Europäischer Wirtschafts- und Sozialausschuss

TEN/254
"Eine Strategie für eine sichere Informations-gesellschaft"

Brüssel, den 16. Februar 2006

STELLUNGNAHME

des Europäischen Wirtschafts- und Sozialausschusses
zu der
"Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Eine Strategie für eine sichere Informationsgesellschaft - Dialog, Partnerschaft und Delegation der Verantwortung"
KOM(2006) 251 endg.

_____

Rue Belliard 99 - B-1040 Brüssel - Tel. +32 (0)2 546 90 11 - Fax +32 (0)2 513 48 93 - Internet http://www.eesc.europa.eu

DE

Die Kommission beschloss am 31. Mai 2006, den Europäischen Wirtschafts- und Sozialausschuss gemäß 262 Artikel des EG-Vertrags um Stellungnahme zu folgender Vorlage zu ersuchen:

> *"Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Eine Strategie für eine sichere Informationsgesellschaft - Dialog, Partnerschaft und Delegation der Verantwortung"*
> KOM(2006) 251 endg.

Die mit den Vorarbeiten beauftragte Fachgruppe Verkehr, Energie, Infrastrukturen, Informationsgesellschaft nahm ihre Stellungnahme am 11. Januar 2007 an. Berichterstatter war Herr PEZZINI.

Der Ausschuss verabschiedete auf seiner 433. Plenartagung am 16. Februar 2007 mit 132 Ja-Stimmen bei 2 Stimmenthaltungen folgende Stellungnahme:

*

* *

1. Schlussfolgerungen und Empfehlungen

1.1 Nach Überzeugung des Ausschusses stellt die Informatiksicherheit ein zunehmendes Problem für Unternehmen, Verwaltungen, öffentliche und private Einrichtungen und für die einzelnen Bürger dar.

1.2 Der Ausschuss schließt sich im Wesentlichen den Analysen und Argumenten an, die eine neue Strategie fordern, um die Netz- und Informationssicherheit zu erhöhen und Angriffe und Eindringlinge abwehren, die ja nicht an Staatsgrenzen Halt machen.

1.3 Nach Ansicht des Ausschusses sollte die Kommission weitere Anstrengungen unternehmen, um eine innovative und strukturierte Strategie umzusetzen, die dem Ausmaß des Phänomens und seinen Auswirkungen auf die Wirtschaft und das Privatleben gerecht wird.

1.3.1 Der EWSA weist auch darauf hin, dass die Kommission unlängst eine neue Mitteilung über Computersicherheit vorgelegt hat und demnächst ein neues Dokument zu demselben Thema erwartet wird. Der Ausschuss behält sich vor, künftig eingehender Stellung zu beziehen und dabei alle Mitteilungen zum Thema zu berücksichtigen.

1.4 Der Ausschuss hebt hervor, dass der Aspekt Informatiksicherheit keineswegs von der Stärkung des Datenschutzes und dem Schutz der Freiheiten losgelöst werden darf, die ja in der europäischen Menschenrechtskonvention garantiert sind.

1.5 Der Ausschuss fragt sich, welchen Mehrwert der Vorschlag derzeit bietet, vergleicht man ihn mit dem 2001 beschlossenen integrierten Ansatz, mit dem dasselbe Ziel wie mit der nun vorliegenden Mitteilung verfolgt wurde[1].

1.5.1 Die dem Vorschlag beiliegende Folgenabschätzung[2] enthält gegenüber der Position von 2001 einige interessante Aktualisierungen, wurde jedoch in einer einzigen Sprache verfasst, ist also für viele europäische Bürger nicht verständlich, die sich nach dem eigentlichen Dokument ein Urteil bilden, das in allen Amtssprachen vorliegt.

1.6 Der Ausschuss erinnert an die Schlussfolgerungen des Weltgipfels 2005 in Tunis zur Informationsgesellschaft, die von der UN-Generalversammlung am 27. März 2006 verabschiedet wurden:

- Grundsatz des Zugangs ohne Diskriminierung;
- Einsatz der IKT als Friedensinstrument;
- Instrumente zur Stärkung der Demokratie, der Kohäsion und der *good governance*;
- Verhütung von Missbrauch unter Achtung der Menschenrechte[3].

1.7 Der Ausschuss hebt hervor, dass eine dynamische und integrierte EU-Strategie außer Dialog, Partnerschaft und Verantwortung auch folgendes zu leisten hätte:

- vorbeugende Maßnahmen;
- Übergang von der Informatiksicherheit zur Informatik"versicherung";[4]
- Schaffung eines sicheren und anerkannten EU-Rechtsrahmens, der auch Strafen vorsieht;
- stärkere technische Standardisierung;
- digitale Identifizierung der Nutzer;
- europäische Analysen und Planungen (Foresight) zur Informatiksicherheit mit multimodalen technologischen Konvergenzen;
- stärkere europäische und einzelstaatliche Mechanismen zur Risikoabschätzung;
- Maßnahmen zur Vermeidung der Entstehung von Informatik-Monokulturen;
- stärkere EU-Koordinierung auf europäischer und internationaler Ebene;
- Schaffung einer IKT-Sicherheitsstelle zwischen den Generaldirektionen;
- Schaffung eines "europäischen Netz- und Informationssicherheitsnetzes";
- Optimierung der Rolle der europäischen Informationssicherheitsforschung;
- Einführung eines europäischen Tages der Computersicherheit;

---

1 Vgl. die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu der "Mitteilung der Kommission an den Rat und das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz", ABl. C 48 vom 21.2.2002, S. 33.

2 Eine Folgenabschätzung hat nicht denselben Wert wie ein Strategiepapier.

3 UN-Empfehlungen Nr. 57 und 58 vom 27.3.2006; Schlussdokument Nr. 15 von Tunis.

4 Vgl. "Emerging technologies in the context of security", CCR, Institut für Schutz und Sicherheit der Bürger, Heft für strategische Forschung, September 2005, Europäische Kommission, http://serac.jrc.it.

– EU-Pilotaktionen zur Informatiksicherheit in verschiedenen Schularten.

1.8 Und schließlich macht der EWSA darauf aufmerksam, dass für eine dynamische und integrierte EU-Strategie entsprechende Haushaltsmittel aufgebracht werden müssen und eine solche Strategie Initiativen und verstärkte Koordinierungsmaßnahmen auf Gemeinschaftsebene umfassen muss, die es Europa ermöglichen, international mit einer Stimme zu sprechen.

2. Begründung

2.1 Die Sicherheit der Informationsgesellschaft ist eine grundlegende Herausforderung, wenn es darum geht, das Vertrauen in Kommunikationsnetze und -dienste sowie deren Zuverlässigkeit zu sichern, sind die doch entscheidende Faktoren für die Entwicklung von Wirtschaft und Gesellschaft.

2.2 Informatiknetze und -systeme müssen geschützt werden, um die Wettbewerbs- und Handelsfähigkeit aufrechtzuerhalten, die Integrität und Kontinuität der elektronischen Kommunikation zu gewährleisten, Betrugsfällen vorzubeugen und den rechtlichen Schutz der Privatsphäre sicherzustellen.

2.3 Die elektronische Kommunikation und die damit zusammenhängenden Dienste sind das größte Segment des gesamten Telekommunikationssektors: 2004 haben etwa 90% der europäischen Unternehmen das Internet aktiv genutzt, 65% haben eine eigene Website entwickelt, während Berechnungen zufolge etwa die Hälfte der europäischen Bevölkerung das Internet regelmäßig nutzt und 25% der Haushalte den Breitbandzugang permanent verwenden[5].

2.4 Angesichts einer beschleunigten Investitionsentwicklung macht das Ausgabenvolumen für die Sicherheit nur 5 bis 13% aller Investitionen in die Informationstechnologien aus. Dieser Prozentsatz ist allzu gering. Aktuellen Studien zufolge sind von durchschnittlich 30 Protokollen, die sich die Schlüsselstrukturen teilen, 23 anfällig für Multiprotokoll-Angriffe[6]. Darüber hinaus werden Schätzungen zufolge jeden Tag durchschnittlich 25 Mio. elektronische SPAM[7]-Nachrichten verschickt; daher begrüßt der Ausschuss den unlängst von der Kommission hierzu vorgelegten Vorschlag.

---

5 i2010:a strategy for a secure information society - Factsheet 8 (June 2006), EC Information Society and Media http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-it.pdf.

6 Protokoll der First International Conference on Availability, Reliability and Security (Erste Internationale Konferenz über Verfügbarkeit, Verlässlichkeit und Sicherheit, ARES 2006). Band 00 ARES 2006, Herausgeber: IEEE Computer Society.

7 SPAM = Unerbetene kommerzielle E-Mail. "Spam" bedeutete ursprünglich "spiced pork and ham" (= gewürztes Schweinefleisch und Schinken) in Dosen, das im Zweiten Weltkrieg sehr beliebt war, als es zur Hauptnahrungsquelle der US-Truppen und der Bevölkerung des Vereinigten Königreichs wurde. Nach dem jahrelangen Verzehr des nicht rationierten "spam" hatten die Menschen genug davon.

2.5 Computerviren[8]: Die rasche Ausbreitung von "Worms"[9] und "Spyware"[10] hat parallel zur wachsenden Entwicklung der Systeme und Netze elektronischer Kommunikation stattgefunden, die immer komplexer und zugleich immer anfälliger wurden - auch aufgrund der Konvergenz von Multimedia, Mobiltelefonie und GRID-Infoware-Systemen[11]: Fälle von Erpressungen mit DDoS-Attacken, Diebstahl der Online-Identität, Phishing[12], Piracy[13] usw. sind Herausforderungen für die Sicherheit der Informationsgesellschaft, welche die Europäische Gemeinschaft in ihrer Mitteilung von 2001[14] - Gegenstand einer Stellungnahme des Ausschusses[15] - entsprechend dreier Interventionsachsen behandelt hat:

– besondere Sicherheitsmaßnahmen,
– Rechtsrahmen einschließlich Datenschutz und Schutz der Privatsphäre,
– Bekämpfung der Cyberkriminalität.

2.6 Die Erfassung der Angriffe auf die Informationstechnik (IT), ihre Identifizierung und ihre Prävention innerhalb eines Netzsystems sind eine Herausforderung für die Suche nach geeigneten Lösungen, denn die Konfigurationen verändern sich kontinuierlich, die Netzprotokolle sowie die angebotenen und entwickelten Dienste sind vielfältig und die asynchronen Angriffsformen äußerst komplex[16].

2.7 Leider werden jedoch die Risiken unterschätzt und wird der Entwicklung einer Sicherheitskultur weniger Aufmerksamkeit geschenkt, da die Investitionsrendite im Sicherheitsbereich kaum sichtbar und die Eigenverantwortlichkeit der nutzenden Bürger wenig ausgeprägt ist.

---

8 Ein Computervirus ist eine Art Malware, ein sich selbst vermehrendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit - im Allgemeinen unbemerkt - reproduziert. Computerviren können für das Betriebssystem mehr oder weniger schädlich sein, verursachen jedoch auch im unschädlichsten Fall einen gewissen Verlust an Ressourcen im Bereich RAM, CPU und Speicherkapazität auf der Festplatte. Siehe http://de.wikipedia.org/wiki/Computervirus.

9 Worm = sich selbst verbreitende Malware: Ein E-Mail-Wurm ist eine zerstörerische Netzwerkattacke, die sämtliche E-Mail-Adressen aus dem Client-E-Mail-Programm (z.B. MS Outlook) sammelt und an diese E-Mail-Adressen Hunderte von E-Mails mit dem Wurm-Programm als Attachment verschickt.

10 Spyware = Softwareprogramme, die "Spuren" vom Internetsurfen des Nutzers speichern und sich ohne Benachrichtigung des Nutzers sowie ohne dessen Wissen, Zustimmung oder Kontrolle selbst installieren.

11 GRID Infoware = ermöglicht das Teilen, Auswählen und Sammeln einer Vielzahl voneinander entfernter Rechnerressourcen (wie Superrechner, Rechnercluster, Speichersysteme, Datenquellen, Instrumente, Humanressourcen) und bündelt sie zu einer einzigen einheitlichen Ressource für komplizierte Berechnungen und datenintensive Computeranwendungen.

12 Phishing = In der Informationstechnik beschreibt der Begriff eine Form des Cracking, um Zugang zu personenbezogenen und vertraulichen Daten mit dem Ziel des Identitätsdiebstahls zu erhalten. Zu diesem Zweck werden gefälschte elektronische Nachrichten verschickt, die so verfasst sind, dass sie authentisch wirken.

13 Piracy = Ein von "Softwarepiraten" verwendeter Begriff für Software, deren Kopierschutz entfernt und die zum Herunterladen ins Internet gestellt wurde.

14 KOM(2001) 298 endg.

15 Vgl. Fußnote 1.

16 Multivariate Statistical Analysis for Network Attacks Detection Guangzhi Qu, Salim Hariri* - 2005 US, Arizona Internet Technology Laboratory, ECE Department, The University of Arizona, http://www.ece.arizona.edu/~hpdc.
Mazin Yousif, Intel Corporation, USA. - Work supported in part by a grant from Intel Corporation IT R&D Council.

3. **Der Kommissionsvorschlag**

3.1 Mit der Mitteilung über die Strategie für eine sichere Informationsgesellschaft[17] will die Kommission die Informationssicherheit durch die Konzeption einer dynamischen, integrierten Strategie auf folgenden Grundlagen verbessern:

a) Verbesserung des Dialogs zwischen den Behörden und der Kommission durch eine vergleichende Bewertung der einzelstaatlichen Maßnahmen und durch die Ermittlung bewährter Verfahren für elektronische Kommunikation im Sicherheitsbereich;
b) eine stärkere Sensibilisierung der Bürger und der KMU für effektive Sicherheitssysteme durch Initiativen der Kommission und eine stärkere Einbindung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA);
c) ein Dialog über die Instrumente und Bestimmungen für ein ausgewogenes Verhältnis zwischen Sicherheit und Grundrechten, einschließlich des Schutzes der Privatsphäre.

3.2 Darüber hinaus ist in der Mitteilung vorgesehen, dass die ENISA mit dem entsprechenden Rahmen für die Sammlung von Daten über Sicherheitsverstöße, über den Grad des Nutzervertrauens und über die Entwicklungen der Sicherheitsindustrie eine vertrauensvolle Partnerschaft

a) mit den Mitgliedstaaten,
b) mit den Verbrauchern und Nutzern sowie
c) mit der Informationssicherheitsindustrie und
d) mit dem Privatsektor

entwickelt und mehrsprachiges EU-Portal zur Information über und Warnung vor Risiken einrichtet - für eine strategische Partnerschaft zwischen Privatsektor, Mitgliedstaaten und Forschern.

3.2.1 Des Weiteren ist in der Mitteilung eine stärkere Eigenverantwortlichkeit der interessierten Kreise hinsichtlich des Bedarfs und der Risiken im Sicherheitsbereich vorgesehen.

3.2.2 Hinsichtlich der internationalen Zusammenarbeit und jener mit Drittstaaten bildet "Die weltweite Dimension der Netz- und Informationssicherheit [NIS] eine Herausforderung für die Kommission, auf internationaler Ebene und in Abstimmung mit den Mitgliedstaaten ihre Bemühungen zu verstärken, eine weltweite Zusammenarbeit in Fragen der NIS […] zu fördern"[18]; unter den Dialog-, Partnerschafts- und Verantwortungsmaßnahmen wird diese Angabe jedoch nicht aufgegriffen.

17 KOM(2006) 251 endg. vom 31.5.2006.

18 KOM(2006) 251, Kap. 3, zweitletzter Absatz.

4. Bemerkungen

4.1 Der Ausschuss stimmt den Analysen und Überlegungen zur Begründung einer integrierten und dynamischen europäischen Strategie für die Netz- und Informationssicherheit uneingeschränkt zu, denn er hält die Sicherheitsfrage für wesentlich, um eine positivere Einstellung zur IT-Anwendung zu fördern und das Vertrauen in letztere zu stärken. Die Positionen des EWSA wurden in zahlreichen Stellungnahmen dargelegt[19].

4.1.1 Der Ausschuss bekräftigt erneut[20], dass "das Internet und die neuen Online-Technologien (wie Mobiltelefone und PDA mit Multimediafunktion und Web-Anschluss, die reißenden Absatz finden) ... nach Ansicht des Ausschusses grundlegende Mittel zur Förderung einer wissensbasierten Wirtschaft, des elektronischen Geschäftsverkehrs und der Online-Verwaltung [sind]".

4.2 Für energischere Kommissionsvorschläge

4.2.1 Der Ausschuss hält jedoch den von der Kommission vorgeschlagenen Ansatz - der darin besteht, diese integrierte und dynamische Strategie auf einen offenen und integrativen Dialog und eine Partnerschaft zwischen den interessierten Kreisen und insbesondere den Nutzern sowie auf stärkere Übernahme von Verantwortung zu stützen - für noch ausbaufähig.

4.2.2 Diese Ansicht wurde bereits in früheren Stellungnahmen unterstrichen: "Darüber hinaus müssen alle Internetnutzer direkt in die Bekämpfung derartiger Inhalte eingebunden werden, um diese wirksam zu gestalten. Die Internetnutzer müssen über die Vorkehrungen und Mittel aufgeklärt und informiert werden, mit denen sie sich gegen derartige gefährliche und unerwünschte Inhalte sowie den Missbrauch ihrer Website als Schnittstelle für die Weiterverbreitung solcher Inhalte schützen können. Dem Bereich Sensibilisierung des Aktionsplanes muss nach Ansicht des Ausschusses Priorität bei der Mobilisierung der Nutzer eingeräumt werden"[21].

4.2.3 Nach Ansicht des Ausschusses muss die Einbindung der Nutzer und der Bürger jedoch so erfolgen, dass der notwendige Informations- und Netzschutz mit den Bürgerrechten und dem Recht der Nutzer auf sicheren Zugang und auf erschwingliche Preise in Einklang steht.

19
- Vgl. Stellungnahme des EWSA zu dem *"Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG"*, ABl. C 69 vom 21.3.2006, S. 16;
- Stellungnahme des EWSA zu der *"Mitteilung der Kommission an den Rat, das Europäische Parlament, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - "i2010 - Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung"*, ABl. C 110 vom 9.5.2006, S. 83;
- Stellungnahme des EWSA zu dem *"Vorschlag für eine Entscheidung des Europäischen Parlaments und des Rates über ein mehrjähriges Gemeinschaftsprogramm zur Förderung der sichereren Nutzung des Internet und neuer Online-Technologien"*, ABl. C 157 vom 28.6.2005, S. 136;
- Stellungnahme des EWSA zu der *"Mitteilung der Kommission an den Rat und das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz"*, ABl. C 48 vom 21.2.2002, S. 33.

20 Vgl. Fußnote 19, 3. Gedankenstrich.

21 Vgl. Fußnote 19, 3. Gedankenstrich.

4.2.4 Es ist zu bedenken, dass das Streben nach Computersicherheit dem Verbraucher Kosten verursacht, auch in Form verlorener Zeit zur Entfernung oder Umgehung der Hindernisse. Nach Ansicht des Ausschusses sollte es obligatorisch sein, in jeden Computer ab Werk Virusschutzsysteme einzubauen, die der Nutzer ein- oder ausschalten könnte.

4.3 **Für eine dynamischere und innovativere Gemeinschaftsstrategie**

4.3.1 Darüber hinaus sollte sich die EU dem Ausschuss zufolge ehrgeizigere Ziele stecken, eine innovative, integrierte und dynamische Strategie ins Leben rufen und neue Initiativen ergreifen, z.B. durch folgende Maßnahmen:

- Maßnahmen, die eine digitale Identifizierung der einzelnen Nutzer ermöglichen, da diese allzu oft aufgefordert werden, ihre persönlichen Daten anzugeben;
- Maßnahmen über das ETSI[22], die als Voraussetzung für eine sichere Nutzung der IKT fungieren und punktuelle, rasche Lösungen bieten können, die durch eine in der ganzen EU einheitliche Sicherheitsschwelle definiert werden;
- vorbeugende Maßnahmen durch die Integration der Mindestsicherheitsanforderungen in den Informatik- und Netzsystemen und Durchführung von Pilotaktionen wie Sicherheitskursen in allen Schultypen;
- Schaffung eines sicheren und anerkannten Rechtsrahmens auf europäischer Ebene. Die Anwendung dieses Rahmens auf die Informatik und auf die Netze würde einen Übergang von Informatiksicherheit zu Informatik"versicherung" ermöglichen;
- Stärkung der europäischen und einzelstaatlichen Risikoabschätzungsmechanismen und stärkere Kapazität zur Umsetzung der Gesetze und Vorschriften, um Informatikkriminalität gegen die Privatsphäre und gegen Datenarchive zu bekämpfen;
- Maßnahmen zur Vermeidung der Entstehung von Informatik-Monokulturen mit leichter "perforierbaren" Produkten und Lösungen; Unterstützung diversifizierter plurikultureller Innovationen mit dem Ziel der Schaffung eines einheitlichen europäischen Informationsraums (SEIS = Single European Information Space).

4.3.2 Zweckmäßig wäre nach Ansicht des EWSA die Schaffung einer IKT-Sicherheitsstelle zwischen den Generaldirektionen[23]. Durch diese Stelle könnte auf folgenden Ebenen gehandelt werden:

- innerhalb der Kommissionsdienststellen;
- auf nationaler Ebene durch horizontale Lösungen für die Aspekte Interoperativität, Identitätsverwaltung, Schutz des Privatlebens, freier Zugang zu Informationen und Dienstleistungen, Mindestsicherheitsanforderungen;

---

22 ETSI = European Telecommunications Standards Institute; s. insbes. den Workshop vom 16./17. Januar 2006. Das ETSI hat u.a. Spezifikationen zu illegalem Abhören (TS 102 232, 102 233 und 102 234), zu LAN-Wireless-Internetzugängen (TR 102 51) und zu elektronischen Unterschriften erarbeitet und Sicherheitsalgorithmen für GPRS- und UMTS-Mobiltelefone entwickelt.

23 Ein solches Zentrum zwischen den Generaldirektionen könnte im Rahmen der IST-Prioritäten des spezifischen Programms "Zusammenarbeit" des 7. FTE-Rahmenprogramms oder durch das Europäische Sicherheitsforschungsprogramm (ESRP) finanziert werden.

– international, damit Europa in verschiedenen Organisationen wie UN, G 8, OSZE und ISO mit einer Stimme spricht.

4.4 **Für stärkere und verantwortungsvolle Koordinierungsmaßnahmen der EU**

4.4.1 Der EWSA misst auch der Schaffung eines "europäischen Netz- und Informationssicherheitsnetzes" große Bedeutung bei, durch das Umfragen, Studien und Workshops zu den Sicherheitsmechanismen und ihrer Interoperativität, über fortgeschrittene Kodierung und den Schutz des Privatlebens durchgeführt werden können.

4.4.2 Nach Ansicht des EWSA sollte für diesen heiklen Sektor die Rolle der europäischen Forschung durch eine sinnvolle inhaltliche Synthese folgender Programme optimiert werden:

– des Europäischen Sicherheitsforschungsprogramms (ESRP)[24] des 7. FTE-Rahmenprogramms,
– des Programms "Safer Internet Plus" und
– des Europäischen Programms für den Schutz kritischer Infrastrukturen (EPCIP)[25].

4.4.3 Diesen Anregungen könnte noch die Einführung eines "europäischen Tags der Computersicherheit" hinzugefügt werden; im Rahmen dieses Tages würden einzelstaatliche Bildungskampagnen in Schulen und Informationskampagnen für die Bürger über Verfahren zum Schutz von Informationen in Computern durchgeführt. Dabei sollten natürlich auch Informationen über die technischen Fortschritte verbreitet werden, die im breiten und sich rasch weiterentwickelnden Computerbereich eingetreten sind.

4.4.4 Der Ausschuss hat wiederholt Folgendes unterstrichen: "Je nachdem, wie sicher sie den elektronischen Geschäftsverkehr einstufen, sind auch die Unternehmen gewillt, IKT in ihrem Betrieb einzusetzen. In gleicher Weise hängt auch die Bereitschaft der Nutzer, ihre Kreditkartendaten auf einer Homepage bekannt zu geben, stark von ihrer Einschätzung der Sicherheit dieser Transaktion ab"[26].

4.4.5 Der Ausschuss ist überzeugt, dass angesichts des enormen Wachstumspotenzials des Sektors besondere Maßnahmen zu ergreifen und die aktuellen Maßnahmen an die neuen Entwicklungen anzupassen sind. Die europäischen Initiativen für Informationssicherheit müssen mit einer integrierten Strategie einhergehen, indem Grenzen zwischen den einzelnen Sektoren beseitigt und eine homogene und sichere Verbreitung der IKT in der Gesellschaft gewährleistet werden.

---

24 Vgl. 7. Rahmenprogramm Forschung, Technologie und Demonstration, spezifisches Programm Zusammenarbeit, thematische Priorität Sicherheitsforschung mit Haushaltsmitteln in Höhe von 1,35 Mrd. EUR für 2007-2013.

25 KOM(2005) 576 vom 17.11.2005.

26 Vgl. Fußnote 19, 2. Gedankenstrich.

4.4.6 Nach Ansicht des Ausschusses kommen einige wichtige Strategien wie diese allzu langsam voran, da die Mitgliedstaaten den auf Gemeinschaftsebene zu fassenden Beschlüssen bürokratische und kulturelle Schwierigkeiten in den Weg stellen.

4.4.7 Nach Ansicht des Ausschusses werden unzureichende Gemeinschaftsmittel dafür eingesetzt, die zahlreichen und dringenden Projekte zu verwirklichen, die nur dann konkrete Antworten auf die durch die Globalisierung entstandenen neuen Probleme liefern, wenn sie auf Gemeinschaftsebene verwirklicht werden.

4.5 **Für stärkeren Verbraucherschutz durch die EU**

4.5.1 Der Ausschuss ist sich bewusst, dass die Mitgliedstaaten ihre technologischen Sicherheitsmaßnahmen und Verfahren des Sicherheitsmanagements nach ihren eigenen Bedürfnissen entwickelt haben und sich hierbei auf unterschiedliche Aspekte konzentrieren. Auch deshalb ist es schwierig, eine eindeutige, wirksame Antwort auf die Sicherheitsprobleme zu finden. Mit Ausnahme einiger Verwaltungsnetze gibt es keine systematische grenzüberschreitende Zusammenarbeit zwischen den Mitgliedstaaten, wenngleich Sicherheitsfragen von den einzelnen Mitgliedstaaten nicht separat angegangen werden können.

4.5.2 Der Ausschuss weist jedoch darauf hin, dass der Rat mit Beschluss 2005/222/JI einen Rahmen für die Zusammenarbeit zwischen den Justiz- und sonstigen zuständigen Behörden geschaffen hat, um einen kohärenten Ansatz der Mitgliedstaaten durch Angleichung ihrer einzelstaatlichen Strafrechtsvorschriften für Angriffe auf Informationssysteme hinsichtlich folgender Aspekte zu gewährleisten:

- rechtswidriger Zugang zu Informationssystemen;
- rechtswidriger Eingriff durch vorsätzliche schwere Behinderung oder Störung des Betriebs eines Informationssystems;
- rechtswidriger Eingriff in die Daten mit dem Ziel, die Computerdaten eines Informationssystems zu löschen, beschädigen, verstümmeln, verändern, unterdrücken oder unzugänglich zu machen;
- Anstiftung oder Beihilfe zu oben genannten Delikten.

4.5.3 Des Weiteren werden in dem Rahmenbeschluss die Kriterien für die Feststellung der Haftung der juristischen Person und die Sanktionen genannt, die bei Feststellung ihrer Haftung angewandt werden können.

4.5.4 Hinsichtlich des Dialogs mit den Behörden der Mitgliedstaaten unterstützt der Ausschuss den Kommissionsvorschlag, dass diese Behörden eine vergleichende Bewertung der eigenen staatlichen Maßnahmen für die Sicherheit der Informationsnetze und -systeme, einschließlich

der besonderen Maßnahmen für den öffentlichen Sektor, vornehmen sollen. Dieser Vorschlag wurde in einer Stellungnahme des EWSA von 2001 unterbreitet[27].

4.6 **Für eine stärkere Verbreitung einer "Sicherheitskultur"**

4.6.1 Die Informationssicherheitsindustrie muss effektiv gewährleisten, dass sie - entsprechend dem Stand der Technik - Systeme zur materiellen Überwachung ihrer eigenen Installationen verwendet und die Kommunikationen verschlüsselt, um das Recht ihrer Kunden auf Schutz der Privatsphäre und auf Vertraulichkeit zu schützen[28].

4.6.2 Hinsichtlich der Sensibilisierungsmaßnahme hält es der Ausschuss für grundlegend, eine echte "Sicherheitskultur" zu schaffen, die vollständig mit der Informations-, der Kommunikations- und der Meinungsfreiheit in Einklang steht. Im Übrigen sind vielen Nutzern sämtliche Sicherheitsrisiken gar nicht bewusst, während viele Betreiber, Verkäufer oder Erbringer von Diensten nicht einschätzen können, ob und in welchem Maße das System Schwachstellen aufweist.

4.6.3 Der Schutz der Privatsphäre und persönlicher Daten sind vorrangige Ziele, die Verbraucher haben aber auch einen Anspruch auf wirklich effizienten Schutz gegen missbräuchliche namentliche Identifizierung durch spezielle Spionierprogramme (Spyware und Web Bugs) oder auf anderem Wege. Der Praxis des Spamming[29] (massiver Versand von nicht verlangten Mails), die häufig mit diesen missbräuchlichen Handlungen einhergeht, muss ebenfalls wirksam entgegengetreten werden. Diese Eingriffe gehen auf Kosten der Opfer solcher Handlungsweisen[30].

4.7 **Für eine stärkere und aktivere EU-Agentur**

4.7.1 Der Ausschuss befürwortet eine wichtigere und wirksamere Rolle der Europäischen Agentur für Netz- und Informationssicherheit (ENISA): bei der Sensibilisierungsmaßnahme, aber auch und vor allem bei Maßnahmen zur Information und Bildung der Betreiber und Nutzer, wie er bereits in einer unlängst vorgelegten Stellungnahme[31] zur Bereitstellung öffentlicher elektronischer Kommunikationsdienste betont hat.

4.7.2 Was schließlich die Maßnahmen zur Stärkung der Eigenverantwortlichkeit jeder Gruppe der interessierten Kreise angeht, so wurde das Subsidiaritätsprinzip hierbei offensichtlich strikt

---

27 Vgl. Fußnote 19, 4. Gedankenstrich.

28 Vgl. Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (ABl. L 24/1998).

29 Spam(ming) = *pourriel* oder *pollupostage* auf Französisch.

30 Vgl. Stellungnahmen über "Elektronische Kommunikationsnetze" (ABl. C 123 vom 25.4.2001, S. 50), über "Elektronischen Geschäftsverkehr" (ABl. C 169 vom 16.6.1999, S. 36) und über "Auswirkungen des elektronischen Handels auf den Binnenmarkt" (ABl. C 123 vom 25.4.2001, S. 1).

31 Vgl. Fußnote 19, 1. Gedankenstrich.

eingehalten. In der Tat ist es Aufgabe der Mitgliedstaaten und des Privatsektors, diese entsprechend ihren besonderen Zuständigkeiten durchzuführen.

4.7.3 Die ENISA sollte die Beiträge des Europäischen Netz- und Informationssicherheitsnetzes nutzen können, um gemeinsame Arbeiten zu organisieren; auch sollte sie das mehrsprachige EU-Webportal für Computersicherheit dafür einsetzen, persönliche und interaktive Informationen in leicht verständlicher Sprache für private Nutzer verschiedenen Alters und für KMU zu übermitteln.

Brüssel, den 16. Februar 2007

Der Präsident des Europäischen Wirtschafts- und Sozialausschusses	Der Generalsekretär des Europäischen Wirtschafts- und Sozialausschusses
Dimitris DIMITRIADOS	**Patrick VENTURINI**