Fiche 1: verordening European Network and Information Security Agency

1. Algemene gegevens

Titel voorstel

1. Voorstel voor een Verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EC) Nr. 460/2004 ten aanzien van de vaststelling van de mandaatsperiode voor de European Network and Information Security Agency (ENISA)
2. Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de European Network and Information Security Agency (ENISA)

Datum Commissiedocument

1. 30 september 2010
2. 30 september 2010

Nr. Commissiedocument

1. COM(2010) 520 definitief
2. COM(2010) 521 definitief

Prelex

1. http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=nl&DosId=199701
2. http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=nl&DosId=199702

Nr. impact-assessment Commissie en Opinie Impact-assessment Board

http://ec.europa.eu/governance/impact/planned_ia/roadmaps_2010_en.htm#information: *impact assessment* voor COM(2010) 521 is in de afrondende fase, maar nog niet online beschikbaar.

Behandelingstraject Raad

De Telecomraad van 2 december 2010 zal geïnformeerd worden over de stand van zaken.

Eerstverantwoordelijk ministerie

Ministerie van Economische Zaken, Landbouw en Innovatie

Rechtsbasis, besluitvormingsprocedure, rol Europees Parlement, delegatie en comitologie

a) Rechtsbasis
Art. 114 VWEU

b) Stemwijze Raad en rol Europees Parlement
Gewone wetgevingsprocedure (gekwalificeerde meerderheidsbesluitvorming in de Raad, medebeslissing Europees Parlement)

c) Delegatie en/of comitologie
Niet van toepassing.

2. Samenvatting BNC-fiche

Het gaat om twee voorstellen. Het ene voorstel vraagt om een verlenging van het mandaat van het European Network and Information Security Agency (ENISA) met 18 maanden zodat er voldoende ruimte is voor debat over het andere voorstel, een verordening om ENISA te versterken en te moderniseren en een mandaat te geven voor vijf jaar. De belangrijkste veranderingen in dit tweede Commissievoorstel ten opzichte van de huidige situatie zijn: grotere flexibiliteit voor ENISA door bredere taakomschrijving; betere afstemming van ENISA met het EU-beleid en regelgevingproces; meer interactie in de strijd tegen *cybercrime*; versterken van bestuursstructuur en een geleidelijke toename van de middelen (qua financiën en mankracht).

Omdat in veel gevallen de netwerk- en informatiebeveiligingsproblematiek grensoverschrijdend is, vindt Nederland een aanpak op Europees niveau gewenst en is een uitbreidende rol van ENISA op zijn plaats. Dit biedt volgens Nederland namelijk goede mogelijkheden om problemen in de netwerk- en informatiebeveiliging op Europees niveau aan te pakken. Wel zal Nederland kritisch kijken naar de voorstellen voor het toekomstig budget in het licht van het nieuwe mandaat voor ENISA.

3. Samenvatting voorstel

Inhoud voorstel

ENISA is in 2004 (Verordening (EC) No 460/2004) opgericht met als doel het verzekeren van een hoog en effectief niveau van netwerk- en informatiebeveiliging binnen de EU, zodat een cultuur van netwerk- en informatiebeveiliging wordt ontwikkeld waar burgers, consumenten, bedrijven en publiekesectororganisaties van de EU van profiteren en die bijdraagt aan het soepel functioneren van de interne markt. ENISA doet dit door deskundig advies uit te brengen aan nationale overheden en EU-instellingen, het uitwisselen van goede methoden en door het leggen van contacten tussen EU-instellingen, nationale autoriteiten en bedrijven.

In COM(2010) 520 wordt voorgesteld het mandaat van ENISA, dat in 2004 is vastgesteld en in 2008 al eens met drie jaar is verlengd, met nog eens achttien maanden te verlengen. Dit om voldoende tijd te creëren om het debat ten aanzien van de wetgevingsprocedure rondom COM(2010) 521, waarin een hervorming van ENISA wordt voorgesteld, te kunnen voeren en te voorkomen dat ENISA in juridisch niemandsland terechtkomt.

De voorgestelde verordening COM(2010)521 heeft als doel ENISA te versterken en te moderniseren en een nieuw mandaat voor vijf jaar vast te stellen.

De belangrijkste voorgestelde veranderingen ten opzichte van de huidige ENISA-verordening uit 2004 zijn grotere flexibiliteit voor ENISA door bredere taakomschrijving, betere afstemming van ENISA met het beleid- en regelgevingproces van de EU en meer interactie in de strijd tegen *cybercrime* door de rechtshandhavingautoriteiten en de autoriteiten die privacy beschermen volwaardige *stakeholders* van ENISA te laten zijn. Bovendien wordt voorgesteld de bestuursstructuur te versterken en een geleidelijke toename van de middelen (qua financiën en mankracht) voor ENISA toe te staan.
Zo zal de focus van ENISA door de uitbreiding van ENISA's rol onder andere komen te liggen op het opbouwen en onderhouden van een samenwerkingsverband tussen *stakeholders* en kennisnetwerken en op het opzetten van een EU-kader voor het verzamelen van gegevens over netwerk- en informatiebeveiliging. Ook beoogt ENISA het centrum voor ondersteuning worden op het gebied van het voor beleidontwikkeling en het implementeren van beleid ten aanzien van netwerk- en informatiebeveiliging.

Impact assessment Commissie
De Commissie heeft ter onderbouwing van het voorstel een *impact assessment* uitgevoerd. Hierin wordt verwezen naar de uitkomsten van een evaluatie van ENISA in 2006/2007, twee publieke consultatierondes (2007 en 2008/2009), een door de Raad in 2009 aangenomen resolutie en de nieuwe Europese Digitale Agenda.

Het doel van de verordening is de EU, de lidstaten en de *stakeholders* de mogelijkheid te geven om een hoger niveau te ontwikkelen van het vermogen en de bereidheid om problemen in de netwerk- en informatiebeveiliging te voorkomen, te ontdekken en er beter op te reageren. Dit zorgt namelijk voor toenemend vertrouwen en betere beveiliging van de Europese digitale markt en het verbeteren van de concurrentiepositie van bedrijven in de EU.

Het blijkt dat de optie van uitbreiding van de huidige aan ENISA toebedeelde taken en toevoeging van rechtshandhavingautoriteiten en de autoriteiten die privacy beschermen als volwaardige *stakeholders* van ENISA, van alle onderzochte opties het meest (kosten)effectief bijdraagt aan de beleidsdoelstellingen. Op basis van deze uitkomst heeft de Commissie haar voorstellen geformuleerd.

4. Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel

a) *Bevoegdheid:* Er is sprake van een gedeelde bevoegdheid op basis van artikel 114 VWEU.

b) *Functionele toets:*
- *Subsidiariteit:* voor beide voorstellen positief.
- *Proportionaliteit:* voor beide voorstellen positief.
- *Onderbouwing:* beleid ten aanzien van netwerk- en informatiebeveiliging vraagt, zeker ook vanwege de bijna per definitie grensoverschrijdende dimensie ervan, een gezamenlijke aanpak van de EU-lidstaten, alsmede afstemming met andere regio's in de wereld. De doelen van het voorstel kunnen niet worden bereikt door de lidstaten afzonderlijk, aangezien de afhankelijkheid van de bestaande informatiesystemen verder gaat dan de landsgrenzen. Bovendien vergroot actie op Europees niveau de effectiviteit van het bestaande nationale beleid. Daarnaast heeft een gezamenlijk beleid op netwerk- en informatiebeveiligingsgebied met name een positieve invloed op het recht van bescherming van persoonsgegevens en persoonlijke levenssfeer. Nederland vindt daarom dat aanpak op Europees niveau gewenst is.
  Het voorstel gaat niet verder dan nodig om de doelen te behalen. De rol van ENISA wordt uitgebreid ten opzichte van haar huidige rol; dit is gericht op het verbeteren en moderniseren van ENISA, maar geeft ENISA nog steeds geen dwingend karakter. Zo

wordt voorgesteld dat er betere afstemming van ENISA komt met het EU-beleid en -regelgevingproces, waarbij instituties ENISA om advies en assistentie kunnen vragen. Verder is in het nieuwe regelgevende kader voor elektronische communicatie een ondersteunende en adviserende rol voor ENISA opgenomen. Dit laat echter ruimte voor eigen nationaal beleid en treedt niet in nationale bevoegdheden.

c) *Nederlands oordeel:* Nederland vindt dat een aanpak op Europees niveau gewenst is, omdat in veel gevallen de netwerk- en informatiebeveiligingsproblematiek grensoverschrijdend is. Nederland staat dan ook positief tegenover beide voorstellen: het verlengen van het mandaat van ENISA om de tijd te hebben een goed debat te voeren over een toekomstig versterkt en gemoderniseerd ENISA en het versterken en moderniseren van ENISA, waarbij onder andere meer samenwerking van ENISA met betrokken partijen op het gebied van bestrijding van cybercriminaliteit wordt voorgesteld.

5. Implicaties financieel

a) *Consequenties EU-begroting*
In de voorgestelde verordening wordt aangegeven dat er sprake zal zijn van een geleidelijke toename van de middelen (qua financiën en mankracht) voor ENISA. Het budget tot en met 2013 is echter vrijwel hetzelfde gebleven, binnen het huidige financiële kader. Het voorstel zegt echter niet om hoeveel beschikbare middelen het vanaf 2014 zal gaan, omdat niet op de onderhandelingen over de nieuwe EU-meerjarenbegroting (2014-2020) vooruit kan worden gelopen. Nederland zal kritisch kijken naar de voorstellen voor het toekomstig budget in het licht van het nieuwe mandaat voor ENISA.

b) *Financiële consequenties (incl. personele) voor rijksoverheid en/ of decentrale overheden*
Een exacte inschatting van de financiële gevolgen van dit voorstel kan op dit moment niet worden gemaakt. Verwachting is dat deze niet substantieel zullen zijn. Budgettaire gevolgen zullen worden ingepast op de begroting van het beleidsverantwoordelijke departement.

c) *Financiële consequenties (incl. personele) voor bedrijfsleven en burger*
Geen veranderingen ten opzichte van de eerdere verordening op dit gebied.

d) *Administratieve lasten voor rijksoverheid, decentrale overheden*
Geen veranderingen ten opzichte van de eerdere verordening op dit gebied.

e) *Administratieve lasten voor bedrijfsleven en burger*
Geen veranderingen ten opzichte van de eerdere verordening op dit gebied.

6. Implicaties juridisch

a) *Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid*
Niet van toepassing.

b) *Voorgestelde datum inwerkingtreding*
   a. Het huidige mandaat loopt af op 13 maart 2012. Voor deze datum zal de termijn moeten worden verlengd met maximaal 18 maanden, tot 13 september 2013
   b. Wanneer het huidige mandaat is verlengd, zal de nieuwe verordening voor 13 september 2013 van kracht moeten gaan. Dit is volgens Nederland een haalbare termijn.

c) *Wenselijkheid evaluatie-/horizonbepaling*
Op basis van deze voorstellen, zal binnen drie jaar na inwerkingtreding van de nieuwe verordening een evaluatie plaatsvinden die kijkt naar de *impact* en de effectiviteit van ENISA bij het behalen van haar doelen en naar de effectiviteit van de werkmethodes van ENISA.

7. Implicaties voor uitvoering en handhaving

a) *Uitvoerbaarheid*
Goed uitvoerbaar.

b) *Handhaafbaarheid*
Niet van toepassing.

8. Implicaties voor ontwikkelingslanden
Niet van toepassing.

9. Nederlandse positie (belangen en eerste algemene standpunt)

Nederland onderschrijft de relevantie van het verlengen van het mandaat van ENISA om de tijd te hebben een goed debat te voeren over een toekomstig versterkt en gemoderniseerd ENISA.

Nederland heeft ENISA de afgelopen jaren altijd gesteund. Het nationale beleid ten aanzien van netwerk- en informatiebeveiliging heeft zich ook altijd gericht op de EU, aangezien problemen op dit gebied vaak verder reiken dan de landsgrenzen. Nederland heeft dan ook waardering voor het voorstel waarin de rol van ENISA wordt versterkt en gemoderniseerd, omdat dit een gezamenlijk aanpak door EU-lidstaten van de problemen in de netwerk- en informatiebeveiliging zal bevorderen. Hierdoor zal de effectiviteit van de maatregelen toenemen, waarvan bedrijven die actief zijn op de EU-markt en de gezamenlijke interne markt als geheel zullen profiteren.

Nederland zal kritisch kijken naar de voorstellen voor het toekomstig budget voor ENISA in het licht van het nieuwe mandaat voor ENISA.

Nederland steunt de voorstellen voor meer samenwerking van ENISA, zowel binnen de EU-instituties als met de private sector, op het gebied van bestrijding van cybercriminaliteit, rekening houdend met de verschillende verantwoordelijkheden en bevoegdheden. Samenwerking tussen de betrokken partijen zal immers van toenemend belang worden om tot verbeteringen te komen, mede omdat de private sector in belangrijke mate eigenaar is van de elektronische netwerken en informatiesystemen. In de Europese Digitale Agenda is, naast het preventieve beleid, ook voorzien om tot een versterking van de bestrijding van cybercriminaliteit te komen onder andere door het opzetten van een samenwerkingsplatform binnen Europol.

Bekeken moet worden hoe een gemoderniseerd ENISA, dat als primair doel versterking van de veiligheid van elektronische netwerken en communicatiesystemen heeft, in deze samenwerking een rol kan vervullen.