Bundesrat Drucksache **926/02**

28.11.02

Unterrichtung

durch das
Europäische Parlament

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"

Zugeleitet mit Schreiben des Generalsekretärs des Europäischen Parlaments - 312825 - vom 26. November 2002. Das Europäische Parlament hat die Entschließung in der Sitzung am 22. Oktober 2002 angenommen.

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 1320, 53003 Bonn
Telefon: 0228/3820840, Telefax: 0228/3820844
ISSN 0720-2946

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),

– unter Hinweis auf seine Empfehlung vom 6. September 2001 betreffend die Strategie zur Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität[1] sowie der am 23. November 2001 in Budapest unterzeichneten Konvention des Europarates über Cyber-Kriminalität,

– in Kenntnis des Vorschlags für einen Rahmenbeschluss des Rates über Angriffe auf Informationssysteme vom 19. April 2002[2], der die entsprechenden Aspekte der oben genannten Konvention des Europarates in die Tat umsetzt,

– in Kenntnis der Schlussfolgerungen des Europäischen Rates von Stockholm vom 23. und 24. März 2001 und von Sevilla vom 21./22. Juni 2002 und der Mitteilung der Kommission „eEuropa 2005: Eine Informationsgesellschaft für alle" (KOM(2002) 263), die die Dringlichkeit hervorheben, die Sicherheit der Netze zu gewährleisten,

– unter Hinweis auf seine anderen diesbezüglichen Entschließungen einschließlich der Entschließung vom 5. September 2001 zur Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon)[3] und der jüngsten internationalen Initiativen (G8, OSZE, UNO),

– 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 sowie 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 grundlegender Bedeutung für Wirtschaft und Gesellschaft werden,

B. in der Erwägung, dass es infolge dieser Konvergenz notwendig ist, einen angemessenen

---

[1] ABl. C 72 E vom 21.3.2002, S. 323.
[2] ABl. C 203 E vom 27.8.2002, S. 109.
[3] ABl. C 72 E vom 21.3.2002, S. 221.

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) und 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 ist[1];

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 Passwörtern 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 bösartiger 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 terroristischen Ursprungs sein können;

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

---

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

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[1] und einer erneuten Bekräftigung in den anschließenden Vorschriften über die Sicherheit und die Integrität der Netze[2] 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 den Organen der Europäischen Union 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

---

[1] ABl. L 281 vom 23.11.1995, S. 31.

[2] Richtlinie 97/66/EG (ABl. L 24 vom 30.1.1998, S. 1); Richtlinie 97/33/EG (ABl. L 199 vom 26.7.1997, S. 32), Richtlinie 98/10/EG (ABl. L 101 vom 1.4.1998, S. 24), Richtlinie 1999/93/EG (ABl. L 13 vom 19.1.2000, S. 12) und Richtlinie 2000/31/EG (ABl. L 178 vom 17.7.2000, S. 1).

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 öffentliche und private 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 all derer, 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 einschließen sowie

    c) die Entwicklung der „Regierung am Netz“ und des elektronischen Geschäftsverkehrs zu fördern;

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 des Vertrags) und bei den einer Harmonisierung bedürfenden Aspekten auf die im Bereich des Binnenmarkts (Artikel 95 des Vertrags) 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;

o

o o

22. beauftragt seinen Präsidenten, diese Entschließung dem Rat und der Kommission, den Regierungen und Parlamenten der Mitgliedstaaten und dem Europarat zu übermitteln.