Fiche 5: Mededeling bescherming van kritieke informatie-infrastructuur (CIIP)

1. Algemene gegevens

Titel voorstel

Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende de bescherming van kritieke informatie-infrastructuur 'Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid'

Datum Commissiedocument

31 maart 2011

Nr. Commissiedocument

COM(2011)163 definitief

Pre-lex

http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=nl&DosId=200304

Nr. impact assessment Commissie en Opinie Impact-assessment Board

Niet opgesteld

Behandelingstraject Raad

De mededeling zal worden besproken in de raadswerkgroep Telecommunicatie.
De VTE-Raad (Telecom) van 27 mei 2011 zal naar verwachting conclusies aannemen.

Eerstverantwoordelijk ministerie

Ministerie van Economische Zaken, Landbouw en Innovatie

2. Essentie voorstel

Deze mededeling geeft de voortgang aan die gemaakt is ten opzichte van de twee jaar eerder uitgebrachte eerste mededeling en actieplan over de bescherming van de vitale informatie-infrastructuur en de te nemen vervolgstappen. De mededeling beschrijft de ontwikkelingen langs de toen uitgezette lijnen van paraatheid en preventie, detectie en respons, migratie en herstel, internationale samenwerking en criteria voor Europese vitale infrastructuur in de ICT-sector. In de Digitale Agenda voor Europa van 2010 is het belang van de uitvoering van dat beleid al meegenomen als een belangrijk element om de veiligheid en veerkracht van ICT-infrastructuren te vergroten en beter te kunnen reageren op aanvallen en criminaliteit. Ook de onlangs voorgestelde versterking van het Europees Agentschap voor Netwerk- en informatiebeveiliging (ENISA) moet daar in versterkte mate aan gaan bijdragen. De activiteiten zijn over het algemeen volgens planning op de rails gezet en zullen verder worden uitgewerkt, waarbij gezien de ontwikkelingen in de bedreigingen sterker zal worden ingezet op mondiale samenwerking en het vergroten van de veiligheid van het internet.

3. Kondigt de Commissie acties, maatregelen of concrete wet- en regelgeving aan voor de toekomst? Zo ja, hoe luidt dan het voorlopige Nederlandse oordeel

over bevoegdheidsvaststelling, subsidiariteit en proportionaliteit en hoe schat Nederland de financiële gevolgen in?

De Commissie kondigt geen wettelijke maatregelen aan maar zet vooral in op voortzetting van de samenwerking in de EU, ingebed in een strategie van mondiale coördinatie, waarbij aansluiting wordt gezocht bij de direct betrokken partijen in zowel individuele landen als internationale organisaties. Overleg met de lidstaten en publiek-private samenwerking blijven daarin belangrijke uitgangpunten.

De belangrijkste beoogde resultaten en vervolgstappen zijn:
- Het Europees forum voor lidstaten (EFMS) en het Europees publiek-privaat partnerschap voor weerbaarheid (E3PR) zijn van de grond gekomen.
- Bij het tot stand komen van mechanismes en structuren voor waarschuwen en delen van informatie zoals Computer Emergence Response Teams (CERT's) is veel vooruitgang geboekt, zoals een minimumset van basiscapaciteiten en diensten en bijbehorende beleidsaanbevelingen.
- Beleidsaanbevelingen voor oefenbeleid alsmede een eerste pan-Europese oefening voor grootschalige incidenten van netwerkbeveiliging heeft plaatsgevonden en vervolgoefeningen zijn voorzien.
- Europese beginselen en richtsnoeren voor de weerbaarheid en de stabiliteit van het internet zijn verder ontwikkeld en worden ingebracht in internationaal overleg.
- Een eerste ontwerp van ICT-sectorspecifieke criteria voor de identificatie van Europese vitale infrastructuren, met speciale aandacht voor vaste en mobiele communicatie en het internet, is tot stand gekomen en worden verder ontwikkeld.
- Voortgaande dan wel enigszins versterkte inspanningen worden aangekondigd bij het opbouwen van strategische internationale partnerschappen (zoals het eind vorig jaar bij de top van Lissabon overeengekomen overleg van de EU met de VS), het ontwikkelen van vertrouwen in *cloud computing*, het verder tot stand komen van een netwerk van CERT's en een mede daarop te ontwikkelen Europees systeem voor informatiedeling en alarmering (EISAS, uitwerking ENISA-onderzoek van 2007), opzetten van nationale en Europese noodplanning (nieuw element), overeenkomstige oefeningen (een oefening heeft eind vorig jaar plaatsgevonden) en het verder stimuleren van het vergroten van de weerbaarheid en stabiliteit van het internet. Dit zal voornamelijk binnen al ontwikkelde structuren plaatsvinden. Bij de versterking van ENISA is hier ook rekening mee gehouden.

Bevoegdheidsvaststelling

De Europese Unie deelt de bevoegdheid op het gebied van de elektronische communicatiesector (telecommunicatie/ICT) met de lidstaten. De EU is op basis van onder meer artikel 114 VWEU bevoegd het regelgevend kader voor deze sector vast te stellen.

Subsidiariteit

De subsidiariteit wordt positief beoordeeld. Telecommunicatie/ICT-diensten met in het bijzonder het internet zijn van nature grensoverschrijdend. Het verbeteren van de veiligheid kan niet alleen nationaal worden aangepakt, maar vraagt om een voortgezette Europese samenwerking. De meerwaarde van gemeenschappelijke samenwerking wordt mede gekregen door het kunnen delen van nieuwe inzichten en ook het meetrekken van achterblijvende landen om het voorgestane beleid tot ontwikkeling te brengen. Dreigingen komen immers

vaak van buiten onze landsgrenzen. Van belang is verder dat nationale verantwoordelijkheden in relevant (mondiaal) overleg en t.a.v. operationele zaken behouden blijven.

Proportionaliteit
Het betreft een voortzetting en versterking van reeds in gang gezette beleidsactiviteiten. Op basis van deze mededeling kan nog geen proportionaliteitsoordeel worden gegeven. Bij de totstandkoming van de verschillende eindresultaten zal gelet moeten worden op de proportionaliteit van beoogde maatregelen of voorzieningen.

Financiële gevolgen
Er zijn geen directe financiële gevolgen op basis van deze mededeling voorzien. De inspanningen zijn in lijn met de Nederlandse beleidsontwikkelingen op dit terrein. De uitwerking van de mededeling zal dit in de loop van de tijd moeten aangeven, waarbij lidstaten een vrijheid behouden in de mate waarin zij aan het voorgestane gemeenschappelijk beleid kunnen bijdragen. Eventuele budgettaire gevolgen worden ingepast conform de betreffende begrotingsregels.

4. Nederlandse positie over de mededeling

Nederland verwelkomt de mededeling omdat deze een voortgaande invulling geeft aan het samenwerken in het verder verbeteren van de bescherming van de vitale informatie-infrastructuren. Dat is nodig om het vertrouwen in het gebruik ervan te vergroten en de potentiële groei van de digitale markt en daarmee de economie een extra impuls te geven. De verschillende activiteiten lopen goed samen met de nationale inspanningen en zijn ook in lijn met het beleid van de Nationale Cyber Security Strategie en de binnenkort uit te brengen Digitale Agenda.nl.

Het verder met de lidstaten bespreken van de ICT-sectorspecifieke criteria is van belang bij de herziening in 2012 van de richtlijn inzake de identificatie van Europese vitale infrastructuren en de beoordeling van de noodzaak om dergelijke infrastructuren beter te beschermen.

Bij de uitwerking van de activiteiten moet wel rekening worden gehouden met de bestaande verschillen in aanpak bij de lidstaten. Hoewel Nederland prima presteert in de Europese aanpak, moet voldoende ruimte blijven voor oplossingen die ook in de nationale context van beleidsontwikkelingen, beschikbare middelen en uitvoering mogelijk zijn. Dit is o.a. van betekenis bij de verdergaande ontwikkeling en invulling van CERT's en van een EISAS.

Naast de gevraagde opzet van nationale noodplannen voor cyberincidenten door lidstaten is het van belang dat ook de aanbieders van de informatie-infrastructuur dit onderdeel laten zijn van hun continuïteitsplanning in het algemeen. Het in het vervolg daarvan voorgestelde Europese rampenplan zal qua rol en inhoud door de Commissie nader moeten worden gemotiveerd. Indien daartoe zou worden besloten moet het in de visie van Nederland in overeenstemming met de lidstaten en alleen indien nodig in aanvulling op bestaande afspraken tussen de lidstaten tot stand komen.

Het is belangrijk dat de private partijen zoals nu verenigd in het E3PR een sterker *commitment* ontwikkelen in de discussie over het verbeteren van de veiligheid en weerbaarheid van

hun informatie-infrastructuren. Zij zijn tenslotte veelal de eigenaren van de betreffende infrastructuur. Daarnaast is het belangrijk dat er meer nadruk wordt gelegd bij de industrie op het ontwikkelen van betrouwbare producten (hardware en software) om ook daarmee een bijdrage te leveren aan het tostand komen van een veiliger en betrouwbaardere informatie-infrastructuur.

Ten slotte zal Nederland blijven inzetten op versterkte internationale samenwerking op dit terrein o.a. in het overleg dat de EU met de VS is overeengekomen rond cyberveiligheid en cybercriminaliteit alsmede in ICANN/GAC verband inzake de weerbaarheid van het internet.