aanzien van het Agentschap dezelfde bevoegdheden als ten aanzien van de diensten van de Commissie.

3. Uiterlijk op 1 maart van het jaar dat volgt op het afgesloten begrotingsjaar dient de rekenplichtige van het Agentschap de voorlopige rekeningen met het verslag over het budgettaire en financiële beheer van dat begrotingsjaar in bij de rekenplichtige van de Commissie. De rekenplichtige van de Commissie consolideert de voorlopige rekeningen van de instellingen en de gedecentraliseerde organen overeenkomstig artikel 128 van Verordening

[33] PB L 136 van 31.5.1999 blz. 1.
[34] PB L 136 van 31.5.1999 blz. 15.

(EG, Euratom) nr. 1605/2002 van de Raad van 25 juni 2002 houdende het Financieel Reglement van toepassing op de algemene begroting van de Europese Gemeenschappen[35] (hierna het "algemeen Financieel Reglement" genoemd).

4. Uiterlijk op 31 maart van het jaar dat volgt op het afgesloten begrotingsjaar dient de rekenplichtige van de Commissie de voorlopige rekeningen van het Agentschap in bij de Rekenkamer, samen met een verslag over het begrotings- en financieel beheer tijdens het begrotingsjaar. Het verslag over het budgettaire en financiële beheer tijdens het begrotingsjaar wordt tevens aan de begrotingsautoriteit gezonden.

5. Na ontvangst van de opmerkingen van de Rekenkamer over de voorlopige rekeningen van het Agentschap krachtens artikel 129 van het algemeen Financieel Reglement maakt de uitvoerend directeur van het Agentschap onder zijn/haar eigen verantwoordelijkheid de definitieve rekeningen op en legt deze voor advies voor aan de raad van bestuur.

6. De raad van bestuur brengt advies uit over de definitieve rekeningen van het Agentschap.

7. Uiterlijk op 1 juli van het jaar dat volgt op het afgesloten begrotingsjaar dient de uitvoerend directeur de definitieve rekeningen, samen met het advies van de raad van bestuur, in bij het Europees Parlement, de Raad, de Commissie en de Rekenkamer.

8. De uitvoerend directeur publiceert de definitieve rekeningen.

9. De uitvoerend directeur zendt de Rekenkamer uiterlijk op 30 september een antwoord op haar opmerkingen. Hij doet dit antwoord ook toekomen aan de raad van bestuur.

10. De uitvoerend directeur verstrekt het Europees Parlement op verzoek, overeenkomstig het bepaalde in artikel 146, lid 3, van het algemeen Financieel Reglement, alle inlichtingen die nodig zijn voor het goede verloop van de kwijtingsprocedure voor het betrokken begrotingsjaar.

11. Het Europees Parlement verleent op aanbeveling van de Raad vóór 30 april van het jaar N + 2 aan de uitvoerend directeur kwijting inzake de uitvoering van de begroting van het jaar N.

HOOFDSTUK 5 ALGEMENE BEPALINGEN

Artikel 22
Rechtspositie

1. Het Agentschap is een orgaan van de Unie. Het heeft rechtspersoonlijkheid.

2. Het Agentschap beschikt in alle lidstaten over de ruimste handelingsbevoegdheid die volgens de geldende wetgeving aan rechtspersonen wordt verleend. Het kan met name roerende en onroerende goederen verwerven of vervreemden en in rechte optreden.

3. Het Agentschap wordt vertegenwoordigd door zijn uitvoerend directeur.

---

[35] PB L 248 van 16.9.2002 blz. 1.

Artikel 23
Personeel

1. De regels en voorschriften die van toepassing zijn op ambtenaren en andere personeelsleden van de Europese Unie zijn eveneens van toepassing op het personeel van het Agentschap, inclusief de uitvoerend directeur.

2. De raad van bestuur oefent ten aanzien van de uitvoerend directeur de bevoegdheden uit die krachtens het Statuut van de ambtenaren van de Europese Gemeenschappen zijn verleend aan het tot aanstelling bevoegde gezag, alsook die welke krachtens de Regeling die van toepassing is op de andere personeelsleden van de Europese Gemeenschappen zijn verleend aan het tot het sluiten van overeenkomsten bevoegde gezag.

3. De uitvoerend directeur oefent ten aanzien van het personeel van het Agentschap de bevoegdheden uit die krachtens het Statuut van de ambtenaren van de Europese Gemeenschappen zijn verleend aan het tot aanstelling bevoegde gezag, alsook die welke krachtens de Regeling die van toepassing is op de andere personeelsleden van de Europese Gemeenschappen zijn verleend aan het tot het sluiten van overeenkomsten bevoegde gezag.

4. Het Agentschap mag gedetacheerde nationale deskundigen van de lidstaten in dienst nemen. Het Agentschap stelt in zijn huishoudelijk reglement de praktische regelingen vast voor dergelijke indienstnames.

Artikel 24
Voorrechten en immuniteiten

Het Protocol inzake voorrechten en immuniteiten van de Europese Gemeenschappen is van toepassing op het Agentschap en het personeel ervan.

Artikel 25
Aansprakelijkheid

1. De contractuele aansprakelijkheid van het Agentschap wordt beheerst door het recht dat op de betrokken overeenkomst van toepassing is.

Het Hof van Justitie van de Europese Unie is bevoegd uitspraak te doen krachtens arbitrageclausules in door het Agentschap gesloten overeenkomsten.

2. In geval van niet-contractuele aansprakelijkheid vergoedt het Agentschap, overeenkomstig de algemene beginselen die de wetgevingen van de lidstaten gemeen hebben, alle schade die door het Agentschap zelf of zijn personeelsleden in de uitoefening van hun functie is veroorzaakt.

Het Hof van Justitie is bevoegd voor geschillen over de vergoeding van dergelijke schade.

3. De persoonlijke aansprakelijkheid van de personeelsleden van het Agentschap ten aanzien van het Agentschap is geregeld bij de desbetreffende bepalingen die van toepassing zijn op het personeel van het Agentschap.

Artikel 26
Talen

1. De bepalingen van Verordening nr. 1 van de Raad van 15 april 1958 tot regeling van het taalgebruik in de Europese Economische Gemeenschap[36] zijn van toepassing op het Agentschap. De lidstaten en de overige door de lidstaten aangewezen instanties kunnen hun verzoeken aan het Agentschap richten en daarop een antwoord verlangen in de EU-taal van-hun keuze.

2. De voor het functioneren van het Agentschap vereiste vertaaldiensten worden geleverd door het Vertaalbureau voor de organen van de Europese Unie.

Artikel 27
Bescherming van persoonsgegevens

Bij het verwerken van gegevens met betrekking tot personen is het Agentschap onderworpen aan de bepalingen van Verordening (EG) nr. 45/2001.

Artikel 28
Deelname van derde landen

1. Het Agentschap staat open voor deelneming van derde landen die met de Europese Unie overeenkomsten gesloten hebben uit hoofde waarvan zij de EU-wetgeving op het onder deze verordening vallende gebied hebben overgenomen en toegepast.

2. Overeenkomstig de desbetreffende bepalingen van deze overeenkomsten worden regelingen getroffen waarin met name de aard, de omvang en de methode van deelneming van deze landen aan de werkzaamheden van het Agentschap worden uiteengezet, met inbegrip van bepalingen met betrekking tot de deelneming aan de door het Agentschap ontwikkelde initiatieven, de financiële bijdragen en het personeel.

HOOFDSTUK 6 SLOTBEPALINGEN

Artikel 29
Toetsing

1. Binnen drie jaar na de in artikel 34 vermelde datum van oprichting van het Agentschap voert de Commissie, rekening houdend met het standpunt van alle belanghebbenden, een toetsing uit op basis van het met de raad van bestuur overeengekomen mandaat. In het kader van deze toetsing beoordeelt de Commissie de impact en effectiviteit van het Agentschap bij het verwezenlijken van de in artikel 2 uiteengezette doelstellingen, en de effectiviteit van de werkmethoden van het Agentschap. De Commissie voert deze toetsing met name uit om na te gaan of het Agentschap nog steeds een effectief instrument is en om te beoordelen of de looptijd van het Agentschap verder moet worden verlengd na afloop van de in artikel 34 gespecificeerde termijn.

[36] PB 17 van 6.10.1958, blz. 385/58. Verordening als laatstelijk gewijzigd bij de Toetredingsakte van 1994.

2. De resultaten van de toetsing worden door de Commissie toegezonden aan het Europees Parlement en de Raad en worden openbaar gemaakt.

3. De raad van bestuur ontvangt de toetsing en doet de Commissie aanbevelingen met het oog op wijzigingen van deze verordening, het Agentschap en zijn werkmethoden. De raad van bestuur en de uitvoerend directeur houden rekening met de resultaten van de toetsing in de meerjarenplanning van het Agentschap.

Artikel 30
Medewerking van de lidstaat van vestiging

De lidstaat van vestiging zorgt voor zo gunstig mogelijke voorwaarden voor de soepele en vlotte werking van het Agentschap.

Artikel 31
Administratieve controle

De activiteiten van het Agentschap staan onder het toezicht van de Ombudsman, overeenkomstig artikel 228 van het Verdrag.

Artikel 32
Intrekking en opvolging

1. Verordening (EG) nr. 460/2004 wordt ingetrokken.

Verwijzingen naar Verordening (EG) nr. 460/2004 en naar het ENISA worden opgevat als verwijzingen naar deze verordening en naar het Agentschap.

2. Het Agentschap is de opvolger van het bij Verordening (EG) nr. 460/2004 opgerichte Agentschap voor wat alle eigendommen, overeenkomsten, wettelijke verplichtingen, arbeidsovereenkomsten, financiële verbintenissen en verplichtingen betreft.

Artikel 33
Duur

Het Agentschap wordt opgericht met ingang van […] voor een periode van vijf jaar.

Artikel 34
Inwerkingtreding

Deze verordening treedt in werking op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie* en is van toepassing met ingang van 14 maart 2012 of de dag na de publicatie ervan, indien dit later is.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te […],

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

FINANCIEEL MEMORANDUM VOOR VOORSTELLEN

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Voorstel voor een verordening van het Europees Parlement en de Raad Inzake het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA)

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

Informatiemaatschappij en media.

Regelgevingskader voor de digitale agenda

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. De met het voorstel/initiatief beoogde strategische meerjarendoelstelling(en) van de Commissie

Coherentie van regelgevende benaderingen – begeleiding en advies verstrekken aan de Commissie en de lidstaten om een holistisch normatief kader op het gebied van netwerk- en informatiebeveiliging te ontwikkelen en te actualiseren.

Preventie, detectie en respons – de paraatheid verbeteren door te bij te dragen tot een Europese capaciteit voor vroegtijdige waarschuwing en respons bij incidenten, pan-Europese noodplannen en oefeningen.

Verbetering van de kennis van beleidmakers – bijstand verlenen en advies verstrekken aan de Commissie en de lidstaten om in de hele Unie een hoog niveau van kennis te bereiken over kwesties die verband houden met netwerk- en informatiebeveiliging en de toepassing ervan op de belanghebbenden uit de sector. Dit omvat ook het produceren, analyseren en beschikbaar stellen van gegevens over de economische aspecten en de gevolgen van inbreuken op de netwerk- en informatiebeveiliging, stimulansen voor belanghebbenden om te investeren in maatregelen voor netwerk- en informatiebeveiliging, risico-identificatie, indicatoren van de toestand op het gebied van netwerk- en informatiebeveiliging in de Unie enz.

---

[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.

Empowerment van belanghebbenden – een cultuur van beveiliging en risicobeheer ontwikkelen door informatie-uitwisseling en brede samenwerking tussen actoren uit de publieke en de private sector aan te moedigen, ook rechtstreeks ten behoeve van de burger, en door een cultuur van bewustzijn van netwerk- en informatiebeveiliging tot stand te brengen.

Europa beschermen tegen internationale bedreigingen – een hoog niveau van samenwerking met derde landen en internationale organisaties tot stand brengen om een gemeenschappelijke mondiale benadering van netwerk- en informatiebeveiliging te bevorderen en om ervoor te zorgen dat internationale activiteiten op hoog niveau in Europa hun effect niet missen.

De weg bereiden voor coöperatieve tenuitvoerlegging – samenwerking bevorderen bij de tenuitvoerlegging van beleid op het gebied van netwerk- en informatiebeveiliging.

Cybercriminaliteit bestrijden – aspecten van de strijd tegen cybercriminaliteit die verband houden met netwerk- en informatiebeveiliging integreren in besprekingen en in de uitwisseling van goede praktijken tussen publieke en private belanghebbenden, met name via samenwerking met autoriteiten van de voormalige tweede en derde pijlers, zoals Europol.

1.4.2. Specifieke doelstelling(en) en betrokken ABM/ABB-activiteiten

Specifieke doelstelling

De netwerk- en informatiebeveiliging vergroten, een cultuur van netwerk- en informatiebeveiliging ontwikkelen ten bate van burgers, consumenten, bedrijven en organisaties uit de publieke sector en beleidsuitdagingen ten gevolge van toekomstige netwerken en het internet identificeren.

Betrokken AMB/ABB-activiteit(en)

Beleid inzake elektronische communicatie en netwerkbeveiliging

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

Het initiatief zal naar verwachting de volgende economische gevolgen hebben:

- grotere beschikbaarheid van informatie over huidige en toekomstige uitdagingen en risico's op het gebied van beveiliging en veerkracht;

- vermijden dat de inspanningen die individuele lidstaten leveren voor het verzamelen van relevante informatie over risico's, bedreigingen en kwetsbare punten, elkaar overlappen;

- beleidmakers zullen beter geïnformeerd zijn wanneer zij beslissingen nemen;

- hogere kwaliteit van nationale beleidsmaatregelen inzake netwerk- en informatiebeveiliging door de verspreiding van goede praktijken;

- schaalvoordelen bij het reageren op incidenten op EU-niveau;

- meer investeringen door gemeenschappelijke beleidsdoelstellingen en normen voor beveiliging en veerkracht op EU-niveau;

- minder operationele risico's voor bedrijven door het hoger niveau van beveiliging en veerkracht;

- coherentere maatregelen ter bestrijding van cybercriminaliteit.

Het initiatief zal naar verwachting de volgende sociale gevolgen hebben:

- groter vertrouwen van de gebruikers in diensten en systemen van de informatiemaatschappij;

- groter vertrouwen in de werking van de interne EU-markt door hogere niveaus van consumentenbescherming;

- meer uitwisseling van informatie en kennis met niet-EU-landen;

- betere bescherming van de grondrechten van de EU door het garanderen van gelijke niveaus van bescherming van de persoonsgegevens en de privacy van EU-burgers.

De gevolgen voor het milieu zullen naar verwachting zeer klein zijn:

- minder CO_2-emissies, bijvoorbeeld omdat de toename van het gebruik van ICT-systemen en diensten minder verplaatsingen tot gevolg heeft en omdat de schaalvoordelen bij de tenuitvoerlegging van de beveiligingsverplichtingen tot minder energieverbruik leiden.

1.4.4. Resultaat- en effectindicatoren

Per doelstelling kan aan de hand van de volgende indicatoren worden nagegaan in hoeverre het initiatief is uitgevoerd:

Coherentie van regelgevende benaderingen:

- Aantal lidstaten dat bij het opstellen van hun beleid gebruik heeft gemaakt van de aanbevelingen van het Agentschap;

- Aantal studies die gericht zijn op het identificeren van hiaten en onverenigbaarheden in het normaliseringslandschap op het gebied van netwerk- en informatiebeveiliging;

- Grotere overeenstemming tussen de nationale benaderingen van netwerk- en informatiebeveiliging.

Preventie, detectie en respons:

- Aantal georganiseerde opleidingen op het gebied van netwerkbeveiliging;

- Beschikbaarheid van een functionerend systeem voor vroegtijdige waarschuwing voor ontluikende risico's en aanvallen;

- Aantal oefeningen op het gebied van netwerk- en informatiebeveiliging die op EU-niveau door het Agentschap worden gecoördineerd.

Verbetering van de kennis van beleidmakers:

- Aantal studies om informatie te verzamelen over actuele en verwachte risico's op het gebied van netwerk- en informatiebeveiliging en over technologieën voor risicopreventie;

- Aantal raadplegingen van overheidsorganen die zich bezighouden met netwerk- en informatiebeveiliging;

- Beschikbaarheid van een Europees kader voor het organiseren van de gegevensverzameling op het gebied van netwerk- en informatiebeveiliging.

Empowerment van belanghebbenden:

- Aantal geïdentificeerde goede praktijken voor het bedrijfsleven;

- Niveau van investeringen in beveiligingsmaatregelen door particuliere belanghebbenden.

Europa beschermen tegen internationale bedreigingen:

- Aantal conferenties/vergaderingen tussen EU-lidstaten om gemeenschappelijke doelstellingen voor netwerk- en informatiebeveiliging vast te stellen;

- Aantal vergaderingen tussen Europese en internationale deskundigen op het gebied van netwerk- en informatiebeveiliging.

De weg bereiden voor coöperatieve tenuitvoerlegging:

- Aantal beoordelingen van de naleving van de regelgeving;

- Aantal EU-wijde praktijken op het gebied van netwerk- en informatiebeveiliging.

Bestrijding van cybercriminaliteit:

- Regelmaat van interacties met agentschappen van de voormalige tweede en derde pijlers;

- Aantal gevallen waarin deskundigheid werd verstrekt voor onderzoeken naar misdrijven.

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoefte(n) waarin op korte of lange termijn moet worden voorzien

Het ENISA is opgericht in 2004 om bedreigingen van de netwerk- en informatiebeveiliging en mogelijke inbreuken op die beveiliging aan te pakken. Sindsdien zijn de uitdagingen in verband met netwerk- en informatiebeveiliging geëvolueerd door technologische en marktontwikkelingen en zijn ze het voorwerp geweest van verdere beschouwing en discussie, waardoor het vandaag mogelijk is nauwkeuriger te beschrijven wat de exacte problemen zijn en hoe deze worden beïnvloed door de veranderingen op het gebied van netwerk- en informatiebeveiliging.

1.5.2. Toegevoegde waarde van de deelname van de EU

Problemen met netwerk- en informatiebeveiliging stoppen niet aan nationale grenzen en kunnen dus ook niet efficiënt worden aangepakt op nationaal niveau alleen. Tegelijk zijn er grote verschillen in de manier waarop het probleem wordt aangepakt door publieke autoriteiten in verschillende lidstaten. Deze verschillen kunnen een belangrijke hinderpaal vormen voor de toepassing van passende mechanismen ter verbetering van netwerk- en informatiebeveiliging in de hele Unie. Door de verwevenheid van ICT-infrastructuren wordt de effectiviteit van nationale maatregelen in een lidstaat nog steeds in grote mate beïnvloed door maatregelen van een lager niveau in andere lidstaten en door het gebrek aan systematische grensoverschrijdende samenwerking. Een gebrek aan maatregelen voor netwerk- en informatiebeveiliging in één lidstaat kan verstoringen van de dienstverlening in andere lidstaten veroorzaken.

Bovendien leidt de vermenigvuldiging van beveiligingseisen tot kosten voor bedrijven die op Europese schaal actief zijn en tot een versnippering en gebrek aan concurrentievermogen op de Europese interne markt.

De afhankelijkheid van netwerk- en informatiesystemen neemt toe, maar er lijkt onvoldoende bereidheid te zijn om incidenten aan te pakken.

De huidige nationale systemen voor vroegtijdige waarschuwing en aanpak van incidenten vertonen belangrijke gebreken. De procedures en praktijken voor het monitoren en rapporteren van incidenten op het gebied van netwerkbeveiliging verschillen sterk per lidstaat. In sommige landen zijn de procedures onvoldoende geformaliseerd, terwijl er in andere landen geen bevoegde autoriteit is voor het ontvangen en verwerken van verslagen over incidenten. Er bestaan geen Europese systemen. Ten gevolge daarvan kan de basisdienstverlening grondig worden verstoord door incidenten op het gebied van netwerk- en informatiebeveiliging; daarom moeten passende reacties worden voorbereid. In de mededeling van de Commissie betreffende de bescherming van kritieke informatie-infrastructuur wordt ook benadrukt dat er behoefte is aan Europese capaciteit voor vroegtijdige waarschuwing en incidentenrespons, eventueel ondersteund door oefeningen op Europese schaal.

Er is een duidelijke behoefte aan beleidsinstrumenten die erop gericht zijn risico's en kwetsbare plekken met betrekking tot netwerk- en informatiebeveiliging proactief te identificeren, passende responsmechanismen vast te stellen (bijv. via de identificatie en verspreiding van goede praktijken) en te garanderen dat de belanghebbenden deze responsmechanismen kennen en toepassen.

1.5.3. De lessen die uit reeds verrichte soortgelijke activiteiten zijn getrokken

Zie punten *1.5.1 en 1.5.2.*

1.5.4. Samenhang en eventuele synergie met andere relevante instrumenten

Dit initiatief is volledig coherent met het algemene debat over netwerk- en informatiebeveiliging en andere beleidsinitiatieven waarin aandacht wordt besteed aan de toekomst van netwerk- en informatiebeveiliging. Het is een van de hoofdonderdelen van de Digitale Agenda voor Europa, een vlaggenschipinitiatief van de Europa 2020-strategie.

1.6. Duur en financiële gevolgen

☑ Voorstel/initiatief met een **beperkte geldigheidsduur**

– ☑ De verlenging van de looptijd met vijf jaar begint op 14.3.2012 of op de dag dat de nieuwe verordening van kracht wordt, als dit later is.

– ☑ Financiële gevolgen van 2012 tot en met 2017

☐ Voorstel/initiatief met een **onbeperkte geldigheidsduur**

– Uitvoering met een opstartperiode vanaf JJJJ tot en met JJJJ,

– gevolgd door een volledige uitvoering.

1.7. Beheersvorm(en)[39]

☐ **Direct gecentraliseerd beheer** door de Commissie

☑ **Indirect gecentraliseerd beheer** door uitvoeringstaken te delegeren aan:

– ☐ uitvoerende agentschappen

– ☑ door de Gemeenschappen 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 de lidstaten

☐ **Gedecentraliseerd beheer** met derde landen

☐ **Gezamenlijk beheer** met internationale organisaties ***(geef aan welke)***

---

[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.html

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

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

De uitvoerend directeur is verantwoordelijk voor het effectieve toezicht en het toetsen van de prestaties van het Agentschap aan zijn doelstellingen en rapporteert jaarlijks aan de raad van bestuur.

De uitvoerend directeur stelt een algemeen verslag op betreffende alle activiteiten van het Agentschap in het afgelopen jaar, waarin met name de behaalde resultaten worden vergeleken met de doelstellingen van het jaarlijkse werkprogramma. Na goedkeuring door de raad van bestuur wordt dit verslag aan het Europees Parlement, de Raad, de Commissie, de Rekenkamer, het Europees Economisch en Sociaal Comité en het Comité van de Regio's toegezonden en gepubliceerd.

2.2. Beheers- en controlesysteem

2.2.1. Geconstateerde risico's

Sinds het ENISA in 2004 is opgericht, werd het aan externe en interne evaluaties onderworpen.

Overeenkomstig artikel 25 van de ENISA-Verordening was de eerste stap in dit proces de onafhankelijke evaluatie van het ENISA door een panel van externe deskundigen in 2006/2007. Het verslag van het panel van externe deskundigen[41] bevestigde dat de oorspronkelijke beleidsredenen voor het oprichten van het ENISA en de oorspronkelijke doelstellingen ervan nog steeds geldig zijn en speelde een rol in het aan de orde stellen van sommige problemen die moeten worden aangepakt.

In maart 2007 heeft de Commissie over de evaluatie verslag uitgebracht aan de raad van bestuur, die vervolgens zelf aanbevelingen heeft gedaan voor de toekomst van het Agentschap en voor wijzigingen van de ENISA-Verordening[42].

In juni 2007 heeft de Commissie haar eigen beoordeling van de resultaten van de externe evaluatie en de aanbevelingen van de raad van bestuur in een mededeling aan het Europees Parlement en de Raad voorgelegd[43]. Volgens de mededeling moet worden gekozen tussen de verlenging van het mandaat van het Agentschap of de vervanging van het Agentschap door een ander mechanisme zoals een permanent forum van belanghebbenden of een netwerk van organisaties op het gebied van beveiliging. De mededeling lanceerde ook een openbare

41 http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm.

42 Overeenkomstig artikel 25 van de ENISA-verordening. De volledige tekst van het door de raad van bestuur van het ENISA aangenomen document, dat ook de overwegingen van de raad van bestuur bevat, is beschikbaar op de volgende website: http://enisa.europa.eu/pages/03_02.htm.

43 Mededeling van de Commissie aan het Europees Parlement en de Raad inzake de evaluatie van het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), COM(2007) 285 definitief van 1.6.2007: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT.

raadpleging over het onderwerp, en vroeg aan de hand van een vragenlijst ter oriëntatie van de verdere besprekingen de Europese belanghebbenden om inbreng[44].

2.2.2. Controlemiddel(en)

Zie punten 2.1 en 2.2.1

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

De rekeningen voor alle uitbestede diensten en studies worden door het personeel van het Agentschap vóór de feitelijke uitbetaling gecontroleerd, met inachtneming van eventuele contractuele verplichtingen, economische beginselen en goede financiële of beheerspraktijken. In alle overeenkomsten en contracten tussen het Agentschap en de begunstigden van eventuele betalingen worden fraudebestrijdingsbepalingen (eisen ten aanzien van toezicht, verslaglegging, enz.) opgenomen.

[44] http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF*

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

- Bestaande begrotingsonderdelen voor uitgaven

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Type uitgaven	Bijdrage			
	Nummer / Beschrijving	GK/ NGK[45]	van EVA-landen[46]	van kandidaat-lidstaten[47]	van derde landen	in de zin van artikel 18, lid 1, onder a bis), van het Financieel Reglement
1.a Concurrentievermogen voor groei en werkgelegenheid	09 02 03 01 Europees Agentschap voor netwerk- en informatiebeveiliging – Subsidie op grond van titels 1 en 2	GK	JA	NEE	NEE	NEE
	09 02 03 02 Europees Agentschap voor netwerk- en informatiebeveiliging – Subsidie op grond van titel 3	GK	JA	NEE	NEE	NEE
5 Administratieve uitgaven	09 01 01 Uitgaven voor personeel in actieve dienst voor het beleidsterrein "Informatiemaatschappij en media"	NGK	NEE	NEE	NEE	NEE
	09 01 02 11 Andere beheersuitgaven	NGK	NEE	NEE	NEE	NEE

* De verwachte financiële gevolgen van het voorstel voor de periode na de huidige financiële programmeringsperiode 2007-2013 komen niet aan bod in dit financieel memorandum. Op basis van het voorstel van de Commissie voor de verordening waarbij het meerjarig financieel kader voor de periode na 2013 wordt vastgesteld, en rekening houdende met de conclusies van de effectbeoordeling, zal de Commissie een gewijzigd financieel memorandum presenteren.

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

46 EVA: Europese Vrijhandelsassociatie.

47 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.a	Concurrentiekracht ter bevordering van groei en werkgelegenheid

ENISA			1 jan. – 13 maart 2012	14 maart – 31 dec. 2012	2013	2014	2015	2016	1 jan. – 13 maart 2017	**TOTAAL 14 maart 2012 – 13 maart 2017**
Beleidskredieten										
09 02 03 02 Europees Agentschap voor netwerk- en informatiebeveiliging – Subsidie op grond van titel 3	Vastleggingen	(1)	0,454	1,976	2,470	--	--	--	--	--
	Betalingen	(2)	0,454	1,976	2,470	--	--	--	--	--
Administratieve kredieten										
09 02 03 01 Europees Agentschap voor netwerk- en informatiebeveiliging – Subsidie op grond van titels 1 en 2		(3)	1,293	4,697	6,120	--	--	--	--	--
TOTAAL kredieten onder RUBRIEK 1a	Vastleggingen	=1 +3	1,747	6,673	8,590	--	--	--	--	--
	Betalingen	=2+3	1,747	6,673	8,590	--	--	--	--	--

TOTAAL operationele	Vastleggingen	(4)	0,454	1,976	2,470	--	--	--	--	--

kredieten	Betalingen	(5)	0,454	1,976	2,470	--	--	--	--	--
TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten		(6)	1,293	4,697	6,120	--	--	--	--	--
TOTAAL kredieten onder rubriek 1.a. van het meerjarig kaderprogramma	Vastleggingen	=4+6	1,747	6,673	8,590	--	--	--	--	--
	Betalingen	=5+6	1,747	6,673	8,590	--	--	--	--	--

in miljoenen euro's (tot op 3 decimalen)

Rubriek van het meerjarig financieel kader:	5	Administratieve uitgaven

		1 jan. – 13 maart 2012	14 maart – 31 dec. 2012	2013	2014	2015	2016	1 jan. – 13 maart 2017	Totaal
Personele middelen		0,085	0,342	0,427	--	--	--	--	--
Andere administratieve uitgaven		0,002	0,013	0,015	--	--	--	--	--
TOTAAL DG INFSO	Kredieten	0,087	0,355	0,442	--	--	--	--	--

TOTAAL kredieten onder RUBRIEK 5 van het meerjarig financieel kader	(Totaal vastleggingen = totaal betalingen)	0,087	0,355	0,442	--	--	--	--	--

		1 jan. – 13 maart 2012	14 maart – 31 dec. 2012	2013	2014	2015	2016	1 jan. – 13 maart 2017	Totaal
TOTAAL kredieten onder RUBRIEKEN 1 tot en met 5 van het meerjarig financieel kader	Vastleggingen	1,834	7,028	9,032	--	--	--	--	--
	Betaling	1,834	7,028	9,032	--	--	--	--	--

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, in miljoenen euro's (tot op 3 decimalen)

Vermeld doelstellingen en outputs ⇩	1 jan. – 13 maart 2012	14 maart – 31 dec. 2012	2013	2014	2015	2016	1 jan. – 13 maart 2017	**TOTAAL 14 maart 2012 – 13 maart 2017**
Coherentie van regelgevende benaderingen	0,114	0,494	0,620	--	--	--	--	--
Preventie, detectie en respons	0,114	0,494	0,620	--	--	--	--	--
Verbetering van de kennis van beleidmakers	0,068	0,297	0,370	--	--	--	--	--
Empowerment van belanghebbenden	0,050	0,218	0,270	--	--	--	--	--
Europa beschermen tegen internationale bedreigingen	0,023	0,099	0,120	--	--	--	--	--
De weg bereiden voor coöperatieve tenuitvoerlegging	0,064	0,276	0,340	--	--	--	--	--
Bestrijding van cybercriminaliteit	0,023	0,098	0,120	--	--	--	--	--
TOTALE KOSTEN	0,454	1,976	2,460	--	--	--	--	--

3.2.3. Geraamde gevolgen voor de administratieve kredieten[48]

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:

a) Administratieve uitgaven onder Rubriek 5 van het meerjarig financieel kader

in miljoenen euro's (tot op 3 decimalen)

RUBRIEK 5 van het meerjarig financieel kader	1 jan. – 13 maart 2012	14 maart – 31 dec. 2012	2013	2014	2015	2016	1 jan. – 13 maart 2017	**Totaal 14 maart 2012 – 13 maart 2017**
Personele middelen	0,085	0,342	0,427	--	--	--	--	--
Andere administratieve uitgaven	0,002	0,013	0,015	--	--	--	--	--
TOTAAL	0,087	0,355	0,442	--	--	--	--	--

b) Administratieve uitgaven met betrekking tot het ENISA - onder begrotingsonderdeel "09.020301 Europese netwerk- en informatiebeveiliging: Titel 1 – Personeel en titel 2 – werking van het Agentschap".

in miljoenen euro's (tot op 3 decimalen)

	1 jan. – 13 maart 2012	14 maart – 31 dec. 2012	2013	2014	2015	2016	1 jan. – 13 maart 2017	**Totaal 14 maart 2012 – 13 maart 2017**
Personele middelen - Titel 1 – Personeel	1,153	4,329	5,607	--	--	--	--	--
Andere uitgaven van administratieve aard – Titel 2 – Werking van het Agentschap	0,140	0,368	0,513	--	--	--	--	--
TOTAAL	**1,293**	**4,697**	**6,120**	--	--	--	--	--

[48] De bijlage bij het financieel memorandum is niet ingevuld omdat het niet van toepassing is op het huidige voorstel.

3.2.3.2. Geraamde personeelsbehoeften

Elk jaar moet het personeelsoverzicht van het Agentschap worden toegelicht en gerechtvaardigd in een 'Personeelsbeleidsplan', dat bij de begrotingsautoriteit moet worden ingediend.

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

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

a) Personele middelen binnen de Commissie

	1 jan. – 13 maart 2012	14 maart – 31 dec. 2012	2013	2014	2015	2016	1 jan. – 13 maart 2017
Plaatsen volgens de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)							
XX 01 01 01 (zetel en vertegenwoordigingen van de Commissie)	3,5	3,5	3,5	--	--	--	--
TOTAAL	**3,5**	**3,5**	**3,5**	--	--	--	--

b) Personele middelen van het ENISA

		1 jan. – 13 maart 2012	14 maart – 31 dec. 2012	2013	2014	2015	2016	1 jan. – 13 maart 2017
Lijst van het aantal ambten van het ENISA (in voltijdequivalent, VTE)								
Ambtenaren en tijdelijk personeel	AD	29	31	31	--	--	--	--
	AST	15	16	16	--	--	--	--
TOTAAL Ambtenaren en tijdelijk personeel		44	47	47	--	--	--	--
Ander personeel (in VTE)								
Arbeidscontractanten		13	14	14	--	--	--	--
Gedetacheerde nationaal deskundigen		5	5	5	--	--	--	--
Totaal ander personeel		18	19	19	--	--	--	--
TOTAAL		**62**	**66**	**66**	--	--	--	--

Beschrijving van de taken die het personeel van het Agentschap moet uitvoeren:

Ambtenaren en tijdelijke functionarissen	Het Agentschap blijft verder: – adviserende en coördinerende functies hebben voor zover het **gegevens** over informatiebeveiliging **verzamelt en analyseert**. Tegenwoordig verzamelen zowel openbare als particuliere instellingen met uiteenlopende bedoelingen gegevens over IT-incidenten en andere gegevens die relevant zijn voor informatiebeveiliging. Er is echter geen centrale entiteit op Europees niveau die gegevens kan verzamelen en analyseren en opinies en advies kan verstrekken voor het ondersteunen van het beleidswerk van de Unie inzake netwerk- en informatiebeveiliging; – **optreden** als een **centrum van deskundigheid** waartoe zowel de lidstaten als de Europese instellingen zich kunnen wenden voor **opinies en advies over technische aangelegenheden** betreffende beveiliging; – bijdragen tot **brede samenwerking tussen verschillende actoren** op het gebied van informatiebeveiliging, bijv. assistentie verlenen bij de vervolgactiviteiten ter ondersteuning van beveiligd e-zakendoen. Dergelijke samenwerking is een essentiële eerste voorwaarde voor een veilige werking van netwerken en informatiesystemen in Europa. Deelname en betrokkenheid van alle belanghebbenden is nodig; – bijdragen tot een gecoördineerde aanpak van informatiebeveiliging door **ondersteuning van lidstaten**, bijv. inzake **bevordering van risicobeoordeling** en bewustmakingsactiviteiten; – de **interoperabiliteit van netwerken en informatiesystemen** waarborgen wanneer lidstaten technische eisen **toepassen** die van invloed zijn op de veiligheid; – de **relevante normalisatie-eisen** identificeren, bestaande beveiligingsnormen en certificeringssystemen beoordelen en het gebruik op zo breed mogelijke schaal ervan ter ondersteuning van de Europese wetgeving bevorderen; – **internationale samenwerking** op dit gebied ondersteunen, die steeds meer nodig is aangezien netwerk- en informatiebeveiligingsproblemen een mondiaal karakter hebben.
Extern personeel	Zie hoger

3.2.4. Verenigbaarheid met het huidige 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/initiatief vergt toepassing van het flexibiliteitsinstrument of herziening van het meerjarig financieel kader[49]

De EU-financiering na 2013 zal worden onderzocht in de context van een bespreking van alle voorstellen voor de periode na 2013 in de hele Commissie. Dit betekent dat de Commissie, zodra zij haar voorstel voor het volgende meerjarig financieel kader heeft ingediend, een gewijzigd financieel memorandum zal presenteren waarin rekening wordt gehouden met de conclusies van de effectbeoordeling.

3.2.5. Bijdrage van derden aan de financiering

– ☐ Het voorstel/initiatief voorziet niet in medefinanciering door derden

– ☑ Het voorstel/initiatief voorziet in medefinanciering, zoals hieronder wordt geraamd:

Indicatieve kredieten, in miljoen euro (tot op 3 decimalen)

	1 jan. – 13 maart 2012	14 maart – 31 dec. 2012	2013	2014	2015	2016	1 jan. – 13 maart 2017	**Totaal 14 maart 2012 – 13 maart 2017**
EVA	0,042	0,160	0,206	--	--	--	--	--

3.3. Geraamde gevolgen voor de ontvangsten

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

– ☐ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:

– ☐ voor de eigen middelen

– ☐ voor de diverse ontvangsten

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