EUROPEES PARLEMENT

1999 *2004*

Zittingsdocument

DEFINITIEVE VERSIE
A5-0311/2002

17 september 2002

VERSLAG

over de mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de regio's inzake netwerk- en informatieveiligheid: voorstel voor een Europese beleidsaanpak (COM(2001) 298 – C5-0657/2001 – 2001/2280(COS))

Commissie vrijheden en rechten van de burger, justitie en binnenlandse zaken

Rapporteur: Elena Ornella Paciotti

INHOUD

Blz.

PROCEDUREVERLOOP 4

ONTWERPRESOLUTIE 5

TOELICHTING 10

ADVIES VAN DE COMMISSIE INDUSTRIE, EXTERNE HANDEL, ONDERZOEK EN ENERGIE.....13

PROCEDUREVERLOOP

Bij schrijven van 7 juni 2001 deed de Commissie haar mededeling inzake netwerk- en informatieveiligheid: voorstel voor een Europese beleidsaanpak (COM(2001) 298 – 2001/2280(COS)) toekomen aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de regio's.

Op 13 december 2001 gaf de Voorzitter van het Parlement kennis van de verwijzing van deze mededeling naar de Commissie vrijheden en rechten van de burger, justitie en binnenlandse zaken als commissie ten principale en naar de Commissie juridische zaken en interne markt, de Commissie industrie, externe handel, onderzoek en energie en de Commissie cultuur, jeugd, onderwijs, media en sport als medeadviserende commissies (C5-0657/2001).

De Commissie vrijheden en rechten van de burger, justitie en binnenlandse zaken benoemde op haar vergadering van 10 oktober 2001 Elena Ornella Paciotti tot rapporteur.

De commissie behandelde de mededeling van de Commissie en het ontwerpverslag op haar vergaderingen van 23 mei, 17 juni, 8 juli en 12 september 2002.

Op laatstgenoemde vergadering hechtte zij met 27 stemmen voor en 1 tegen bij 2 onthoudingen haar goedkeuring aan de ontwerpresolutie.

Bij de stemming waren aanwezig: Jorge Salvador Hernández Mollar (voorzitter), Robert J.E. Evans en Giacomo Santini (ondervoorzitters), Elena Ornella Paciotti (rapporteur), Niall Andrews, Roberta Angelilli, Alima Boumediene-Thiery, Marco Cappato (verving Mario Borghezio), Michael Cashman, Charlotte Cederschiöld, Ozan Ceyhun, Carlos Coelho, Gérard M.J. Deprez, Giuseppe Di Lello Finuoli, Adeline Hazan, Anna Karamanou (verving Martin Schulz), Timothy Kirkhope, Eva Klamt, Alain Krivine (verving di Ole Krarup), Bill Newton Dunn, José Ribeiro e Castro, Martine Roure, Miet Smet (verving Hubert Pirker), Patsy Sörensen, The Earl of Stockton (verving The Lord Bethell), Joke Swiebel, Fodé Sylla, Anna Terrón i Cusí, Maurizio Turco, Christian Ulrik von Boetticher en Olga Zrihen Zaari (verving Walter Veltroni) .

Het advies van de Commissie industrie, externe handel, onderzoek en energie is bij dit verslag gevoegd. De Commissie juridische zaken en interne markt heeft op 27 november 2001 besloten geen advies uit te brengen en de Commissie cultuur, jeugd, onderwijs, media en sport op 21 november 2001.

Het verslag werd ingediend op 17 september 2002.

ONTWERPRESOLUTIE

Resolutie van het Europees Parlement over de mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de regio's inzake netwerk- en informatieveiligheid: voorstel voor een Europese beleidsaanpak (COM(2001) 298 – C5-0657/2001 - 2001/2280(COS))

Het Europees Parlement,

– gezien de mededeling van de Commissie (COM(2001) 298 – C5-0657/2001[1]),

– gezien zijn aanbeveling van 6 september 2001 betreffende de strategie om de informatiemaatschappij veiliger te maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden en het verdrag van de Raad van Europa over computercriminaliteit, dat op 26 november 2001 in Boedapest werd ondertekend[2],

– gezien het voorstel voor een kaderbesluit van de Raad van 19 april 2002 over aanvallen op informatiesystemen, waarin de corresponderende elementen van het hierboven aangehaalde verdrag van de Raad van Europa ten uitvoer worden gelegd (COM(2002) 173),

– gezien de conclusies van de Europese Raad in Stockholm van maart 2001 en in Sevilla van 21 en 22 juni 2002, en de mededeling van de Commissie over "*e*Europe 2005: een informatiemaatschappij voor iedereen", waarin erop wordt gehamerd dat het dringend noodzakelijk is dat de veiligheid van netwerken wordt gegarandeerd,

– onder verwijzing naar zijn eerdere resoluties over dit thema, met name zijn resolutie van 5 september 2001 over het bestaan van een wereldwijd systeem voor de interceptie van particuliere en economische communicatie (ECHELON-interceptiesysteem) en de meest recente internationale initiatieven (G8, OESO, VN)[3],

– gelet op artikel 47, lid 1 van zijn Reglement,

– gezien het verslag van de Commissie vrijheden en rechten van de burger, justitie en binnenlandse zaken en het advies van de Commissie industrie, externe handel, onderzoek en energie (A5-0311/2002),

Het belang van veilige netwerken in het kader van de informatiemaatschappij

A. overwegende dat de convergentie van elektronische communicatienetwerken in een hoog tempo plaatsvindt, en dat deze netwerken steeds meer van kritisch economisch en maatschappelijk belang worden,

B. overwegende dat het als gevolg van deze convergentie noodzakelijk is een adequaat beleids- en juridisch kader in de Europese Unie te scheppen, waardoor de handhaving van netwerk- en informatieveiligheid, een cruciale voorwaarde voor de

[1] PB C 43 van 16.2.2002, blz. 2.
[2] Goedgekeurde teksten (P5 TAPROV(2001)0284).
[3] Goedgekeurde teksten (P5 TAPROV(2001)0264).

informatiesamenleving, wordt gewaarborgd,

C. overwegende dat een toereikende veiligheid van netwerken een sleutelfactor is voor de ontwikkeling van netwerkdiensten en elektronische handel en voor de goede werking van de gemeenschappelijke markt,

D. overwegende dat oplossingen ter verhoging van de veiligheid enkel effectief zijn als alle betrokken partijen (overheid, consumenten, wetenschappelijke onderzoekers en bedrijven), inclusief de burgers, zich bewust zijn van veiligheidsrisico's en de eigen verantwoordelijkheid ten aanzien van de te nemen voorzorgsmaatregelen,

E. overwegende dat oplossingen ter verhoging van de veiligheid enkel effectief zijn als deze door alle relevante marktspelers worden toegepast, bij voorkeur op basis van open internationale normen,

F. overwegende dat de Computer Emergency Response Teams (CERT's) in de verschillende lidstaten op uiteenlopende wijze te werk gaan, waardoor de samenwerking onnodig complex is,

1. stelt vast dat netwerken momenteel onvoldoende beveiligd zijn, aangezien 60% van de Europese bedrijven in de afgelopen twee jaar al ernstige problemen heeft gehad, dat slechts 14% van hen een netwerkveiligheidsbeleid heeft, en dat voor 62% van de kleine en middelgrote ondernemingen en voor 81% van de grote ondernemingen het gebrek aan veiligheid de belangrijkste belemmering is voor het gebruik van Internet[1];

2. constateert eveneens dat gebruikers vaak niet in staat lijken zich te verdedigen tegen bedreigingen voor de veiligheid van netwerken, waaronder aanvallen waarbij sprake is van boos opzet en onvoorziene gebeurtenissen als:

- onderscheppen van al dan niet draadloze gegevensoverdracht via elektronische SOTA-bewakingssystemen, *routers, gateways* en *netwerkservers*; niet-geautoriseerde toegang met behulp van gekraakte wachtwoorden of een vervalste identiteit;
- netwerkstoringen als gevolg van aanvallen op de *server* of de *router*, *flooding*, *denial of service* of aanvallen op de integriteit van gegevens door middel van kwaadaardige software, zoals virussen, die de gegevens wijzigen of vernietigen;
- omgevingsfactoren en onvoorziene gebeurtenissen (zoals natuurrampen);
- criminele aanvallen, in sommige gevallen met een terroristisch oogmerk;

3. neemt kennis van het feit dat essentiële infrastructuren voor bijvoorbeeld vervoer, communicatie, levering van energie en water, financiële diensten en banken het doelwit kunnen zijn van netwerkaanvallen en dat de kwetsbaarheid van netwerken dientengevolge een groot risico vormt voor de correcte werking van de economie van de Unie en het dagelijks leven van de burgers;

4. is van mening dat bij dergelijke zwakke plekken en vanwege uiteenlopende handelwijzen, het gebrek aan gemeenschappelijke standaarden en de snelle evolutie van de technologie, een reactie die uitsluitend is gebaseerd op de vrijwillige inzet van de betrokkenen niet

[1] ESTO, *Future Bottlenecks in the information society*, verslag aan het EP, Commissie industrie, externe handel, onderzoek en energie, blz. 143 en Eurostat.

volstaat; benadrukt tevens de wenselijkheid dat de producenten veilige producten ontwikkelen en participeren in de ontwikkeling op gebied van productveiligheid;

5. onderstreept dat er zo snel mogelijk voor moet worden gezorgd dat alle burgers, bedrijven en administraties toegang hebben tot de openbare elektronische diensten van alle communautaire instellingen, via een systeem van beveiligde en persoonlijke toegang met authenticatie, die moet worden gegarandeerd aan de hand van het gebruik van de elektronische handtekening en de bepaling van Europese normen die voor de EU-instellingen onmiddellijk van kracht moeten worden;

6. benadrukt het belang van het betrekken van de relevante sectoren bij het ontwikkelen van beleid voor netwerkveiligheid, netwerkintegriteit en informatieveiligheid in relatie tot IP-omgevingen;

7. neemt kennis van de toename van particuliere en overheidsinitiatieven op internationaal niveau om de betrouwbaarheid van netwerken te garanderen, zoals het White House Office of Cyberspace Security in de Verenigde Staten, het netwerk voor de uitwisseling van informatie over veiligheid in het kader van de G8, de netwerken van Europol en Interpol;

8. is het eens met de Europese Raad, de Raad en de Commissie dat een Europese aanpak nodig is om te garanderen dat de gemeenschappelijke markt van communicatiediensten kan profiteren van de voordelen van de gemeenschappelijke oplossingen en doeltreffend kan optreden op het wereldtoneel;

9. herinnert eraan dat de verantwoordelijken voor de levering van netwerkdiensten op grond van artikel 17 van de algemene richtlijn betreffende de bescherming van gegevens (95/46/EG) en de daaropvolgende bepalingen betreffende de veiligheid en integriteit van netwerken[4], waarin dit artikel wordt bevestigd, al verplicht zijn maatregelen te treffen om een passend niveau van databescherming te garanderen;

10. onderstreept de noodzaak van het zo snel mogelijk ontwikkelen van gemeenschappelijke definities voor netwerkveiligheid, netwerkintegriteit en informatieveiligheid;

11. verzoekt de Commissie een actieplan op te stellen ter bevordering van het gebruik van de digitale handtekening, bijvoorbeeld via het vastleggen van Europese normen die voor de communautaire instellingen onmiddellijk van kracht moeten worden;

Institutionele aspecten

12. verzoekt de Commissie het Parlement en de Raad de gegevens te doen toekomen over de problemen bij de toepassing van de bestaande richtlijnen inzake gegevensbescherming, in het bijzonder in verband met de artikelen over netwerkveiligheid;

13. is van mening dat niet langer gewacht kan worden met de vaststelling van een Europese strategie, die neutraal moet zijn ten opzichte van de gebruikte technologie, maar de

[4] Richtlijn 97/66/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector; richtlijn 97/33/EG inzake interconnectie; richtlijn 98/10/EG over spraaktelefonie; richtlijn 99/93/EG inzake elektronische handtekeningen en richtlijn 2000/31/EG inzake elektronische handel.

volgende doelstellingen moet hebben:

a) definiëren of actualiseren van de standaarden op het gebied van veiligheid van telecommunicatienetwerken en garanderen van hun compatibiliteit;

b) bevorderen van de ontwikkeling van versleutelings- en certificatiesystemen op Europese schaal en versterken van de maatregelen ter bescherming van gegevens;

c) preventie en doeltreffende bestrijding van misdaad met inachtneming van de wettelijke garanties;

d) bewustmaken van burgers, gebruikers en exploitanten uit de particuliere sector en binnen de overheid door middel van voorlichtingscampagnes op nationaal en Europees niveau en bevorderen van de verspreiding van de beste praktijken op dit terrein;

e) wetenschappelijk onderzoek in de sectoren met de grootste achterstand versterken, zoals de evaluatie van de veiligheid van IT, de integratie ervan in het systeem, de bescherming van de eindgebruiker en de technologieën voor de verbetering van privacybescherming, waaronder systemen als Anti-Echelon/Magic Lantern/Carnivore;

14. is het eens met de Commissie dat er zo snel mogelijk een *taskforce* voor netwerkveiligheid opgezet moet worden met als doelstellingen:

- identificatie van de nationale autoriteiten die verantwoordelijk zijn voor het beheer van netwerken;
- identificatie van de nationale autoriteiten die verantwoordelijk zijn voor de coördinatie en de bevelslijnen bij de opvang van crises in de kritische en elektronische infrastructuur van de EU;
- coördinatie van de activiteiten van deze autoriteiten en uitwisseling van de beste praktijken;
- oprichting van een centrum voor geavanceerd onderzoek dat verantwoordelijk wordt voor preventie en uitwisseling van informatie;
- verzameling en analyse van gegevens over de problemen op het gebied van netwerkveiligheid;
- analyse van de actuele en toekomstige risico's voor de veiligheid;
- organisatie van discussiefora op Europees niveau tussen degenen die betrokken zijn bij het probleem van de veiligheid (overheid, consumenten, wetenschappelijke onderzoekers, bedrijfsleven);

15. spoort de Commissie aan erop toe te zien dat die task force bij zijn werkzaamheden rekening houdt met hetgeen reeds in het Cyberline Forum is gezegd en het Forum ook bij zijn toekomstige werkzaamheden betrekt;

16. vraagt de Commissie om, na zorgvuldig overleg met de lidstaten en de privé-sector, de doelstellingen, taken en verantwoordelijkheden van de op te richten task force helder te formuleren en te zorgen voor voldoende personele en financiële middelen voor de task force;

17. verzoekt de Commissie met voorrang te onderzoeken wat de veiligheidsvereisten zijn en het onderzoek naar eerste-waarschuwingssytemen in de elektronische infrastructuur toe

te passen op netwerken van de
a) kritische infrastructuren, essentiële openbare diensten en diensten in verband met de menselijke gezondheid en op
b) eerste-waarschuwingssystemen en de interoperabiliteit daarvan,
c) en de ontwikkeling van e-government en e-business te stimuleren;

18. meent dat een eerste aanzet tot EU-wetgeving op dit terrein gebaseerd moet zijn op de aan de EU toegewezen bevoegdheden op het terrein van de trans-Europese netwerken (Titel XV VEG) en, voor de aspecten die harmonisatie behoeven, op het terrein van de gemeenschappelijke markt (art. 95 VEG); de oprichting van een *taskforce* moet worden opgenomen in dezelfde regeling waarin de doelstellingen op Europees niveau worden vastgelegd;

19. verzoekt de Commissie zo snel mogelijk een evaluatie in te dienen van de financiële impact van het optreden van de Unie in deze sector, met vergelijkende gegevens over analoge initiatieven in de lidstaten of in derde landen (bijvoorbeeld de VS);

20. is het met de Europese Raad, de Raad en de Commissie eens, dat een Europese benadering nodig is voor nieuwe wetgeving of herziening van bestaande wetgeving inzake opsporing, vervolging en bestraffing van van criminele of terroristische activiteiten tegen kritische infrastructuren;

21. nodigt Commissie en Raad uit deze discussie zoveel mogelijk te plaatsen in het kader van de taken van Eurojust om een geharmoniseerd juridisch kader te ontwikkelen voor de opsporing en vervolging van computercriminelen;

22. verzoekt zijn Voorzitter deze resolutie te doen toekomen aan de Raad, de Commissie, de regeringen en de parlementen van de lidstaten en aan de Raad van Europa.

TOELICHTING

Inleiding

De mededeling inzake netwerk- en informatieveiligheid werd een jaar geleden gepubliceerd en beoogt een globale strategie vast te stellen voor de veiligheid van elektronische netwerken, overeenkomstig het verzoek dat werd gedaan door de Europese Raad van Stockholm op 23 en 24 maart 2001. De mededeling sluit aan op de voorgaande mededeling van de Commissie van 8 oktober 1997, getiteld "Zorgen voor veiligheid van en vertrouwen in de elektronische communicatie" (COM(1997) 503).

De voorgestelde aanpak vormt een aanvulling op de kadermededeling van 22 januari 2001 inzake cybermisdaad. Dit thema werd door de Raad van ministers van Telecommunicatie weer opgevat en verder uitgediept, toen die 6 december 2001 een gedetailleerde resolutie goedkeurde. In dit kader valt ook het voorstel van de Commissie van 19 april 2002 voor een kaderbesluit inzake aanvallen op informatiesystemen.

In maart 2002 had de Europese Raad van Barcelona de Commissie verzocht een voorstel in te dienen voor een nieuw actieplan "e-Europa 2005", dat ook betrekking zou moeten hebben op de veiligheid van de netwerken en de informatie in een perspectief van meerdere zuilen. Op 21-22 juni 2002 heeft de Commissie dit plan voorgelegd aan de Europese Raad te Sevilla, die hieraan zijn goedkeuring heeft gehecht.

Huidige stand van de communautaire wetgeving en de vooruitzichten

Maatregelen op het gebied van de netwerkveiligheid heeft de communautaire wetgever reeds in drie sectoren genomen:

a) databescherming: in dit verband moeten met name worden genoemd **richtlijn 95/46/EG** inzake de bescherming van fysieke personen met betrekking tot de verwerking en het vrije vervoer van persoonlijke gegevens (art. 17) en **richtlijn 97/66/EG** van het Europees Parlement en van de Raad van 15 december 1997 inzake de behandeling van persoonlijke gegevens en de bescherming van het privé-leven in de sector van de telecommunicatie (art. 4 en 5), welke laatste zal worden vervangen door de op 25 juni 2002 door de Raad goedgekeurde richtlijn (verslag-Cappato A5-0130/2002).

b) het telecommunicatiebeleid: het streven naar een grotere netwerkveiligheid ligt ook ten grondslag aan **richtlijn 99/93/EG** van het Europees Parlement en de Raad van 13 december 1999 inzake een communautair kader voor elektronische ondernemingen en **richtlijn 2000/31/EG** inzake de elektronische handel. Een ander aspect dat met de netwerkveiligheid verband houdt is de bescherming van de netwerken tegen natuurrampen of grootschalige schade (**richtlijn 97/33/EG** inzake interconnectie, artikel 10 en **richtlijn 98/10/EG** inzake spraaktelefonie, artikel 13).

c) Bestrijding van de computercriminaliteit. een specifiek aspect van de netwerkveiligheid betreft de bestrijding van de netwerkcriminaliteit. De referentieteksten in dit verband zijn de **mededeling van de Commissie** inzake het veiliger maken van de informatiemaatschappij door de computercriminaliteit te bestrijden (COM(2000) 890); de **aanbeveling van de Raad** van 25 juni 2001 over 24 uur per dag toegankelijke contactpunten voor de bestrijding van

criminaliteit op hoog technologisch niveau en het **voorstel voor een kaderbesluit** van de Raad inzake aanvallen op informatiesystemen (COM(2002) 173) .

De mededeling beoogt de drie bovengenoemde aspecten met elkaar te verbinden in een geïntegreerde strategie, die een ruim kader biedt voor maatregelen, welke zich uitstrekken van:

- de sensibilisering van het publiek, om dit zich zelf te leren beschermen

tot meer specifieke initiatieven zoals:

- invoering van een Europees systeem voor het signaleren en analyseren van de problemen;
- steun aan het onderzoek op veiligheidsgebied;
- normalisering en verstrekking van certificaten;
- vrij verkeer van coderingsproducten;
- veiligheid van de overheidsadministratie;
- internationale samenwerking.

De rechtvaardiging voor communautair ingrijpen

In de Verenigde Staten is de privé-sector een pro-actieve rol gaan spelen en heeft deze het initiatief genomen tot zelfreglementeringsmechanismen, zoals gedragscodes en veiligheidsprogramma's. De privé-sector heeft er namelijk belang bij zorg te dragen voor een vertrouwensklimaat bij het gebruik van de netwerken, zodat het ingrijpen van de wetgever tot een minimum beperkt kan blijven.

Alleen te vertrouwen op dit vrijwillige aspect, volstaat echter niet altijd om de veiligheid te garanderen. Bovendien beantwoorden regelingen die door particuliere personen zijn ontwikkeld meer aan de behoeften van de markt dan aan de vereisten in verband met de bescherming van de fundamentele rechten van de burgers. Bovendien dragen particuliere personen, zoals bijvoorbeeld detailhandelaren in software, geen aansprakelijkheid voor de uit hun gedragingen voortvloeiende schade op veiligheidsgebied. Zoals de Commissie het in haar mededeling formuleert "*dragen gebruikers en leveranciers die voor een laag veiligheidsniveau kiezen geen wettelijke aansprakelijkheid daarvoor*". Om deze reden heeft de Europese Unie voor een legislatieve benadering gekozen. Het doel is een veiligheidscultuur te ontwikkelen en de uitwisseling van veilige informatie te bevorderen, met gebruikmaking van instrumenten die reeds op de markt bestaan, maar die onvoldoende bekend of onderling niet compatibel zijn.

Het communautaire ingrijpen wordt ook gerechtvaardigd door het feit dat de communicatie- en informatiediensten van grensoverschrijdende aard zijn, hetgeen trouwens ook geldt voor de veiligheidsproblemen. Daarom is een Europese strategische actie noodzakelijk om de ontwikkeling van de elektronische handel te bevorderen en een werkelijke binnenmarkt voor de telecommunicatie- en informatiediensten te creëren, die gebruik kan maken van gemeenschappelijke oplossingen en op wereldschaal doeltreffend kan functioneren. Zo heeft bijvoorbeeld de invoering van de domeinnaam "Europees Internet", met de extensie .eu, niet alleen een bevestiging betekend van de Europese presentie in de cyberspace, maar is deze vooral ook een gelegenheid geweest om in de cyberspace het vertrouwensklimaat te introduceren dat de EU dankzij haar binnenmarkt gecreëerd heeft.

Door de Commissie voorgestelde maatregelen

Het Europees Parlement ondersteunt de Commissie bij haar voornemen om een task force voor informatieveiligheid op te richten, die halverwege 2003 operationeel zou moeten zijn. Het Parlement verzoekt de Commissie evenwel in overweging te nemen om als rechtsgrondslag van het wetgevend optreden op dit gebied te kiezen voor titel XV van het EG-Verdrag betreffende de trans-Europese netwerken en artikel 95 van het EG-Verdrag waar het de aspecten betreft waarvoor in het kader van de binnenmarkt een harmonisering vereist is.

Het Europees Parlement zou zodoende op voet van gelijkwaardigheid betrokken zijn bij het besluitvormingsproces op een gebied dat van zo grote betekenis is voor de belangen van de door haar vertegenwoordigde burgers.

Woordenlijst:

Server: een programma op afstand dat informatie verstrekt aan de gebruiker. Houdt zich alleen bezig met het bewaren, opvragen en verzenden van gegevens aan de gebruiker die daarom heeft verzocht. Wanneer de gebruiker een bepaald document opvraagt dat zich op een zeker punt in het netwerk bevindt, stuurt de gebruiker een verzoek aan de server via het Internet. Na het verzoek in ontvangst te hebben genomen, zoekt de server de gewenste gegevens op en stuurt die naar de computer van de gebruiker.
***Gateway* (portal):** verbindt alle computers van een netwerk (b.v. van een bedrijfsnetwerk) met het Internet met gebruikmaking van elk denkbaar type verbinding.
Router: een inrichting of computerprogramma dat het dichtstbijzijnde punt van het netwerk vaststelt waartoe gebruiker zich moet richten om de gewenste informatie te verkrijgen. De *router* is met ten minste twee netwerken verbonden en beslist over welk netwerk de informaties moeten worden verzonden, op grond van een evaluatie van de huidige stand van de netwerken waarmee hij verbonden is. De *router* bevindt zich in elke portal (*gateway*).

29 mei 2002

ADVIES VAN DE COMMISSIE INDUSTRIE, EXTERNE HANDEL, ONDERZOEK EN ENERGIE

aan de Commissie vrijheden en rechten van de burger, justitie en binnenlandse zaken

inzake de mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de regio's "Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak"
(COM(2001) 298 – C5-0657/2001 – 2001/2280(COS))

Rapporteur voor advies: W.G. van Velzen

PROCEDUREVERLOOP

De Commissie industrie, externe handel, onderzoek en energie benoemde op haar vergadering van 22 november 2001 W.G. van Velzen tot rapporteur voor advies.

De commissie behandelde het ontwerpadvies op haar vergaderingen van 16 april en 22 mei 2002.

Op laatstgenoemde vergadering hechtte zij met algemene stemmen haar goedkeuring aan de hierna volgende conclusies.

Bij de stemming waren aanwezig: Carlos Westendorp y Cabeza (voorzitter), Peter Michael Mombaur en Yves Piétrasanta (ondervoorzitters), W.G. van Velzen (rapporteur voor advies), Nuala Ahern, Sir Robert Atkins, María del Pilar Ayuso González (verving Jaime Valdivielso de Cué), Guido Bodrato, David Robert Bowe (verving Norbert Glante), Marco Cappato, Massimo Carraro, Gérard Caudron, Giles Bryan Chichester, Willy C.E.H. De Clercq, Concepció Ferrer, Francesco Fiori (verving Umberto Scapagnini), Christos Folias (verving Christian Foldberg Rovsing), Michel Hansenne, Hans Karlsson, Bashir Khanbhai, Bernd Lange (verving Rolf Linkohr), Werner Langen, Caroline Lucas, Marjo Matikainen-Kallström, Eryl Margaret McNally, William Francis Newton Dunn (verving Nicholas Clegg), Angelika Niebler, Reino Paasilinna, Paolo Pastorelli, Elly Plooij-van Gorsel, Samuli Pohjamo (verving Colette Flesch), Godelieve Quisthoudt-Rowohl, Paul Rübig, Konrad K. Schwaiger, Alejo Vidal-Quadras Roca, Dominique Vlasto, Anders Wijkman (verving John Purvis), Myrsini Zorba en Olga Zrihen Zaari.

BEKNOPTE MOTIVERING

Veiligheid speelt een rol in alle facetten van het dagelijkse leven. Van burgers en bedrijven wordt verwacht dat zij in eerste plaats hun eigen verantwoordelijkheid kennen én nemen op het gebied van veiligheid van zichzelf en van hun (directe) omgeving. Dit geldt dus ook in het geval van elektronische communicatienetwerken. Ontwrichtende aanvallen op het internet zijn gemeengoed geworden. Zich snel verspreidende virussen via het e-mailverkeer hebben in korte tijd veel gebruikers bewust gemaakt van dit risico en van de kwetsbaarheid van hun computersystemen. Tegelijkertijd vindt de convergentie van elektronische communicatienetwerken in hoog tempo plaats. Het is daarom van belang dat de bekendheid van zowel netwerkconvergentie als mogelijke veiligheidsrisico's vergroot wordt.

Naast de inmiddels bekende computervirussen bestaan er nog vele andere veiligheidsrisico's op het gebied van elektronische communicatienetwerken. Niet alleen virussen die verspreid worden via e-mailverkeer, maar ook het onderscheppen van communicatie, vervalsing van identiteit of ongeoorloofde toegang tot een netwerk zijn reële risico's waarvan gebruikers zich bewust dienen te worden. Ook risico's waaraan geen kwade opzet ten grondslag ligt, zoals menselijk falen of natuurrampen dienen hier in beschouwing te worden genomen.

Daar komt bij dat de beschikbaarheid van elektronische communicatienetwerken van steeds groter vitaal belang is voor andere infrastructuren, zoals de drinkwater- en energievoorziening. De alsmaar toenemende netwerkconvergentie vergroot dus ook de afhankelijkheid en kwetsbaarheid van een (informatie-)samenleving.

Omdat voorkomen beter is dan genezen, is bewustwording in dit kader van cruciaal belang. Het is de taak van de overheid om burgers en bedrijven in de eerste plaats in staat te stellen zich te wapenen tegen bepaalde veiligheidsrisico's. Hier is een belangrijke informatietaak weggelegd voor overheden. Een onderdeel hiervan zou moeten zijn het ontwikkelen van goede gemeenschappelijke definities voor netwerkveiligheid, netwerkintegriteit en informatieveiligheid.

Een computerwaarschuwingssysteem kan dienen om een reeds op handen zijnde aanval of andere bedreiging zo spoedig mogelijk onder controle te krijgen. De bestaande CERT [1]-initiatieven (door overheden en grote bedrijven) zijn een voorbeeld van een dergelijk systeem. Deze initiatieven dienen echter beschikbaar te worden voor iedereen, dus ook voor particulieren en kleine(re) bedrijven. Hier ligt ook een belangrijke taak voor de overheid. Reeds bestaande CERT's dienen te worden uitgebreid en goed te functioneren op het niveau van lidstaten, alvorens initiatieven tot het oprichten van een Europese CERT worden genomen.

Oplossingen en te nemen maatregelen ter verhoging van de veiligheid zijn enkel effectief als iedereen ervan kan profiteren. Anders gezegd: initiatieven ter vergroting van de veiligheid zijn minder effectief als de betreffende spelers kiezen voor verschillende oplossingen, die niet interoperabel zijn. In dit kader is het van cruciaal belang dat er oplossingen komen op basis van open internationale standaarden. Het ontbreekt niet aan standaardiseringsactiviteiten, maar een groot aantal concurrerende normen en specificaties heeft tot versnippering van de markt en niet-interoperabele oplossingen geleid. Oplossingen op basis van *open source*

[1] Computer Emergency Response Team.

software kunnen een bijdrage leveren aan een sneller herstel van fouten en aan een hogere transparantie, hetgeen de veiligheid ten goede komt. Oplossingen ter vergroting van de netwerkveiligheid dienen daarom tot stand te komen in samenspraak met álle relevante sectoren.

Naast het ontwikkelen van maatregelen is het van belang op continue basis en op internationaal niveau te onderzoeken in welke mate de veiligheid in het geding is en hoe effectief bepaalde maatregelen zijn. *Benchmarking* kan een nuttig instrument zijn om constant een vinger aan de pols te houden. Door het globale karakter van elektronische communicatienetwerken en dus ook de veiligheidsrisico's is het noodzakelijk in dialoog te treden met andere landen en instellingen in de wereld om bijvoorbeeld snel op de hoogte te zijn van risico's die spelen of ervaringen uit te wisselen op het gebied van maatregelen en implementatie van beleid.

Gegeven het vaak criminele karakter van bedreigingen van netwerkveiligheid (met uitzondering natuurlijk van eerder genoemde natuurrampen of menselijk falen) dienen beleidsmaatregelen ten aanzien van netwerkveiligheid zoveel mogelijk geplaatst te worden in het kader van de taken van Eurojust, om zo een geharmoniseerd juridisch kader te ontwikkelen voor de opsporing en vervolging van computercriminelen.

CONCLUSIES

De Commissie industrie, externe handel, onderzoek en energie verzoekt de ten principale bevoegde Commissie vrijheden en rechten van de burger, justitie en binnenlandse zaken onderstaande suggesties in de goed te keuren ontwerpresolutie op te nemen:

A. overwegende dat de convergentie van elektronische communicatienetwerken in een hoog tempo plaatsvindt, en dat deze netwerken steeds meer van kritisch economisch en maatschappelijk belang worden,

B. overwegende dat het als gevolg van deze convergentie noodzakelijk is een adequaat beleids- en juridisch kader in de Europese Unie te scheppen, waardoor de handhaving van netwerk- en informatieveiligheid, een cruciale voorwaarde voor de informatiesamenleving, wordt gewaarborgd,

C. overwegende dat oplossingen ter verhoging van de veiligheid enkel effectief zijn als alle betrokken partijen, inclusief de burgers, zich bewust zijn van veiligheidsrisico's en de eigen verantwoordelijkheid ten aanzien van de te nemen voorzorgsmaatregelen,

D. overwegende dat oplossingen ter verhoging van de veiligheid enkel effectief zijn als deze door alle relevante marktspelers worden toegepast, bij voorkeur op basis van open internationale normen,

E. overwegende dat de Computer Emergency Response Teams (CERT's) in de verschillende lidstaten op uiteenlopende wijze te werk gaan, waardoor de samenwerking onnodig complex is,

1. onderstreept de noodzaak van het zo snel mogelijk ontwikkelen van gemeenschappelijke

definities voor netwerkveiligheid, netwerkintegriteit en informatieveiligheid;

2. verwelkomt het voornemen van de Commissie tot de oprichting van een Cyber Security Taskforce en spoort de Raad aan om zo spoedig mogelijk dit voornemen te verwezenlijken en de oprichting van deze task force te bewerkstelligen voor het einde van 2002;

3. vraagt de Commissie om, na zorgvuldig overleg met de lidstaten en de privé-sector, de doelstellingen, taken en verantwoordelijkheden van de op te richten task force helder te formuleren en te zorgen voor voldoende personele en financiële middelen voor de task force;

4. beveelt de Commissie aan de task force in ieder geval de functie van onafhankelijk Europees competentiecentrum op het gebied van netwerk en informatieveiligheid toe te bedelen, zodat de task force o.a. kan fungeren als vraagbaak voor lidstaten voor wat betreft het formuleren van nationaal beleid en als onafhankelijke adviseur voor lidstaten en de privé sector, en zodat de task force onafhankelijk onderzoek kan doen op het gebied van netwerk- en informatieveiligheid;

5. onderstreept dat er zo snel mogelijk voor moet worden gezorgd dat alle burgers, bedrijven en administraties toegang hebben tot de openbare elektronische diensten van alle communautaire instellingen, via een systeem van beveiligde en persoonlijke toegang met authenticatie, die moet worden gegarandeerd aan de hand van het gebruik van de elektronische handtekening en de bepaling van Europese normen die voor de EU-instellingen onmiddellijk van kracht moeten worden;

6. roept de Commissie op het initiatief te nemen om de bewustwording van veiligheidsrisico's op elektronische communicatienetwerken bij burgers, bedrijven en de publieke sector te vergroten en een voortrekkersrol te spelen in de coördinatie en inhoudelijke afstemming van voorlichtingscampagnes in de lidstaten over veiligheidsaspecten- en risico's van elektronische communicatienetwerken en beveelt de Commissie aan deze taak primair in handen te leggen van de op korte termijn op te richten Cyber Security Task Force;

7. verzoekt de Commissie een actieplan op te stellen ter bevordering van het gebruik van de digitale handtekening, bijvoorbeeld via het vastleggen van Europese normen die voor de communautaire instellingen onmiddellijk van kracht moeten worden;

8. benadrukt het belang van het betrekken van de relevante sectoren bij het ontwikkelen van beleid voor netwerkveiligheid, netwerkintegriteit en informatieveiligheid in relatie tot IP-omgevingen;

9. verwelkomt het voornemen van de Commissie samen met de lidstaten te onderzoeken hoe de inzameling van gegevens, de analyse en de planning van preventieve maatregelen tegen de huidige en nieuwe veiligheidsrisico's het best kunnen worden georganiseerd;

10. nodigt Commissie en Raad uit deze discussie zoveel mogelijk te plaatsen in het kader van de taken van Eurojust om een geharmoniseerd juridisch kader te ontwikkelen voor de opsporing en vervolging van computercriminelen.