

EUROPÄISCHES PARLAMENT

1999



2004

Sitzungsdokument

ENDGÜLTIG
A5-0311/2002

17. September 2002

BERICHT

über die Mitteilung der Kommission an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen
„Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz“
(KOM(2001)298 – C5-0657/2001 – 2001/2280(COS))

Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere
Angelegenheiten

Berichterstatlerin: Elena Ornella Paciotti

INHALT

	Seite
GESCHÄFTSORDNUNGSSEITE	4
ENTSCHLIESSUNGSANTRAG.....	5
BEGRÜNDUNG.....	11
STELLUNGNAHME DES AUSSCHUSSES FÜR INDUSTRIE, AUSSENHANDEL, FORSCHUNG UND ENERGIE.....	14

GESCHÄFTSORDNUNGSSEITE

Mit Schreiben vom 7. Juni 2001 übermittelte die Kommission dem Europäischen Parlament ihre Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz“ (KOM(2001)298 – 2001/2280(COS)).

In der Sitzung vom 13. Dezember 2002 gab die Präsidentin des Europäischen Parlaments bekannt, dass sie diese Mitteilung an den Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten als federführenden Ausschuss sowie an den Ausschuss für Recht und Binnenmarkt und den Ausschuss für Industrie, Außenhandel, Forschung und Energie sowie an den Ausschuss für Kultur, Jugend, Bildung, Medien und Sport als mitberatende Ausschüsse überwiesen hat (C5-0657/2001).

Der Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten benannte in seiner Sitzung vom 10. Oktober 2001 Elena Ornella Paciotti als Berichterstatterin.

Er prüfte die Mitteilung der Kommission und den Berichtsentwurf in seinen Sitzungen vom 23. Mai 2002, 17. Juni 2002, 8. Juli 2002 und 12. September 2002.

In der letztgenannten Sitzung nahm der Ausschuss den Entschließungsantrag mit 27 Stimmen bei 1 Gegenstimme und 2 Enthaltungen an.

Bei der Abstimmung waren anwesend: Jorge Salvador Hernández Mollar, Vorsitzender; Robert J.E. Evans, stellvertretender Vorsitzender; Giacomo Santini, stellvertretender Vorsitzender; Elena Ornella Paciotti, Berichterstatterin; Niall Andrews, Roberta Angelilli, Alima Boumediene-Thiery, Marco Cappato (in Vertretung von Mario Borghezio), Michael Cashman, Charlotte Cederschiöld, Ozan Ceyhan, Carlos Coelho, Gérard M.J. Deprez, Giuseppe Di Lello Finuoli, Adeline Hazan, Anna Karamanou (in Vertretung von Martin Schulz), Timothy Kirkhope, Eva Klamm, Alain Krivine (in Vertretung von Ole Krarup), Bill Newton Dunn, José Ribeiro e Castro, Martine Roure, Miet Smet (in Vertretung von Hubert Pirker), Patsy Sörensen, The Earl of Stockton (in Vertretung von The Lord Bethell), Joke Swiebel, Fodé Sylla, Anna Terrón i Cusí, Maurizio Turco, Christian Ulrik von Boetticher und Olga Zrihen Zaari (in Vertretung von Walter Veltroni).

Die Stellungnahme des Ausschusses für Industrie, Außenhandel, Forschung und Energie ist diesem Bericht beigelegt; der Ausschuss für Recht und Binnenmarkt hat am 27. November 2001 beschlossen, keine Stellungnahme abzugeben; der Ausschuss für Kultur, Jugend, Bildung, Medien und Sport hat am 21. November 2001 beschlossen, keine Stellungnahme abzugeben.

Der Bericht wurde am 17. September 2002 eingereicht.

ENTSCHLIESSUNGSANTRAG

Entschließung des Europäischen Parlaments zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz“ (KOM(2001)298 – C5-0657/2001 – 2001/2280(COS))

Das Europäische Parlament,

- in Kenntnis der Mitteilung der Kommission (KOM(2001)298 – C5-0657/2001)¹,
- in Kenntnis der Empfehlung betreffend die Strategie zur Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität vom 6. September 2001 sowie der am 26. November 2001 in Budapest unterzeichneten Konvention des Europarates über Cyber-Kriminalität²,
- in Kenntnis des Rahmenbeschlusses des Rates über Angriffe auf Informationssysteme vom 19. April 2002, der die entsprechenden Aspekte der oben genannten Konvention des Europarates in die Tat umsetzt (KOM(2002)173,
- in Kenntnis der Schlussfolgerungen des Europäischen Rates von Stockholm vom März 2001 und von Sevilla vom 21./22. Juni 2002 und der Mitteilung der Kommission „eEuropa 2005: eine Informationsgesellschaft für alle“, die die Dringlichkeit hervorheben, die Sicherheit der Netze zu gewährleisten,
- in Kenntnis der anderen diesbezüglichen Entschließungen einschließlich der Entschließung vom 5. September 2001 zur Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) und der jüngsten internationalen Initiativen (G8, OSZE, UNO)³,
- gestützt auf Artikel 47 Absatz 1 seiner Geschäftsordnung,
- in Kenntnis des Berichts des Ausschusses für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten und der Stellungnahme des Ausschusses für Industrie, Außenhandel, Forschung und Energie (A5-0311/2002),

Die Bedeutung sicherer Netze in der Informationsgesellschaft

- A. in der Erwägung, dass die Konvergenz der elektronischen Kommunikationsnetze in hohem Tempo erfolgt, und dass diese Netze in immer stärkerem Maße von kritischer Bedeutung für Wirtschaft und Gesellschaft werden,
- B. in der Erwägung, dass es infolge dieser Konvergenz notwendig ist, einen

¹ ABl. C 43 vom 16.2.2002, S. 2.

² Angenommene Texte (P5_TPROV(2001)0284.

³ Angenommene Texte (P5_TPROV(2001)0264.

angemessenen politischen und rechtlichen Rahmen in der Europäischen Union zu schaffen, mit dem die Erhaltung der Netz- und Informationssicherheit, eine wesentliche Voraussetzung für die Informationsgesellschaft, gewährleistet wird,

- C. in der Erwägung, dass eine angemessene Sicherheit der Netze einen Schlüsselfaktor für die Entwicklung der Netzdienste, des elektronischen Geschäftsverkehrs und für das gute Funktionieren des Binnenmarktes darstellt;
 - D. in der Erwägung, dass Lösungen zur Erhöhung der Sicherheit nur dann wirksam sind, wenn alle Betroffenen (öffentliche Behörden, Verbraucher, Wissenschaftler an Universitäten, Unternehmen), auch die Bürger, sich der Sicherheitsrisiken sowie der eigenen Verantwortung im Hinblick auf die zu treffenden Vorsorgemaßnahmen bewusst sind,
 - E. in der Erwägung, dass alle Lösungen zur Erhöhung der Sicherheit nur dann wirksam sind, wenn diese von allen relevanten Marktteilnehmern angewandt werden, vorzugsweise auf der Grundlage offener internationaler Normen,
 - F. in der Erwägung, dass die „Computer Emergency Response Teams“ (CERT) in den einzelnen Mitgliedstaaten unterschiedlich vorgehen, wodurch die Zusammenarbeit unnötig erschwert wird,
1. hebt hervor, dass diese Sicherheit unzureichend ist, da 60% der europäischen Unternehmen in den letzten zwei Jahren bereits ernste Probleme hatten, dass nur 14% davon eine Politik der Netzsicherheit verfolgt und dass die fehlende Sicherheit das Haupthindernis für die Nutzung des Internet für 62% der KMU und für 81% der großen Unternehmen ist¹;
 2. hebt ferner hervor, dass die Nutzer häufig nicht in der Lage zu sein scheinen, sich vor den Bedrohungen der Netzsicherheit zu schützen, zu denen absichtliche Angriffe und unbeabsichtigte Schäden gehören wie z.B.:
 - Abhören des ans Festnetz gebundenen und des drahtlosen Fernmeldeverkehrs über elektronische SOTA-Überwachungssysteme, Router, Gateways und Netzserver; nicht autorisierter Zugang durch das Entschlüsseln von *Passwords* oder die Täuschung/Irreführung des Benutzers,
 - Störung von Netzen aufgrund von Angriffen auf *Server*, *Router* oder Angriffe in Form von „Flooding“ oder „Denial of Service“ sowie Angriffe auf die Integrität der Daten mittels bössartiger Software wie z.B. Viren, die Daten verändern oder zerstören,
 - Risiken unabsichtlicher Handlungen und Umweltereignisse (wie z.B. Naturkatastrophen),
 - kriminelle Angriffe, die in bestimmten Fällen auch auf terroristische Zwecke zurückzuführen sind;

¹ ESTO „Future Bottlenecks in the information society“, Bericht für das EP, ITRE, S. 143, und Eurostat.

3. nimmt die Tatsache zur Kenntnis, dass von den Angriffen auf die Netze die wesentlichen Infrastrukturen betroffen sein können wie z.B. im Bereich Verkehr, Kommunikation, Energie- und Wasserversorgung, Finanzdienstleistungen und Banken und dass folglich die Anfälligkeit der Netze ein ernstes Risiko für das korrekte Funktionieren der Wirtschaft der Union und des Alltags der Bürger darstellt;
4. hält angesichts dieser Schwächen eine Antwort allein auf der Grundlage eines freiwilligen Handelns der betroffenen Akteure wegen der Heterogenität ihres Verhaltens, des Fehlens gemeinsamer Standards und der raschen Weiterentwicklung der Technologien für unzureichend; betont gleichzeitig, dass die Hersteller sichere Erzeugnisse entwickeln und sich an der Entwicklung im Bereich der Produktsicherheit beteiligen sollten;
5. unterstreicht die Notwendigkeit, so bald wie möglich zu gewährleisten, dass alle Bürger, Unternehmen und Verwaltungen Zugang zu den öffentlichen elektronischen Diensten aller EU-Verwaltungen haben, im Rahmen eines sicheren und individuellen authentifizierten Zugangssystems, das durch die Verwendung der digitalen Unterschrift und die Festlegung europäischer Normen, die bei den Organen der Union unverzüglich in Kraft treten sollten, zu gewährleisten ist;
6. betont die Bedeutung der Teilhabe der relevanten Sektoren an der Entwicklung einer Politik für Netzsicherheit, Netzintegrität und Informationssicherheit in Bezug auf das IP-Umfeld;
7. nimmt die wachsende Zahl öffentlicher und privater Initiativen auf internationaler Ebene zur Gewährleistung der Verlässlichkeit der Netze wie das White House Office of Cyberspace Security in den Vereinigten Staaten, das im Rahmen der G8 eingerichtete Netz für den Informationsaustausch über die Sicherheit, und die Europol und Interpol-Netze zur Kenntnis;
8. teilt mit dem Europäischen Rat, dem Rat und der Kommission die Ansicht, dass ein europäisches Vorgehen notwendig ist, um zu gewährleisten, dass der Binnenmarkt der Kommunikationsdienste Nutzen aus den Vorteilen der gemeinsamen Lösungen ziehen und weltweit effizient tätig sein kann;
9. weist darauf hin, dass die für die Bereitstellung der Netzdienste Verantwortlichen bereits auf der Grundlage von Artikel 17 der allgemeinen Richtlinie zum Datenschutz (95/46/EG) und einer erneuten Bekräftigung in den anschließenden Vorschriften über die Sicherheit und die Integrität der Netze¹ gehalten sind, die Maßnahmen zur Gewährleistung eines angemessenen Schutzes personenbezogener Daten zu ergreifen;
10. unterstreicht die Notwendigkeit einer möglichst raschen Entwicklung gemeinsamer Definitionen für Netzsicherheit, Netzintegrität und Informationssicherheit;
11. fordert die Kommission auf, einen Aktionsplan zur Förderung der digitalen Unterschrift auszuarbeiten, zum Beispiel durch die Festlegung europäischer Normen, die gegenüber

¹ Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, Richtlinie 97/33/EG über die Zusammenschaltung, Richtlinie 98/10/EG über den Sprachtelefondienst, Richtlinie 99/93/EG über elektronische Signaturen und Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr.

den Organen der EU unverzüglich in Kraft treten sollten;

Institutionelle Aspekte

12. fordert die Kommission auf, dem Parlament und dem Rat die Informationen über die bei der Anwendung der bestehenden Richtlinien im Bereich des Datenschutzes aufgetretenen Probleme, insbesondere im Zusammenhang mit den Artikeln über die Netzsicherheit, zur Verfügung zu stellen;
13. hält die Festlegung einer europäischen Strategie für unaufschiebbar, die zwar, was die verwendete Art von Technologie angeht, neutral ist, aber:
 - a) die Standards für die Sicherheit der Telekommunikationsnetze festlegt oder aktualisiert und ihre Interoperabilität sicherstellt,
 - b) die Entwicklung von Verschlüsselungs- und Zertifizierungssystemen auf europäischer Ebene fördert und die Maßnahmen zum Datenschutz intensiviert,
 - c) die wirkungsvolle Verbrechensvorbeugung und -bekämpfung unter Achtung der Rechtsgarantien sicherstellt,
 - d) die Bürger, Nutzer und öffentlichen und privaten Anbieter mit Informationskampagnen auf nationaler und europäischer Ebene sensibilisiert und die Verbreitung der bewährtesten Praktiken in diesem Bereich fördert,
 - e) die wissenschaftliche Forschung in den am wenigsten entwickelten Sektoren wie z.B. Bewertung der Sicherheit der EDV-Technologien, ihre Integration in das System, Schutz des Endnutzers und Technologien zur Verbesserung des Schutzes der Privatsphäre intensiviert und dabei Systeme wie Anti-Echelon, Magic Latern, Carnivore einbezieht;
14. stimmt mit der Kommission darin überein, dass unverzüglich eine für die Sicherheit der Netze zuständige *Taskforce* eingerichtet werden muss, die folgende Zielsetzungen verfolgt:
 - Ermittlung der für die Verwaltung der Netze zuständigen nationalen Behörden
 - Festlegung der für die Koordinierung zuständigen einzelstaatlichen Behörden und der Befehlskette für die Krisenverwaltung bei Gefahren für die Gemeinschaft und die elektronische Infrastruktur,
 - Koordinierung der Tätigkeiten dieser Behörden und Austausch der bewährtesten Praktiken
 - Einrichtung eines für die Vorbeugung und den Informationsaustausch zuständigen hochspezialisierten Zentrums
 - Sammlung und Analyse von Daten über die Probleme im Zusammenhang mit der

Sicherheit der Netze

- Analyse der derzeitigen und künftigen Risiken für die Sicherheit
- Veranstaltung von Diskussionsforen auf europäischer Ebene unter Beteiligung aller, die die Sicherheit etwas angeht (öffentliche Behörden, Verbraucher, Universitätsforscher, Unternehmen);

15. fordert die Kommission auf, darauf zu achten, dass diese Taskforce bei ihrer Arbeit das bereits auf dem Forum Cyberkriminalität Dargelegte berücksichtigt und das Forum in die künftige Arbeit einbezieht;
16. ersucht die Kommission, nach eingehender Konsultation der Mitgliedstaaten und des Privatsektors, Ziele, Aufgaben und Zuständigkeiten der zu gründenden Taskforce klar zu formulieren und für genug Personal und ausreichende finanzielle Mittel für die Taskforce zu sorgen;
17. fordert die Kommission auf, vorrangig den Sicherheitsbedarf zu prüfen und die Forschung an Frühwarnsystemen der elektronischen Infrastruktur der Netze umzusetzen, die
 - a) der Bereitstellung wesentlicher Infrastrukturen, öffentlicher Versorgungsdienstleistungen und Dienstleistungen im Interesse der Volksgesundheit dienen,
 - b) Frühwarnsysteme und deren Zusammenwirken,
 - c) die Entwicklung der „Regierung am Netz“ und des elektronischen Geschäftsverkehrs zu fördern;

(Der Aufbau dieses Änderungsantrags ist nicht logisch. Falls er angenommen werden sollte, muss er umgearbeitet werden. Anmerkung d. Übers.)

18. ist der Ansicht, dass sich die Union bei einem ersten legislativen Schritt in diesem Bereich auf die ihr zuerkannten Befugnisse auf dem Gebiet der transeuropäischen Netze (Titel XV EGV) und bei den einer Harmonisierung bedürftigen Aspekten auf die im Bereich des Binnenmarkts (Artikel 95 EGV) stützen sollte. Die Einsetzung einer *Taskforce* sollte in der gleichen Regelung vorgesehen werden, die die Zielsetzungen auf europäischer Ebene festlegt;
19. fordert die Kommission auf, unverzüglich eine Bewertung der finanziellen Auswirkungen des Tätigwerdens der Union in diesem Sektor vorzulegen und vergleichende Daten über ähnliche Initiativen auf Ebene der Mitgliedstaaten oder von Drittstaaten (z.B. USA) zu liefern;
20. unterstützt den Europäischen Rat, den Rat und die Kommission hinsichtlich der Notwendigkeit eines europäischen Herangehens für neue Rechtsvorschriften oder Änderungen bestehender Rechtsvorschriften über Untersuchungsbefugnisse, Verfolgung und Strafen für kriminelle oder terroristische Aktivitäten gegen kritische Infrastrukturen;

21. fordert die Kommission und den Rat auf, diese Diskussion so weit wie möglich im Rahmen der Aufgaben von Eurojust zu führen, um einen harmonisierten Rechtsrahmen für die Ermittlung und Ahndung von Computerkriminalität zu entwickeln;
22. beauftragt seinen Präsidenten, diese Entschliebung dem Rat und der Kommission, den Regierungen und Parlamenten der Mitgliedstaaten und dem Europarat zu übermitteln.

BEGRÜNDUNG

Einleitung

Die Mitteilung über die Sicherheit der Netze ist ein Jahr alt und zielt darauf ab, eine globale Strategie für die Sicherheit der elektronischen Netze entsprechend der Forderung des Europäischen Rats von Stockholm vom 23. und 24. März 2001 festzulegen. Die Mitteilung entwickelt somit die vorangegangene Mitteilung der Kommission „Sicherheit und Vertrauen in elektronische Kommunikation“ vom 8. Oktober 1997 (KOM(1997) 503) weiter.

Der vorgeschlagene Ansatz ergänzt die Rahmenmitteilung über die Cyberkriminalität vom 22. Januar 2001 und wurde auf der Tagung des Rates der Telekommunikationsminister vom 6. Dezember 2001 übernommen und vertieft, der eine detaillierte Entschließung angenommen hat; außerdem wurde dieser Ansatz um den Vorschlag der Kommission für einen Rahmenbeschluss über Angriffe auf Informationssysteme vom 19. April 2002 bereichert.

Der Europäische Rat von Barcelona vom März 2002 hatte die Kommission aufgefordert, einen neuen Aktionsplan e-Europe 2005 auszuarbeiten, der sich auch mit der Sicherheit der Netze und der Informationen in einer Pfeilerübergreifenden Perspektive befassen sollte. Die Kommission hat diesen Plan dem Europäischen Rat von Sevilla vom 21./22. Juni 2002 vorgelegt, welcher ihn angenommen hat.

Derzeitiger Stand der Rechtsvorschriften der Gemeinschaft und Perspektiven

Der Gesetzgeber der Gemeinschaft hat bereits auf dem Gebiet der Sicherheit der Netze in drei grundlegenden Sektoren Maßnahmen getroffen:

a) Datenschutz: Insbesondere mit der **Richtlinie 95/46/EG** zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Artikel 17) und mit der **Richtlinie 97/66/EG** des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (Artikel 4 und 5), die durch die vom Rat am 25. Juni 2002 verabschiedete Richtlinie ersetzt wird – Bericht Cappato A5-0130/2002).

b) Maßnahmen im Bereich der Telekommunikation: Das Bemühen um eine größere Sicherheit der Netze bildet auch die Grundlage für die in **Richtlinie 99/93/EG** des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen und der **Richtlinie 2000/31/EG** über den elektronischen Geschäftsverkehr. Ein weiterer Aspekt im Zusammenhang mit der Sicherheit der Netze betrifft ihren Schutz vor Naturkatastrophen oder umfassenden Schäden (**Richtlinie 97/33/EG** über die Zusammenschaltung, Artikel 10, und **Richtlinie 98/10/EG** über den Sprachtelefondienst, Artikel 13).

c) Bekämpfung der Computerkriminalität: Ein spezifischer Aspekt der Sicherheit der Netze betrifft die Bekämpfung der Internetkriminalität. Die diesbezüglichen Bezugstexte sind die **Mitteilung der Kommission** über die Computerkriminalität (KOM(2000) 890); die **Empfehlung des Rates** vom 25. Juni 2001 über Kontaktstellen mit einem rund um die Uhr erreichbaren Dauerdienst zur Bekämpfung der Hightech-Kriminalität, der **Vorschlag für**

einen Rahmenbeschluss des Rates über Angriffe auf Informationssysteme (KOM(2002) 173).

In der Mitteilung wird vorgeschlagen, die drei oben genannten Aspekte in einer integrierten Strategie miteinander zu verbinden und so einen groß angelegten Rahmen für Maßnahmen vorzusehen, die von

- ♦ der Sensibilisierung der Öffentlichkeit, auch da sie nicht in der Lage ist, sich zu schützen, bis zu spezifischeren Maßnahmen reichen wie z.B.:
- ♦ Schaffung eines europäischen Systems zur Warnung vor und zur Analyse von Problemen;
- ♦ Förderung der Forschung im Bereich der Sicherheit;
- ♦ Standardisierung und Zertifizierung;
- ♦ freier Verkehr von Verschlüsselungsprodukten;
- ♦ Sicherheit bei der Anwendung durch staatliche Stellen;
- ♦ internationale Zusammenarbeit.

Rechtfertigung einer Gemeinschaftsmaßnahme

In den Vereinigten Staaten hat der Privatsektor eine Initiativrolle mit Selbstregulierungsmechanismen wie z.B. Verhaltenskodizes und Sicherheitsprogrammen übernommen. Der Privatsektor hat nämlich ein Interesse an der Förderung eines Klimas des Vertrauens in die Nutzung der Netze und in eine möglichst geringe legislative Intervention.

Das Konzept der Freiwilligkeit ist jedoch nicht immer ausreichend, um die Sicherheit zu gewährleisten, darüber hinaus entsprechen die von privater Seite dargelegten Pläne mehr den Markterfordernissen als dem Schutz der Grundrechte der Bürger. Außerdem übernehmen Privatleute, z.B. Verkäufer von *Software*, keine Schäden, die sich aus ihrem Verhalten in Bezug auf die Sicherheit ergeben. So stellt die Kommission in ihrer Mitteilung fest, dass „Benutzer und Lieferanten mit niedrigem Sicherheitsniveau nicht für Schäden Dritter haften“. Aus diesem Grund hat die Europäische Union einen legislativen Ansatz gewählt. Es wird damit bezweckt, eine Kultur der Sicherheit zu entwickeln und den Austausch sicherer Informationen zu fördern, indem die Instrumente genutzt werden, die es bereits auf dem Markt gibt, die aber nicht bekannt genug oder untereinander nicht kompatibel sind.

Die Maßnahme der Gemeinschaft ist auch deshalb gerechtfertigt, weil die Kommunikations- und Informationsdienste grenzübergreifend sind, ebenso wie die Gefahren, die für die Sicherheit bestehen. Eine europäische strategische Aktion ist erforderlich, um die Entwicklung des elektronischen Geschäftsverkehrs zu unterstützen und einen echten Binnenmarkt der Telekommunikations- und Informationsdienste zu schaffen, der die gemeinsamen Lösungen nutzen und international wirkungsvoll operieren kann. Die Schaffung z.B. des Bereichsnamens für das europäische Internet vom Typ .EU hat nicht nur die Bedeutung, die europäische Präsenz im Cyberspace zu bekräftigen, sondern ist vor allem auch eine Gelegenheit, auf diesem Wege den Raum des Vertrauens zu vermitteln, den die EU dank des Binnenmarkts geschaffen hat.

Von der Kommission vorgeschlagene Aktionen

Das Europäische Parlament unterstützt die Kommission in ihrer Absicht, eine *Taskforce* für Computersicherheit einzurichten, die ihre Tätigkeit Mitte 2003 aufnehmen sollte. Das Parlament fordert die Kommission jedoch auf, zu berücksichtigen, dass die legislative Intervention in diesem Bereich als Rechtsgrundlage Titel XV des EG-Vertrags über die transeuropäischen Netze und für die Aspekte, die eine Angleichung der Rechtsvorschriften erforderlich machen, Artikel 95 EGV im Bereich des Binnenmarkts heranziehen sollte.

Das Europäische Parlament wäre auf diese Weise voll und ganz am Entscheidungsprozess in einem Bereich beteiligt, der für die Interessen der Bürger, die es vertritt, von so großer Bedeutung ist.

Glossar:

Server: ist ein rechnerfernes Programm, das dem Nutzer Informationen bereitstellt. Er dient nur der Datenhaltung, dem Auffinden und Übermitteln von Daten an den Nutzer, der sie angefragt hat. Benötigt der Nutzer ein an einem bestimmten Netzknoten befindliches Dokument, so sendet er über das Internet eine Anfrage an den Server. Der *Server* sucht nach Eingang der Anfrage die gewünschten Daten und leitet sie an den Computer des Nutzers weiter.

Gateway (Portal): verbindet alle Computer des Netzes (z.B. ein betriebsinternes Netz) mit dem Internet und nützt dabei jede Art von Verbindung.

Router: ist ein System oder ein Programm im Computer, das den nächstgelegenen Punkt des Netzes bestimmt, an den der Nutzer sich wendet, um Informationen zu erhalten. Der *Router* ist mit mindestens zwei Netzen verbunden und entscheidet, auf welchem Netz die Informationen gesendet werden, wobei er sich auf die Beurteilung des derzeitigen Standes der Netze stützt, mit denen er verbunden ist. Der *Router* befindet sich in jedem Portal (*Gateway*).

29. Mai 2002

STELLUNGNAHME DES AUSSCHUSSES FÜR INDUSTRIE, AUSSENHANDEL, FORSCHUNG UND ENERGIE

für den Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere
Angelegenheiten

zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Wirtschafts-
und Sozialausschuss und den Ausschuss der Regionen „Sicherheit der Netze und
Informationen: Vorschlag für einen europäischen Politikansatz“
(KOM(2001) 298 – C5-0657/2001 – 2001/2280 (COS))

Verfasser der Stellungnahme: W.G. van Velzen

VERFAHREN

In seiner Sitzung vom 22. November 2001 benannte der Ausschuss für Industrie,
Außenhandel, Forschung und Energie W.G. van Velzen als Verfasser der Stellungnahme.

Der Ausschuss prüfte den Entwurf einer Stellungnahme in seinen Sitzungen vom 16. April
2002 und 22. Mai 2002.

In der letztgenannten Sitzung nahm er die nachstehenden Schlussfolgerungen einstimmig an.

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

KURZE BEGRÜNDUNG

Die Sicherheit spielt bei allen Aspekten des Alltags eine Rolle. Von den Bürgern und den Unternehmen wird erwartet, dass sie zuallererst ihre eigene Verantwortung hinsichtlich der Sicherheit ihrer eigenen Person und die ihrer (unmittelbaren) Umgebung kennen und übernehmen. Dies gilt daher auch für elektronische Kommunikationsnetze.

Disruptive Angriffe auf das Internet sind inzwischen recht verbreitet. Sich schnell verbreitende Viren über E-Mail haben in kurzer Zeit viele Benutzer für dieses Risiko sensibilisiert und ihnen die Anfälligkeit ihrer Computersysteme vor Augen geführt. Gleichzeitig wird die Konvergenz elektronischer Kommunikationsnetze mit Hochdruck betrieben. Es ist daher von Bedeutung, dass sowohl die Netzwerkkonvergenz als auch den möglichen Sicherheitsrisiken schneller bekannt werden.

Neben den mittlerweile bekannten Computerviren gibt es noch zahlreiche weitere Sicherheitsrisiken auf dem Gebiet der elektronischen Kommunikationsnetze.

Nicht nur die Viren, die über E-Mail verbreitet werden, sondern auch das Abhören von Nachrichten, die Fälschung der Identität oder der unberechtigte Zugang zu einem Netz sind reale Risiken, deren sich die Benutzer bewusst werden müssen. Auch die Risiken, denen keine böse Absicht zugrunde liegt, wie menschliches Versagen oder Naturkatastrophen, müssen hier berücksichtigt werden.

Hinzu kommt, dass die Verfügbarkeit elektronischer Kommunikationsnetze von immer wesentlicher Bedeutung ist für andere Infrastrukturen, wie zum Beispiel die Trinkwasser- und Energieversorgung. Die stets zunehmende Netzwerkkonvergenz erhöht daher auch die Abhängigkeit und die Anfälligkeit einer (Informations-)Gesellschaft.

Da Vorbeugen besser ist als Heilen, ist die Sensibilisierung in diesem Rahmen von wesentlicher Bedeutung. Es ist die Aufgabe des Staates, dafür zu sorgen, dass Unternehmen und Bürger in der Lage sind, sich gegen bestimmte Sicherheitsrisiken zu wappnen. Dies ist eine wichtige Informationsaufgabe für die Behörden. Ein Teil dieser Aufgabe bestünde in der Entwicklung vernünftiger gemeinsamer Definitionen von Netzsicherheit, Netzintegrität und Informationssicherheit.

Ein Computerwarnsystem kann dazu dienen, einen bevorstehenden Angriff oder eine andere Bedrohung so rasch wie möglich unter Kontrolle zu bekommen. Die bestehenden CERT¹-Initiativen (von Seiten der Behörden und großen Unternehmen) sind ein Vorbild für ein solches System. Diese Initiativen müssen jedoch für jeden zugänglich sein, also auch für Privatpersonen und kleine bzw. kleinere Unternehmen. Auch dies ist eine wichtige Aufgabe für den Staat. Bereits existierende CERT müssen ausgeweitet werden und müssen auf der Ebene der Mitgliedstaaten gut funktionieren, bevor Initiativen zur Gründung eines europäischen CERT ergriffen werden.

Lösungen und Maßnahmen zur Erhöhung der Sicherheit sind nur dann wirksam, wenn jeder davon profitieren kann. Mit anderen Worten, Initiativen zur Erhöhung der Sicherheit sind weniger wirksam, wenn die Betroffenen sich für unterschiedliche Lösungen entscheiden, die nicht kompatibel sind. In diesem Rahmen ist es von wesentlicher Bedeutung, dass Lösungen

¹ Computer Emergency Response Team

auf der Grundlage offener internationaler Normen gefunden werden. Es fehlt nicht an Normungsaktivitäten, eine große Zahl konkurrierender Normen und Spezifikationen hat jedoch zu einer Zersplitterung des Marktes und zu inkompatiblen Lösungen geführt. Lösungen auf der Grundlage einer „Open-Source“-Software können einen Beitrag im Hinblick auf eine raschere Fehlerbeseitigung und eine höhere Transparenz leisten, was wiederum der Sicherheit zugutekommt.

Lösungen zur Erhöhung der Netzsicherheit müssen daher gemeinsam mit allen relevanten Sektoren erfolgen.

Zusätzlich zu der Entwicklung von Maßnahmen ist es von Bedeutung, regelmäßig und auf internationaler Ebene zu prüfen, in wie weit die Sicherheit betroffen ist und wie wirksam bestimmte Maßnahmen sind. Benchmarking kann ein sinnvolles Instrument sein, um diesen Aspekt dauerhaft im Auge zu behalten. Aufgrund des globalen Charakters der elektronischen Kommunikationsnetze und daher auch der Sicherheitsrisiken ist es notwendig, mit anderen Ländern und Institutionen in der Welt einen Dialog einzugehen, um z.B. rasch über Risiken informiert zu werden, oder Erfahrungen auf dem Gebiet der einschlägigen Maßnahmen und der Umsetzung des Politikansatzes auszutauschen.

Angesichts des oft kriminellen Charakters der Bedrohung der Netzsicherheit (natürlich mit Ausnahme der oben genannten Naturkatastrophen oder des menschlichen Versagens) müssen politische Maßnahmen im Hinblick auf die Netzsicherheit möglichst im Rahmen der Aufgaben von Eurojust erfolgen, um auf diese Weise einen harmonisierten Rechtsrahmen für die Ermittlung und Ahndung der Computerkriminalität zu entwickeln.

SCHLUSSFOLGERUNGEN

Der Ausschuss für Industrie, Außenhandel, Forschung und Energie ersucht den federführenden Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten, folgende Punkte in seinen Entschließungsantrag zu übernehmen:

- A. in der Erwägung, dass die Konvergenz der elektronischen Kommunikationsnetze in hohem Tempo erfolgt, und dass diese Netze in immer stärkerem Maße von kritischer Bedeutung für Wirtschaft und Gesellschaft werden,
- B. in der Erwägung, dass es infolge dieser Konvergenz notwendig ist, einen angemessenen politischen und rechtlichen Rahmen in der Europäischen Union zu schaffen, mit dem die Erhaltung der Netz- und Informationssicherheit, eine wesentliche Voraussetzung für die Informationsgesellschaft, gewährleistet wird,
- C. in der Erwägung, dass Lösungen zur Erhöhung der Sicherheit nur dann wirksam sind, wenn alle Betroffenen, auch die Bürger, sich der Sicherheitsrisiken sowie der eigenen Verantwortung im Hinblick auf die zu treffenden Vorsorgemaßnahmen bewusst sind,
- D. in der Erwägung, dass alle Lösungen zur Erhöhung der Sicherheit nur dann wirksam sind, wenn diese von allen relevanten Marktteilnehmern angewandt werden, vorzugsweise auf der Grundlage offener internationaler Normen,
- E. in der Erwägung, dass die „Computer Emergency Response Teams“ (CERT) in den

einzelnen Mitgliedstaaten unterschiedlich vorgehen, wodurch die Zusammenarbeit unnötig erschwert wird,

1. unterstreicht die Notwendigkeit einer möglichst raschen Entwicklung gemeinsamer Definitionen für Netzsicherheit, Netzintegrität und Informationssicherheit;
2. begrüßt das Vorhaben der Kommission, eine Taskforce „Cyber Security“ zu bilden, und fordert den Rat nachdrücklich auf, dieses Vorhaben so bald wie möglich zu verwirklichen und die Bildung dieser Taskforce bis Ende 2002 abzuschließen;
3. ersucht die Kommission, nach eingehender Konsultation der Mitgliedstaaten und des Privatsektors, Ziele, Aufgaben und Zuständigkeiten der zu gründenden Taskforce klar zu formulieren und für genug Personal und ausreichende finanzielle Mittel für die Taskforce zu sorgen;
4. empfiehlt der Kommission, die Taskforce auf jeden Fall als unabhängiges Kompetenzzentrum auf dem Gebiet der Netz- und Informationssicherheit zu gestalten, damit sie die Mitgliedstaaten bei der Formulierung nationaler politischer Maßnahmen beraten und als unabhängiger Berater für die Mitgliedstaaten und den Privatsektor tätig sein sowie unabhängige Untersuchungen auf dem Gebiet der Netz- und Informationssicherheit durchführen kann;
5. unterstreicht die Notwendigkeit, so bald wie möglich zu gewährleisten, dass alle Bürger, Unternehmen und Verwaltungen Zugang zu den öffentlichen elektronischen Diensten aller EU-Verwaltungen haben, im Rahmen eines sicheren und individuellen authentifizierten Zugangssystems, das durch die Verwendung der digitalen Unterschrift und die Festlegung europäischer Normen, die bei den Organen der Union unverzüglich in Kraft treten sollten, zu gewährleisten ist;
6. fordert die Kommission auf, die Initiative zu ergreifen, um die Sensibilisierung für Sicherheitsrisiken bei elektronischen Kommunikationsnetzen bei Bürgern, Unternehmen und im öffentlichen Sektor zu erhöhen und im Rahmen der elektronischen Kommunikationsnetze bei der Koordinierung und der inhaltlichen Abstimmung von Aufklärungskampagnen in den Mitgliedstaaten über Sicherheitsaspekte und -risiken der elektronischen Kommunikationsnetze eine Vorreiterrolle zu übernehmen, und empfiehlt der Kommission, diese Aufgabe in erster Linie der in Kürze zu errichtenden Taskforce Cyber Security anzuvertrauen;
7. fordert die Kommission auf, einen Aktionsplan zur Förderung der digitalen Unterschrift auszuarbeiten, zum Beispiel durch die Festlegung europäischer Normen, die gegenüber den Organen der EU unverzüglich in Kraft treten sollten;
8. betont die Bedeutung der Teilhabe der relevanten Sektoren an der Entwicklung einer Politik für Netzsicherheit, Netzintegrität und Informationssicherheit in Bezug auf das IP-Umfeld;
9. begrüßt die Absicht der Kommission, gemeinsam mit den Mitgliedstaaten zu prüfen, wie die Datensammlung, die Analyse und die Planung von Vorbeugungsmaßnahmen gegen derzeitige und neu anstehende Sicherheitsrisiken am besten organisiert werden können;

10. fordert die Kommission und den Rat auf, diese Diskussion so weit wie möglich im Rahmen der Aufgaben von Eurojust zu führen, um einen harmonisierten Rechtsrahmen für die Ermittlung und Ahndung von Computerkriminalität zu entwickeln.