COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 30.3.2009
COM(2009) 149 definitief

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

"Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht"

{SEC(2009) 399}
{SEC(2009) 400}

(door de Commissie ingediend)

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

"Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht"

1. INLEIDING

Informatie- en communicatietechnologieën (ICT's) zijn steeds meer met onze dagelijkse activiteiten vervlochten. Sommige van deze ICT-systemen, -diensten, -netwerken en –infrastructuren (kortom, ICT-infrastructuren) vormen een vitaal onderdeel van de Europese economie en maatschappij: ze verschaffen essentiële goederen en diensten of vormen het ondersteunende platform van andere kritieke infrastructuren. Zij worden doorgaans als kritieke informatie-infrastructuren (KII's)[1] beschouwd, omdat de verstoring of vernietiging ervan een ernstige impact op vitale maatschappelijke functies zou hebben. Recente voorbeelden daarvan zijn onder meer de grootschalige cyberaanvallen tegen Estland in 2007 en de breuken van transcontinentale kabels in 2008.

Het Economisch Wereldforum schatte in 2008 de kans op een grote KII-verstoring, die de mondiale economie zo'n 250 miljard Amerikaanse dollar kan kosten, in de volgende 10 jaar op 10 à 20%[2].

De onderhavige mededeling spitst zich toe op preventie, paraatheid en bewustmaking en schetst een plan voor onmiddellijke acties om de beveiliging en veerkracht van KII's te verbeteren. Een en ander sluit aan bij de discussie die op verzoek van de Raad en het Europees Parlement is begonnen om een antwoord te bieden op de uitdagingen en prioriteiten voor een beleid inzake netwerk- en informatiebeveiliging (NIB) en de geschiktste instrumenten op EU-niveau voor de aanpak daarvan. De voorgestelde acties vullen ook de acties aan om criminele en terroristische activiteiten tegen KII's te voorkomen, te bestrijden en te vervolgen en zorgen in combinatie met lopende en toekomstige EU-onderzoeksinspanningen op het gebied van netwerk- en informatiebeveiliging alsmede met internationale initiatieven op dit gebied voor synergie.

2. DE BELEIDSCONTEXT

De onderhavige mededeling ontwikkelt het Europese beleid om de beveiliging van en het vertrouwen in de informatiemaatschappij te bevorderen. In 2005 al heeft de Commissie[3] gewezen op de dringende noodzaak van coördinering van de inspanningen om bij de stakeholders vertrouwen te wekken in elektronische communicatie en diensten. Daartoe is in

---

1 Een definitie van KII's werd voorgesteld in COM(2005) 576 definitief.
2 Global Risks 2008.
3 COM(2005) 229.

2006 een strategie voor een veilige informatiemaatschappij[4] aangenomen. De hoofdelementen daarvan, inclusief beveiliging en veerkracht van ICT-infrastructuren, zijn bevestigd in Resolutie 2007/068/01 van de Raad. De stakeholders blijken deze echter onvoldoende te hebben overgenomen en uitgevoerd. Deze strategie versterkt ook de rol, op tactisch en operationeel niveau, van het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA), dat in 2004 is opgericht om bij te dragen tot de realisering van de doelstellingen die erin bestaan een hoog en effectief niveau van NIB binnen de Gemeenschap te verzekeren en een NIB-cultuur te ontwikkelen ten behoeve van de burgers, consumenten, ondernemingen en overheidsdiensten van de EU.

In 2008 is het mandaat van het ENISA ongewijzigd verlengd tot maart 2012[5]. Tegelijk hebben de Raad en het Europees Parlement opgeroepen tot verdere discussie over de toekomst van het ENISA en over de algemene koers van het Europese streven naar een betere netwerk- en informatiebeveiliging. Om dit debat te ondersteunen, is de Commissie afgelopen november een publieke onlineraadpleging begonnen[6] waarvan de analyse binnenkort beschikbaar wordt gesteld.

De in de onderhavige mededeling beoogde activiteiten zullen worden uitgevoerd in het kader van en parallel aan het Europees programma voor de bescherming van kritieke infrastructuur (EPCIP)[7]. Een essentieel element van het EPCIP is de Richtlijn[8] inzake de identificatie van en aanmerking als Europese kritieke infrastructuren[9], die de ICT-sector als een voor de toekomst prioritaire sector aanwijst. Een ander belangrijk onderdeel van het EPCIP is het Netwerk voor alarmering en informatie inzake kritieke infrastructuur (CIWIN)[10].

Wat de regelgeving betreft, bevat het voorstel van de Commissie tot wijziging van het regelgevingskader voor elektronische-communicatienetwerken en –diensten[11] nieuwe bepalingen over beveiliging en integriteit, met name om de verplichtingen van de exploitanten aan te scherpen ten aanzien van het nemen van passende maatregelen om vastgestelde risico's aan te pakken, het waarborgen van de continuïteit van de dienstverlening en het melden van beveiligingslekken[12]. Deze aanpak is bevorderlijk voor de verwezenlijking van de doelstelling om de beveiliging en de veerkracht van KII's te verbeteren. Er bestaat in het Europees Parlement en de Raad een breed draagvlak voor deze bepalingen.

De in de onderhavige mededeling voorgestelde acties completeren bestaande en toekomstige maatregelen op het gebied van politiële en justitiële samenwerking om criminele en terroristische activiteiten tegen ICT-infrastructuren te voorkomen, te bestrijden en te vervolgen zoals onder meer vastgesteld bij het Kaderbesluit van de Raad betreffende aanvallen op informatiesystemen[13] en de geplande actualisering ervan[14].

---

4 COM(2006) 251.
5 Verordening (EG) nr. 1007/2008.
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 COM(2006) 786 definitief.
8 2008/114/EG.
9 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/nl/gena/105456.pdf
10 COM(2008) 676 definitief.
11 COM (2007) 697, COM (2007) 698, COM (2007) 699.
12 Art. 13 Kaderrichtlijn.
13 2005/222/JBZ.
14 COM(2008) 712.

Dit initiatief houdt rekening met NAVO-activiteiten betreffende gemeenschappelijk beleid inzake cyberverdediging, d.w.z. in verband met de Cyber Defence Management Authority en het Cooperative Cyber Defence Centre of Excellence.

Ten slotte wordt ten volle rekening gehouden met internationale beleidsontwikkelingen, met name de G8-beginselen betreffende de bescherming van kritieke informatie-infrastructuren[15], Resolutie 58/199 van de Algemene Vergadering van de VN *Creation of a global culture of cybersecurity and the protection of critical information infrastructures* en de recente aanbeveling betreffende de bescherming van kritieke informatie-infrastructuren van de OESO.

3. WAT STAAT OP HET SPEL

3.1. Kritieke informatie-infrastructuren zijn van vitaal belang voor de economie en de maatschappelijke groei van de EU

De economische en maatschappelijke rol van de ICT-sector en ICT-infrastructuren wordt op de voorgrond gesteld in recente rapporten betreffende innovatie en economische groei, onder meer de Mededeling betreffende de middenevaluatie van i2010[16], het rapport van de Aho Group[17] en de jaarlijkse economische rapporten van de Europese Unie[18]. De OESO onderstreept het belang van ICT's en het internet "to boost economic performance and social well-being, and to strengthen societies' capacity to improve the quality of life for citizens worldwide"[19] De OESO beveelt voorts beleid aan dat het vertrouwen in de internetinfrastructuur verhoogt.

De ICT-sector is van vitaal belang voor alle geledingen van de maatschappij. De ondernemingen steunen op de ICT-sector zowel op het gebied van directe verkoop als wat de efficiency van de interne procedures betreft. ICT's zijn een kritieke component van innovatie en zijn goed voor bijna 40% van de productiviteitsgroei[20]. Ook bij overheden en overheidsdiensten zijn ICT's alomtegenwoordig: in verband met de acceptatie van e-overheidsdiensten op alle niveaus alsook nieuwe toepassingen zoals innovatieve oplossingen met betrekking tot gezondheid, energie en beleidsparticipatie is de overheidssector sterk afhankelijk van ICT's. Ten slotte, niet het minst, steunen burgers bij hun dagelijkse activiteiten steeds meer op en maken zij steeds meer gebruik van ICT's: het verhogen van de KII-beveiliging zou, vooral dankzij een betere bescherming van de persoonsgegevens en privacy, het vertrouwen van de burgers in ICT's doen toenemen.

3.2. De risicoblootstelling van kritieke informatie-infrastructuren

De met menselijke aanvallen, natuurrampen of technische storingen verband houdende risico's worden vaak niet volledig begrepen en/of voldoende geanalyseerd. De stakeholders zijn dan ook onvoldoende van de risico's doordrongen om effectieve beveiligings- en tegenmaatregelen te gaan ontwikkelen.

---

15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf

16 COM(2008) 199 definitief.

17 http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm

18 EU Economy 2007 Review Review http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf

19 http://www.oecd.org/dataoecd/1/29/40821707.pdf

20 http://epp.eurostat.ec.europa.eu/ - Science and Technology/Information Society.

Cyberaanvallen hebben een ongekend niveau van complexiteit bereikt. Eenvoudige experimenten zijn aan het uitgroeien tot complexe activiteiten met winstoogmerk of politieke motieven. De recente grootschalige cyberaanvallen tegen Estland, Litouwen en Georgië zijn de bekendste voorbeelden van een algemene trend. Uit het enorme aantal virussen, wormen en andere vormen van kwaadaardige software, de uitbreiding van botnets en de continue groei van spam blijkt de ernst van het probleem[21].

De grote afhankelijkheid van KII's, hun grensoverschrijdende koppeling met andere infrastructuren, de onderlinge afhankelijkheid tussen KII's en andere infrastructuren alsook hun kwetsbaarheid en blootstelling aan bedreigingen vereisen dat hun beveiliging en veerkracht systemisch als frontlijnverdediging tegen storingen en aanvallen worden aangepakt.

3.3. Beveiliging en veerkracht van kritieke informatie-infrastructuren om het vertrouwen in de informatiemaatschappij te stimuleren

Om ervoor te zorgen dat ICT-infrastructuren maximaal worden benut en zo de economische en sociale kansen van de informatiemaatschappij ten volle te realiseren, moeten alle stakeholders er een groot vertrouwen in hebben. Een en ander hangt af van verschillende elementen, waarvan het belangrijkste de zorg voor een hoog niveau van beveiliging en veerkracht van die infrastructuren is. Diversiteit, openheid, interoperabiliteit, bruikbaarheid, transparantie, aanspreekbaarheid, auditeerbaarheid van de verschillende componenten en concurrentie zijn belangrijke aanjagers voor het ontwikkelen van de beveiliging, en stimuleren een beroep op producten, processen en diensten die de beveiliging bevorderen. Zoals de Commissie al heeft benadrukt[22], is dit een gedeelde verantwoordelijkheid: geen enkele individuele stakeholder heeft de middelen om voor de beveiliging en veerkracht van alle ICT-infrastructuren te zorgen en alle desbetreffende verantwoordelijkheden te dragen.

Het opnemen van dergelijke verantwoordelijkheden vereist een aanpak en cultuur van risicobeheer waarmee op bekende bedreigingen kan worden gereageerd en op onbekende toekomstige bedreigingen kan worden geanticipeerd, zonder te overreageren en de opkomst van innovatieve diensten en toepassingen te onderdrukken.

3.4. De uitdagingen voor Europa

Bovendien dient, complementair aan alle activiteiten in verband met de tenuitvoerlegging van de Richtlijn inzake de identificatie van en aanmerking als Europese kritieke infrastructuren – met name de identificatie van voor de ICT-sector specifieke criteria – een aantal bredere uitdagingen te worden aangepakt om de beveiliging en veerkracht van KII's te verbeteren.

3.4.1. Ongelijke en ongecoördineerde nationale benaderingen

Hoewel de uitdagingen en problemen die op ons afkomen gemeenschappelijke kenmerken vertonen, verschillende de maatregelen en regelingen met het oog op de beveiliging en veerkracht van KII's alsook het niveau van expertise en paraatheid per lidstaat.

Bij een louter nationale aanpak bestaat de kans dat in Europa fragmentering en inefficiëntie ontstaan. Verschillen in nationale benaderingen en het gebrek aan systematische

---

21 COM(2006) 688 definitief.

22 COM(2006) 251 definitief.

grensoverschrijdende samenwerking verminderen de effectiviteit van nationale tegenmaatregelen sterk, onder meer doordat wegens de onderlinge koppeling van KII's een laag niveau van beveiliging en veerkracht van KII's in één land de kwetsbaarheid van en risico's in ander landen kan vergroten.

Om deze situatie te verhelpen, is een Europese inspanning nodig om voor nationale beleidslijnen en programma's toegevoegde waarde te creëren door het bewustzijn van en gemeenschappelijk inzicht in uitdagingen te bevorderen, de goedkeuring van gedeelde beleidsdoelstellingen en –prioriteiten te stimuleren, de samenwerking tussen de lidstaten op te voeren en nationaal beleid in een Europeser en mondialer kader in te passen.

3.4.2. Noodzaak van een nieuw Europees beheersmodel voor KII's

Het bevorderen van de beveiliging en veerkracht van KII's vormt een bijzondere beheersuitdaging. Hoewel in laatste instantie de lidstaten voor het vaststellen van KII-gerelateerd beleid verantwoordelijk blijven, hangt de uitvoering ervan af van het hierbij betrekken van de marktsector, die een groot aantal KII's bezit of controleert. Anderzijds verschaffen markten niet steeds voldoende stimulansen voor de marktsector om in de bescherming van KII's te investeren op het doorgaans door overheden verlangde niveau.

Om dit beheersprobleem aan te pakken, zijn op nationaal niveau publiek-private partnerschappen (PPP's) ontstaan als referentiemodel. Ondanks de consensus dat PPP's ook op Europees niveau wenselijk zijn, zijn Europese PPP's nog geen werkelijkheid geworden. Een Europawijd multistakeholders-bestuursmodel, dat een grotere rol van het ENISA kan inhouden, zou de deelname van de marktsector bij de vaststelling van strategische overheidsbeleidsdoelstellingen alsook operationele prioriteiten en maatregelen kunnen bevorderen. Dit kader kan de kloof tussen nationale beleidsvorming en operationele realiteit op het terrein overbruggen.

3.4.3. Beperkte Europese capaciteit voor vroegtijdige waarschuwing en incidentenrespons

Beheersmechanismen zijn alleen echt doeltreffend indien alle deelnemers naar betrouwbare informatie kunnen handelen. Dit is in het bijzonder relevant voor overheden die in laatste instantie verantwoordelijk zijn voor de beveiliging en het welzijn van de burgers.

De procedures en praktijken voor het monitoren en rapporteren van incidenten op het gebied van netwerkbeveiliging verschillen echter sterk per lidstaat. Sommige lidstaten hebben geen referentieorganisatie als monitoringpunt. Belangrijker is dat de samenwerking en informatiedeling tussen lidstaten van betrouwbare gegevens over beveiligingsincidenten waarnaar men kan handelen onvoldoende ontwikkeld lijken en een informeel karakter hebben of beperkt zijn tot bilaterale of beperkt multilaterale uitwisselingen. Bovendien is het simuleren van incidenten en houden van oefeningen om de responscapaciteiten te testen van strategisch belang voor de verbetering van de beveiliging en veerkracht van KII's; hierbij moeten met name flexibele strategieën en procedures voor het omgaan met de onvoorspelbaarheid van potentiële crises centraal staan. In de EU bevinden cyberbeveiligingsoefeningen zich nog in een embryonaal stadium. Grensoverschrijdende oefeningen komen in zeer beperkte mate voor. Zoals uit recente gebeurtenissen is gebleken[23],

[23] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

is wederzijdse hulp een essentieel element van een passende respons op grootschalige bedreigingen van en aanvallen op KII's.

Krachtige Europese capaciteit voor vroegtijdige waarschuwing en incidentenrespons moet steunen op goed functionerende nationale of overheids-CERT's (responsteams voor computernoodgevallen), d.w.z. teams met een gemeenschappelijk basisniveau wat capaciteiten betreft. Deze instanties dienen te fungeren als nationale katalysator van de stakeholdersbelangen en capaciteit voor activiteiten inzake overheidsbeleid (inclusief activiteiten die betrekking hebben op informatie- en alarmdelende systemen die burgers en KMO's beogen) en dienen effectieve grensoverschrijdende activiteiten voor samenwerking en informatie-uitwisseling aan te vatten, die mogelijk als hefboom werken voor de activiteiten van bestaande organisaties zoals de European Governmental CERTs Group (EGC)[24].

3.4.4. Internationale samenwerking

De opkomst van het internet als een essentiële KII vereist dat aan de veerkracht en stabiliteit ervan bijzondere aandacht wordt besteed. Het internet heeft dankzij zijn gedistribueerde, redundante opzet bewezen een zeer robuuste infrastructuur te zijn. Zijn fenomenale groei heeft tot toenemende fysieke en logische complexiteit en de opkomst van nieuwe diensten en toepassingen geleid: het is geoorloofd een vraagteken te plaatsen bij de capaciteit van het internet om het stijgende aantal verstoringen en cyberaanvallen te weerstaan.

Het feit dat de meningen over het kritieke karakter van de elementen waaruit het internet bestaat verschillen, verklaart voor een deel de diversiteit van regeringsstandpunten die op internationale fora worden vertolkt en de vaak tegenstrijdige perceptie van het belang van deze kwestie. Dit zou een passende preventie van, paraatheid voor en capaciteit om te herstellen van dreigingen die het internet treffen, kunnen belemmeren. Zo zouden de gevolgen van de overgang van IPv4 naar IPv6 ook op het punt van KII-beveiliging moeten worden aangepakt.

Het internet is een mondiaal, hooggedistribueerde aaneenschakeling van netwerken, met controlecentra die niet noodzakelijk nationale grenzen volgen. Dit vereist een specifieke, gerichte aanpak op basis van twee convergerende maatregelen om de veerkracht en stabiliteit ervan te verzekeren. In de eerste plaats dient gestreefd te worden naar consensus over de Europese prioriteiten voor de veerkracht en stabiliteit van het internet op het stuk van overheidsbeleid en operationele inzet. In de tweede plaats dient de mondiale gemeenschap, in het kader van onze strategische dialoog en samenwerking met derde landen en internationale organisaties, ervan te worden overtuigd een aantal uitgangspunten te ontwikkelen die de Europese kernwaarden voor internetveerkracht en –stabiliteit weergeven. Deze activiteiten zouden voortbouwen op de erkenning door de Wereldtop over de informatiemaatschappij[25] van het fundamentele belang van een stabiel internet.

4. DE WEG VOORUIT: NAAR MEER EU-COÖRDINATIE EN -SAMENWERKING

Vanwege de communautaire en internationale dimensie van het probleem zou een geïntegreerde EU-benadering om de beveiliging en de veerkracht van KII's te verbeteren een

[24] http://www.egc-group.org/

[25] De agenda van Tunis voor de informatiemaatschappij, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

aanvulling zijn op en waarde toevoegen aan nationale programma's alsook aan de bestaande regelingen voor bilaterale en multilaterale samenwerking tussen de lidstaten.

Tijdens publieke beleidsdiscussies na de gebeurtenissen in Estland is geopperd dat de effecten van dergelijke aanvallen kunnen worden beperkt door preventieve maatregelen en gecoördineerde actie in de loop van de crisis. Een meer gestructureerde uitwisseling van informatie en goede praktijken over heel de EU zou de bestrijding van grensoverschrijdende bedreigingen aanzienlijk kunnen vergemakkelijken.

Het is nodig de bestaande instrumenten voor samenwerking, inclusief het ENISA, te versterken en zo nodig nieuwe instrumenten te creëren. Een aanpak, met verschillende stakeholders en op verschillende niveaus, op Europese schaal, waarbij de nationale verantwoordelijkheden worden gerespecteerd en aangevuld, is van essentieel belang.

Een grondig begrip van de omgeving en de beperkingen is nodig. Zo is het gedistribueerde karakter van het internet, waar randknooppunten gebruikt kunnen worden als aanvalsvector, bv. botnets, een zorg. Dit gedistribueerde karakter is echter een essentiële component van stabiliteit en veerkracht en kan bijdragen tot een sneller herstel dan normaal het geval zou zijn met overgeformaliseerde top-down procedures. Een en ander vereist een voorzichtige analyse per geval van het te voeren overheidsbeleid en de in te stellen operationele procedures.

Ook de tijdhorizon is belangrijk. Het is duidelijk dat nu gehandeld dient te worden en onverwijld de basis dient te worden gelegd voor het creëren van een kader dat ons in staat zal stellen op de actuele uitdagingen te reageren en een plaats zal krijgen in de toekomstige strategie voor netwerk- en informatiebeveiliging.

Er worden vijf pijlers voorgesteld als basis om deze uitdagingen aan te gaan:

(1) paraatheid en preventie: paraatheid op alle niveaus verzekeren;

(2) detectie en respons: voorzien in mechanismen voor vroegtijdige waarschuwing;

(3) mitigatie en herstel: versterken van EU-verdedigingsmechanismen voor KII's;

(4) internationale samenwerking: internationaal bevorderen van EU-prioriteiten;

(5) criteria voor de ICT-sector: ondersteunen van de tenuitvoerlegging van de Richtlijn inzake de identificatie van en aanmerking als Europese kritieke infrastructuren[26].

5. HET ACTIEPLAN

5.1. Paraatheid en preventie:

Basisniveau van capaciteiten en diensten voor pan-Europese samenwerking. De Commissie verzoekt de lidstaten en betrokken stakeholders om

[26] Richtlijn 2008/114/EG van de Raad.

- met ondersteuning van het ENISA een minimumniveau van capaciteiten en diensten voor nationale/overheids-CERT's en activiteiten voor incidentenrespons ter ondersteuning van pan-Europese samenwerking vast te stellen;

- ervoor te zorgen dat nationale/overheids-CERT's fungeren als essentiële component van de nationale capaciteit voor paraatheid, informatiedeling, coördinatie en respons.

Doelstelling: eind 2010 minimumnormen overeenkomen; eind 2011 in alle lidstaten goed functionerende nationale/overheids-CERT's oprichten.

Europees publiek-privaat partnerschap voor veerkracht (EP3R). De Commissie bevordert

- samenwerking tussen de overheids- en de marktsector betreffende beveiligings- en veerkrachtdoelstellingen, basisniveau-eisen en goede beleidspraktijken en –maatregelen. Het EP3R dient de Europese dimensie vanuit strategisch (bv. goede beleidspraktijken) en taktisch/operationeel (bv. industriële inzet) perspectief centraal te stellen. Het EP3R moet op bestaande nationale initiatieven en de operationele activiteiten van het ENISA voortbouwen en deze aanvullen.

Doelstelling: eind 2009 met een wegenkaart en plan voor het EP3R komen; medio 2010 het EP3R oprichten; eind 2010 dient het EP3R met eerste resultaten te komen.

Europees Forum voor informatiedeling tussen lidstaten De Commissie richt

- een Europees Forum op voor de lidstaten om informatie en goede beleidspraktijken inzake beveiliging en veerkracht van KII's te delen. Dit zou mee profiteren van de resultaten van de activiteiten van andere organisaties, in het bijzonder het ENISA.

Doelstelling: eind 2009 het forum opstarten; eind 2010 met de eerste resultaten komen.

5.2. Detectie en respons

Europees informatiedelings- en alarmeringssysteem (EISAS) De Commissie ondersteunt

het ontwikkelen en opzetten van EISAS, dat burgers en KMO's beoogt en gebaseerd is op informatie- en alarmdelingssystemen van de overheids- en de marktsector. De Commissie verleent financiële steun aan twee aanvullende projecten voor prototypebouw[27]. Er wordt op het ENISA een beroep gedaan om de resultaten van deze projecten en andere nationale initiatieven te inventariseren en met een wegenkaart te komen om de ontwikkeling en opzet van EISAS te bevorderen.

Doelstelling: eind 2010 de projecten voor prototypebouw voltooien; eind 2010 met een wegenkaart voor een Europees systeem komen;

[27] In het kader van het EG-programma "*Terrorisme en andere aan veiligheid gerelateerde risico's: preventie, paraatheid en beheersing van de gevolgen*", http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

5.3. Mitigatie en herstel

Nationale rampenplanning en alarmoefeningen. De Commissie verzoekt de lidstaten

- als een stap in de richting van pan-Europese coördinatie, nationale rampenplannen te ontwikkelen en regelmatig oefeningen te houden voor respons in verband met grootschalige beveiligingsincidenten op netwerken en noodherstel. Nationale/overheids-CERT's/CSIRT's kunnen belast worden met de leiding van nationale rampenplanningsoefeningen en –tests waarbij stakeholders uit de markt- en overheidssector betrokken zijn. Het ENISA wordt verzocht deel te nemen om de uitwisseling van goede praktijken tussen de lidstaten te ondersteunen.

Doelstelling: eind 2010 ten minste één nationale oefening in elke lidstaat houden.

Pan-Europese oefeningen in verband met grootschalige netwerkbeveiligingsincidenten. De Commissie verleent

- financiële ondersteuning voor de ontwikkeling van pan-Europese oefeningen in verband met internetbeveiligingincidenten[28] die ook het operationele platform kunnen vormen voor pan-Europese deelname aan oefeningen in verband met internationale netwerkbeveiligingsincidenten, zoals het Amerikaanse Cyber Storm.

Doelstelling: eind 2010 de eerste pan-Europese oefening ontwerpen en houden; eind 2010 aan pan-Europese internationale oefeningen deelnemen.

Verhoogde samenwerking tussen nationale/overheids-CERT's. De Commissie verzoekt de lidstaten

- de samenwerking tussen nationale/overheids-CERT's op te voeren, ook door bestaande samenwerkingsmechanismen zoals de EGC als hefboom te gebruiken en uit te breiden[29]. Er wordt een beroep gedaan op het ENISA om actief de pan-Europese samenwerking tussen nationale/overheids-CERT's te stimuleren en te ondersteunen hetgeen zou moeten leiden tot verhoogde paraatheid, verhoogde Europese capaciteit voor reactie en respons op incidenten en de organisatie van pan-Europese (en/of regionale) oefeningen.

Doelstelling: eind 2010 het aantal nationale instanties dat aan de EGC deelneemt verdubbelen; ontwikkeling door het ENISA tegen eind 2010 van referentiematerialen om pan-Europese samenwerking te ondersteunen.

5.4. Internationale samenwerking

Veerkracht en stabiliteit van het internet. Er worden drie aanvullende activiteiten gepland

- Europese prioriteiten betreffende veerkracht en stabiliteit van het internet op lange termijn. De Commissie organiseert een Europawijde discussie met alle relevante publieke en private stakeholders om prioriteiten betreffende veerkracht en stabiliteit van het internet op lange termijn vast te stellen.

[28] Zie voetnoot 27.
[29] Zie voetnoot 24.

Doelstelling: eind 2010 met prioriteiten betreffende kritieke internetcomponenten en -vraagstukken komen.

- Beginselen en richtsnoeren voor veerkracht en stabiliteit van het internet (Europees niveau). De Commissie stelt samen met de lidstaten richtsnoeren voor veerkracht en stabiliteit van het internet vast die toegespitst zijn op regionale remediërende acties, overeenkomsten voor wederzijdse bijstand, gecoördineerde strategieën voor herstel en continuïteit, geografische spreiding van kritieke internethulpbronnen, technologische beveiligingsmaatregelen in de internetarchitectuur en –protocollen, reproductie en diversiteit van diensten en gegevens. De Commissie financiert nu reeds een taskforce voor DNS-veerkracht die samen met andere relevante projecten zal bijdragen tot de consensusvorming[30].

Doelstelling: eind 2009 met een Europese wegenkaart betreffende beginselen en richtsnoeren voor internetveerkracht en- stabiliteit komen; eind 2010 overeenstemming bereiken over het eerste concept voor dergelijke beginselen en richtsnoeren;

- Beginselen en richtsnoeren betreffende internetveerkracht en -stabiliteit (mondiaal niveau). De Commissie werkt samen met de lidstaten aan een wegenkaart om beginselen en richtsnoeren op mondiaal niveau te bevorderen. Er wordt, met name in het kader van dialogen over de informatiemaatschappij, strategische samenwerking met derde landen ontwikkeld als middel om tot consensusvorming te komen[31].

Doelstelling: begin 2010 met een wegenkaart voor internationale samenwerking betreffende beginselen en richtsnoeren voor beveiliging en veerkracht komen; eind 2010 het eerste concept voor internationaal erkende beginselen en richtsnoeren met derde landen en in relevante fora, inclusief het Forum voor internetbeheer, bespreken.

Mondiale oefeningen inzake herstel en mitigatie van grootschalige internetincidenten. De Commissie verzoekt de Europese stakeholders om

- na te denken over een praktische manier om, voortbouwend op regionale rampenplannen en –capaciteiten, de in het kader van de mitigatie- en herstelpijler gehouden oefeningen tot het mondiale niveau uit te breiden.

Doelstelling: eind 2010 dient de Commissie een kader en een wegenkaart voor te stellen ter ondersteuning van de Europese betrokkenheid bij en deelname aan mondiale oefeningen inzake herstel en mitigatie van grootschalige internetincidenten.

5.5. Criteria voor Europese kritieke infrastructuur in de ICT-sector

Voor de ICT-sector specifieke criteria. Door op het in 2008 uitgevoerde eerste initiatief voort te bouwen ontwikkelt de Commissie

- in samenwerking met de lidstaten en alle relevante stakeholders verder de criteria voor het aanwijzen van Europese kritieke infrastructuren voor de ICT-sector. Daartoe wordt relevante informatie ontleend aan een specifieke studie waartoe het initiatief is genomen[32].

30 Zie voetnoot 27.
31 COM(2008) 588 definitief.
32 Zie voetnoot 27.

Doelstelling: de eerste helft van 2010 dient de Commissie de criteria betreffende de Europese kritieke infrastructuren voor de ICT-sector vast te stellen.

6. CONCLUSIES

Beveiliging en veerkracht van KII's zijn de frontlijnverdediging tegen verstoringen en aanvallen. De verbetering ervan over heel de EU is van essentieel belang om ten volle van de voordelen van de informatiemaatschappij te kunnen profiteren. Om dit ambitieuze doel te bereiken, wordt een actieplan voorgesteld teneinde de tactische en operationele samenwerking op Europees niveau te verhogen. Het succes van deze acties hangt af van hun effectiviteit om als grondslag te dienen en bevorderlijk te zijn voor activiteiten van de overheids- en de marktsector en van de inzet en deelname van alle lidstaten, Europese instellingen en stakeholders.

In dat verband vindt op 27-28 april 2009 een ministeriële conferentie plaats om de voorgestelde initiatieven met de lidstaten te bespreken en duidelijkheid te verschaffen over hun inzet in de discussie over een gemoderniseerd en versterkt NIB-beleid in Europa.

Tenslotte is de verbetering van de beveiliging en veerkracht van KII's een langetermijndoelstelling en dienen de desbetreffende strategie en maatregelen regelmatig te worden beoordeeld. Bijgevolg zal de Commissie, aangezien deze doelstelling aansluit bij de brede discussie over de toekomst van het beleid voor netwerk- en informatiebeveiliging in de EU na 2012, naar het eind van 2010 toe een initiatief nemen voor een inventarisatieronde om de eerste fase van acties te evalueren en, voor zover dit aangewezen is, verdere maatregelen aan te wijzen en voor te stellen.