RAAD VAN DE EUROPESE UNIE

Brussel, 19 mei 2011 (24.05)
(OR. en)

10299/11

TELECOM 71
DATAPROTECT 55
JAI 332
PROCIV 66

NOTA

van:	het Coreper
aan:	de Raad
nr. Comv.:	8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV 38
nr. vorig doc.:	10003/11 TELECOM 60 DATAPROTECT 48 JAI 308 PROCIV 64
Betreft:	Bescherming van kritieke informatie-infrastructuur (CIIP) "Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid" - Aanneming van conclusies van de Raad

1. De Commissie heeft de Raad op 1 april 2011 haar mededeling toegezonden betreffende de bescherming van kritieke informatie-infrastructuur, "Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid".

2. In de mededeling wordt bekeken hoe het staat met de resultaten sedert de aanneming van het CIIP-actieplan in 2009[1], dat werd gelanceerd om de beveiliging en de robuustheid van de infrastructuur voor informatie- en communicatietechnologie te verbeteren. Voorts worden er de volgende stappen in beschreven die de Commissie voorstelt voor iedere actie op zowel Europees als internationaal niveau.

[1] Het CIIP-actieplan wordt ontvouwd in de Mededeling van de Commissie van 30 maart 2009 betreffende de bescherming van kritieke informatie-infrastructuur - "Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht."

3. Cyberbeveiliging en de bescherming van kritieke informatie-infrastructuur zijn essentieel opdat mensen en bedrijven vertrouwen zouden hebben in internet en andere netwerken, en vormen een kernprioriteit van de digitale agenda voor Europa[2]. De CIIP-mededeling gaat met name over de wereldwijde dimensie van de uitdagingen en het belang van het stimuleren van samenwerking tussen de lidstaten en de particuliere sector op nationaal, Europees en internationaal vlak, zulks in verband met de mondiale interdependentie. Voorgesteld wordt gecoördineerde maatregelen te bevorderen om allerlei verstoringen, door de mens veroorzaakt of natuurlijk, te voorkomen, op te sporen, te beperken of erop te reageren, en de belanghebbenden daarbij te betrekken.

4. Om in de EU tot meer bewustwording en betere paraatheid te komen stelt de Commissie verscheidene concrete maatregelen voor. Het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa) speelt daarbij in veel gevallen een belangrijke rol. In de mededeling worden onder meer maatregelen voorgesteld ter bevordering van richtsnoeren voor de robuustheid en stabiliteit van het internet, het vormen van strategische en internationale partnerschappen, het leveren van gecoördineerde inspanningen op internationale fora en het vergroten van de paraatheid van de EU.

5. Het voorzitterschap van de Raad heeft in samenwerking met de Commissie op 14-15 april in 2011 in Balatonfüred een ministeriële conferentie over de bescherming van kritieke informatie-infrastructuur belegd. De Groep telecommunicatie en informatiemaatschappij heeft rekening gehouden met het resultaat van deze conferentie en de desbetreffende verklaring van het voorzitterschap. In de verklaring van het voorzitterschap werd benadrukt dat het noodzakelijk is dat de lidstaten hun inspanningen opvoeren om hun nationale vermogens inzake cyberbeveiliging te versterken. Onderstreept werd ook het belang van een spoedige hervorming, modernisering en versterking van Enisa om de uitdagingen aan te blijven kunnen en te kunnen voldoen aan de behoefte aan hoogwaardige netwerk- en informatiebeveiliging voor de Unie.

---

[2] Doc. 9981/10.

6. Duurzame bescherming van de Europese kritieke informatie-infrastructuur is van strategisch belang. In de ontwerp-conclusies wordt het belang onderstreept van het ontwikkelen van nationale of overheidsresponsteams voor computercalamiteiten (cert's), alsook het opstellen van nationale noodplannen voor cyberincidenten en het organiseren van nationale cyberoefeningen. Wat Europese samenwerking betreft, handelen de ontwerp-conclusies over de noodzaak de samenwerking tussen de lidstaten te ondersteunen door samenwerkings-mechanismen tussen de lidstaten te ontwikkelen, pan-Europese oefeningen te organiseren en de dialoog over thema's in verband met ict-beveiliging aan te moedigen. De inspanningen van lidstaten in internationale fora zijn erg belangrijk. Met betrekking tot het ontwikkelen van internationale samenwerking op het gebied van wereldwijde netwerk- en informatie-beveiliging en het vormen van strategische internationale partnerschappen op bilateraal en multilateraal niveau, worden de lidstaten en de Commissie verzocht in nauwe coördinatie samen te werken. In de ontwerp-conclusies wordt het Enisa opgeroepen de lidstaten actief te ondersteunen bij hun streven hun nationale vermogens te ontwikkelen en onderling samen te werken. De lidstaten benadrukken in dit verband het belang van een snelle en aangepaste modernisering van het Enisa. Ten slotte wordt de belanghebbenden verzocht initiatieven te nemen en te ijveren voor, en deel te nemen aan, acties ter versterking van netwerk- en informatiebeveiliging, en de beveiliging van en het vertrouwen van de gebruikers in elektronische-communicatienetwerken en -diensten te stimuleren.

7. De Groep telecommunicatie en informatiemaatschappij heeft de voorgestelde ontwerp-conclusies in verscheidene vergaderingen besproken en een beginselakkoord bereikt over de bijgaande tekst. In de vergadering van het Coreper op 18 mei 2011 kaartte de Commissie nogmaals enkele punten aan die al in de Groep waren besproken.

8. De Raad wordt verzocht de bijgaande conclusies te bespreken met het oog op aanneming.

CONCLUSIES VAN DE RAAD

over de bescherming van kritieke infrastructuur
"Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid"

DE RAAD VAN DE EUROPESE UNIE

I. VERWELKOMT

De mededeling van de Commissie van 31 maart 2011 betreffende de bescherming van kritieke informatie-infrastructuur "Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid"[3];

II. HERINNERT AAN

1. De conclusies van de Raad van 20 april 2007 betreffende een Europees programma voor de bescherming van kritieke infrastructuur[4];
2. De richtlijn van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren[5];
3. De mededeling van de Commissie van 30 maart 2009 betreffende de bescherming van kritieke informatie-infrastructuur - "Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht", waarin een actieplan wordt ontvouwd om de beveiliging en robuustheid van vitale infrastructuur voor informatie- en communicatietechnologie te verbeteren[6];
4. De conclusies van het voorzitterschap over CIIP van de ministeriële conferentie van Tallinn van 27-28 april 2009[7];

---

3 Doc. 8548/11.
4 Doc. 7743/07.
5 PB L 345 van 23.12.2008, blz. 75-82.
6 Doc. 8375/09.
7 http://www.riso.ee/tallinnciip/
http://www.riso.ee/tallinnciip/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

5. De toepasselijke bepalingen over informatie- en netwerkbeveiliging van het nieuwe regelgevingskader voor elektronische-communicatienetwerken[8];
6. De resolutie van de Raad van 18 december 2009 over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging[9];
7. De mededeling van de Commissie van 19 mei 2010 over een "digitale agenda voor Europa", waarin wordt benadrukt dat de beveiliging in de digitale maatschappij moet worden opgeschroefd om zodoende het vertrouwen in netwerken te verhogen[10];
8. De conclusies van de Raad van 31 mei 2010 over een digitale agenda voor Europa[11];
9. De Commissiemededeling van 22 november 2010 "De EU-interneveiligheidsstrategie in actie: vijf stappen voor een veiliger Europa"[12];
10. De conclusies van het voorzitterschap over CIIP van de ministeriële conferentie van Balatonfüred van 14-15 april 2011[13].

III. ONDERKENT

1. Het toenemende belang van ICT-systemen, -infrastructuren en -diensten alsmede van internet voor met name de Europese burgers, bedrijven en de Europese economie in het algemeen, waaruit blijkt hoe afhankelijk Europa in sociaal, politiek en economisch opzicht is van ICT en hoe noodzakelijk het is om IT-systemen en -netwerken voldoende robuust te maken en ze te beveiligen tegen alle mogelijke accidentele of opzettelijke verstoringen;
2. Behalve dat zij netwerken en informatiesystemen ernstig verstoren, kunnen beveiligingsincidenten ook het vertrouwen van de gebruikers in technologie, netwerken en diensten ondermijnen en zodoende hun vermogen aantasten om het volle potentieel en het wijdverspreide gebruik van ICT te benutten om bij te dragen aan economische groei en een hogere levenskwaliteit;

---

8 PB L 337 van 18.12.2009, blz. 11-68.
9 Doc. 15841/09.
10 Doc. 9981/10.
11 Doc. 10130/10.
12 Doc. 16797/10.
13 http://www.eu2011.hu/document/presidency-statement-en-ministerial-conference-critical-information-infrastructure-protecti

3. De inspanningen ter zake moeten niet alleen de groei en de werkgelegenheid helpen bevorderen, maar ook de Unie in staat stellen doeltreffend haar vitale belangen te beschermen;
4. De steeds grotere risico's ten gevolge van nieuwe en geraffineerdere bedreigingen voor ICT-netwerken en -diensten en voor internet in het bijzonder, die onder meer kunnen worden aangepakt door op grond van effectief onderzoek en innovatie nieuwe en geraffineerdere zelfbeschermende systemen te ontwikkelen, maar ook effectieve bescherming dringender dan ooit maken;
5. De grote schade die kwetsbaarheid of verstoring van informatie- en communicatie-technologiesystemen, -infrastructuren en -diensten de Europese economie kunnen toebrengen, waarbij bedacht moet worden dat een aanzienlijke verstoring in één lidstaat ook de andere lidstaten en de EU in haar geheel treft;
6. Bijgevolg de noodzaak om als gemeenschappelijk Europees streven de ontwikkeling van een hoge mate van paraatheid, veiligheid en robuustheid te stimuleren en te ondersteunen en om de technische bekwaamheid te vergroten, opdat Europa de uitdaging kan aangaan om de netwerken en de informatie-infrastructuur te beveiligen;
7. De noodzaak om uit te gaan van bestaande algemeen erkende minimumeisen, basisbeginselen en -normen op het gebied van netwerk- en informatiebeveiliging en die verder te ontwikkelen teneinde zoveel mogelijk ingebouwde beveiliging en inherent veilige producten en diensten te bevorderen;
8. De noodzaak om vertrouwen en veiligheid te stimuleren bij alle belanghebbenden, die een basisvoorwaarde is om hechtere samenwerking te bevorderen bij het beschermen van essentiële infrastructuren en om iedere Europeaan digitaal te laten gaan, zoals door de Digitale Agenda voor Europa wordt nagestreefd;
9. De noodzaak van een op samenwerking gebaseerde aanpak van netwerk- en informatie-beveiliging waarbij alle belanghebbenden worden betrokken, in het licht van het algemene gebruik van ICT en internet door alle soorten gebruikers en voor alle soorten doeleinden, waarbij voor alle belanghebbenden een rol is weggelegd om de kennis van de gebruikers te vergroten en hen meer bewust te maken bij het gebruik;
10. De noodzaak dat openbare en particuliere belanghebbenden samenwerken en verantwoordelijkheid nemen bij het ontwikkelen van hun eigen capaciteiten en hun paraatheid om beveiligingsproblemen met potentiële gevolgen voor de beschikbaarheid van elektronische communicatienetwerken en -diensten te voorkomen, op te sporen, erop te reageren.

11. De noodzaak om van het voorkomen van verstoringen niet alleen een nationale en Europese, maar ook een internationale en mondiale uitdaging te maken, gezien de onderlinge verbondenheid van informatie- en communicatietechnologiesystemen, -infrastructuren en -diensten.

IV. ONDERSTREEPT

1. Het strategisch belang van de Europese bedrijfstak op het gebied van ICT en netwerk- en informatiebeveiliging (NIS) voor de duurzame bescherming van de Europese kritieke informatie-infrastructuren;
2. Wat de nationale capaciteiten betreft, het belang van het opzetten van nationale/overheidsgestuurde computercalamiteitenteams (Computer Emergency Response Teams, cert's), het opstellen van nationale rampenplannen bij cyberincidenten en het organiseren van nationale cyberoefeningen;
3. Wat de Europese samenwerking betreft, de noodzaak tot bevordering van samenwerking tussen de lidstaten door regelingen voor samenwerking tussen de lidstaten bij incidenten uit te werken, door pan-Europese oefeningen te organiseren, door aan te zetten tot een dialoog over onderwerpen in verband met ICT-beveiliging - bijvoorbeeld, in voorkomend geval, over ICT-criteria voor Europese kritieke infrastructuur of over de stabiliteit en robuustheid van internet - en door zich samen met de particuliere sector in te zetten voor een sterke IT-beveiligingssector;
4. De aanzienlijke vooruitgang die het Europees Forum van de lidstaten (EFMS) heeft geboekt bij het bevorderen van discussie en uitwisseling tussen de lidstaten onderling en tussen de lidstaten en de Unie over goede beleidspraktijken in samenhang met de beveiliging en robuustheid van ICT-infrastructuur;
5. Het belang van inspanningen van de verschillende belanghebbenden, bijvoorbeeld in verband met het Europees publiek-privaat partnerschap voor veerkracht (EP3R), een voortschrijdend Europawijd samenwerkingskader voor de robuustheid van ICT-infrastructuur;
6. De voorname rol van het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa) in samenhang met de activiteiten van de lidstaten en publieke en private belanghebbenden in de Unie op het gebied van netwerk- en informatiebeveiliging, in het bijzonder bij het opzetten van goed functionerende nationale/overheidsgestuurde cert's;

7. Het welslagen van de eerste pan-Europese cyberoefening van 4 november 2010, waaruit de gezamenlijke wil sprak om over de grenzen heen tussen de lidstaten samen te werken;
8. De voordelen voor netwerk- en informatiebeveiliging die voortvloeien uit een nationale, Europese en mondiale cultuur van risicoanalyse en -beheersing op alle niveaus en bij alle belanghebbenden, die gericht is op het ondernemen van gecoördineerde acties om alle soorten verstoringen te voorkomen, op te sporen en te beperken en daarop te reageren;
9. De mogelijkheden die voor economische concurrentie zijn gecreëerd door benutting van de kracht van nieuwe kennis over netwerk- en informatiebeveiligingssystemen en met name over toepassingen in verband met ingebouwde beveiliging en nieuwe zelfbeschermende systemen;
10. De voordelen van het verder stimuleren, met steun van het Enisa, van een coherente, op samenwerking gebaseerde aanpak voor netwerk- en informatiebeveiliging in de lidstaten, de EU-instellingen en het bedrijfsleven.

V. BENADRUKT

Het belang van een spoedige en adequate modernisering van het Enisa, zodat dat agentschap beter en gerichter zijn rol kan vervullen en verder kan bijdragen aan het versterken van de netwerk- en informatiebeveiliging in Europa.

VI. VERZOEKT DE LIDSTATEN

1. Hun inspanningen voor het bevorderen van een cultuur van risicobeheersing en onderwijs-, opleidings- en onderzoeksprogramma's op het gebied van netwerk- en informatiebeveiliging op te voeren;
2. Cert's op te richten in de lidstaten die daar nog niet over beschikken;
3. De samenwerking tussen reeds opgerichte of nog op te richten nationale/overheids-gestuurde cert's en andere internationaal erkende, in de lidstaten werkzame cert's te bevorderen;
4. Te ijveren voor de totstandkoming in 2012 van een goed functionerend netwerk van nationale/overheidsgestuurde cert's en andere internationaal erkende, in de lidstaten werkzame cert's, met steun van het Enisa waar dat van toepassing is;

5. Overeenstemming te bereiken over de wijze waarop een Europees Informatie-uitwisselings- en waarschuwingssysteem (Eisas) zou kunnen worden ingevoerd teneinde, met steun van het Enisa, waar dat van toepassing is, hun nationale informatie-uitwisselings- en waarschuwingssystemen op te zetten;
6. Te overwegen een nationale cyberbeveiligingsstrategie in te voeren indien die ontbreekt;
7. Nationale rampenplannen bij cyberincidenten te ontwikkelen, teneinde erop voorbereid te zijn om op te treden en, indien dat passend is, overleg te plegen met de lidstaten in geval van ernstige incidenten;
8. De samenwerking tussen de lidstaten te intensiveren en op basis van de nationale crisisbeheersingservaringen en -resultaten en in samenwerking met het Enisa te helpen bij de ontwikkeling van Europese samenwerkingsmechanismen bij cyberincidenten, die zullen worden uitgetest in het kader van de volgende CyberEurope-oefening in 2012;
9. Nationale of grensoverschrijdende cyberoefeningen te organiseren teneinde de paraatheid bij verstoring van de netwerk- en informatiebeveiliging te testen, adequaat bij te dragen aan de organisatie van en de deelname aan Europese cyberoefeningen volgens een geschikt, haalbaar tijdschema en andere capaciteitsopbouwactiviteiten in de Unie;
10. Binnen het EFMS en in samenwerking met EP3R verder te werken aan de criteria voor het in kaart brengen van Europese kritieke infrastructuren in de ICT-sector, met name voor vaste en mobiele communicatie en voor internet;
11. Op basis van onderlinge wederzijdse bijstand tussen de lidstaten elkaar bij grens-overschrijdende incidenten te hulp te komen;
12. Hun inspanningen op alle internationale fora ter zake te bestendigen en te coördineren en zich samen met de instellingen van de Unie in te zetten voor het versterken van de internationale samenwerking op het gebied van de wereldwijde netwerk- en informatie-beveiliging en voor het opzetten van strategische internationale partnerschappen op bilateraal en multilateraal niveau, bijvoorbeeld door in nauwe coördinatie met de Commissie deel te nemen aan de activiteiten van de EU-VS-werkgroep cyber-beveiliging en cybercriminaliteit;
13. Op zowel nationaal als Europees niveau de samenwerking met de particuliere sector te bevorderen en te ondersteunen.

VII. VERZOEKT DE COMMISSIE

1. De robuustheid en de stabiliteit van internet op alle niveaus te stimuleren in samenwerking met openbare en particuliere belanghebbenden;
2. Een samenhangende, efficiënte Europese aanpak van netwerk- en informatiebeveiliging te stimuleren om overlapping te voorkomen en een gemeenschappelijke visie te smeden inzake de verschillende uitdagingen waarmee de Unie wordt geconfronteerd;
3. Samen met de lidstaten en het Enisa te bevorderen dat wordt uitgegaan van bestaande algemeen erkende minimumeisen, basisbeginselen en -normen op het gebied van netwerk- en informatiebeveiliging en dat die verder worden ontwikkeld, teneinde zo veel mogelijk ingebouwde veiligheid en inherent veilige producten en diensten te bevorderen;
4. Indien nodig, nauw met de lidstaten samen te werken en hun uit deze conclusies voortvloeiende inspanningen te ondersteunen;
5. De lidstaten binnen het EFMS en EP3R te helpen bij het werken aan de criteria voor het in kaart brengen van Europese kritieke infrastructuur in de ICT-sector, met name voor vaste en mobiele communicatie en voor internet;
6. Zoveel mogelijk de particuliere sector te betrekken bij haar inspanningen om wereldwijde netwerk- en informatiebeveiliging te bewerkstelligen;
7. Een ambitieus O&O-programma inzake beveiliging van netwerken en informatiesystemen en toepassingen te stimuleren en dat op doeltreffende wijze te koppelen aan de verdedigingsplannen betreffende de bescherming van kritieke informatie-infrastructuur;
8. De lidstaten te steunen bij het verkennen van de mogelijkheden voor het ontwikkelen van Europese samenwerkingsmechanismen bij cyberincidenten, die zullen worden uitgetest in het kader van de volgende CyberEurope-oefening in 2012;
9. De ontwikkeling van de beste governancestrategieën voor opkomende technologieën met een wereldwijde impact, waaronder "cloud computing", in het oog te houden;

10. De paraatheid van de EU te verhogen door een cert voor de Unie-instellingen op te zetten;
11. In nauwe coördinatie met de lidstaten en samen met de bevoegde Unie-instanties te ijveren voor versterking van de internationale samenwerking op het gebied van netwerk- en informatiebeveiliging met relevante internationale partners en op verschillende relevante fora, zoals de EU-VS-werkgroep Cyberbeveiliging en cybercriminaliteit;
12. Het Europees Parlement en de Raad geregeld op de hoogte te stellen van initiatieven op EU-niveau inzake netwerk- en informatiebeveiliging.

VIII. ROEPT HET ENISA OP

1. De lidstaten actief te blijven ondersteunen in hun inspanningen die gericht zijn op nationale capaciteitsopbouw en onderlinge samenwerking;
2. Zijn deskundigheid op het gebied van netwerk- en informatiebeveiliging verder te ontwikkelen en bij te dragen aan een beter begrip van de nieuwe uitdagingen die zich in Europa voordoen op het gebied van netwerk- en informatiebeveiliging.

IX. VERZOEKT DE BELANGHEBBENDEN OM

1. Initiatieven te nemen en te ijveren voor, en deel te nemen aan, acties ter versterking van netwerk- en informatiebeveiliging, en de beveiliging van en het vertrouwen van de gebruikers in elektronische-communicatienetwerken en -diensten te stimuleren;
2. Samen met de openbare belanghebbenden de uitdagingen op het gebied van netwerk- en informatiebeveiliging aan te gaan en de afzonderlijke verantwoordelijkheden, met name voor eindgebruikers, te helpen afbakenen;
3. Veiliger en betrouwbaarder ICT-producten, -diensten en -apparatuur en -programmatuuroplossingen te ontwikkelen en te produceren en zodoende bij te dragen aan de bescherming van onze economieën, die grotendeels afhankelijk zijn van ICT;
4. Aan publiek-private partnerschappen deel te nemen teneinde bij te dragen aan de ontwikkeling van robuuste en beveiligde netwerken en een sterke Europese IT-beveiligingssector. Die partnerschappen moeten ook bevorderlijk zijn voor een multi-stakeholderdialoog en het inzicht in alle uitdagingen waarvoor wij ons geplaatst zien;

5. De gebruikers bewuster te maken van de risico's in verband met netwerk- en informatiebeveiliging, en hen te informeren over de beste manieren om dergelijke risico's te vermijden en/of erop te reageren;
6. Indien nodig, de lidstaten te ondersteunen bij het opstellen van nationale rampenplannen bij cyberincidenten en bij de organisatie van cyberoefeningen;
7. Alle vereiste technische en organisatorische maatregelen te treffen voor het beschermen van de beschikbaarheid en de beveiliging van elektronische-communicatienetwerken en -diensten;
8. Deel te nemen aan het invoeren en verder ontwikkelen van minimumeisen en algemeen en internationaal erkende normen inzake netwerk- en informatiebeveiliging.