(2) zu prüfen, ob diese Initiative finanzielle Unterstützung aus Mitteln erhalten kann, die im Rahmen der Entscheidung des Rates vom 9. Dezember 1999 über ein Aktionsprogramm der Gemeinschaft für den Katastrophenschutz [1] für den Zeitraum 1. Januar 2000 bis 31. Dezember 2004 oder im Rahmen des Ratsbeschlusses zur Einrichtung eines Gemeinschaftsverfahrens zur Förderung einer verstärkten Zusammenarbeit bei Katastrophenschutzeinsätzen für Bildungsmaßnahmen vorgesehen sind.

(3) die Bewerberländer an ihrer Arbeit zu beteiligen,

(4) am Ende dieser Pilotphase unter Berücksichtigung der erzielten Ergebnisse alle Initiativen in Betracht zu ziehen, die die Herbeiführung einer langfristigen Zusammenarbeit bei der Aus- und Fortbildung im Bereich des Katastrophenschutzes zum Ziel haben, beispielsweise durch die Gründung einer Europäischen Akademie für Katastrophenschutz, durch die das oben genannte Netz institutionalisiert würde.

[1] ABl. L 327 vom 21.12.1999, S. 53.

ENTSCHLIESSUNG DES RATES

vom 28. Januar 2002

zu einem gemeinsamen Ansatz und spezifischen Maßnahmen im Bereich der Netz- und Informationssicherheit

(2002/C 43/02)

DER RAT DER EUROPÄISCHEN UNION —

IM ANSCHLUSS AN

die Schlussfolgerungen des Europäischen Rates von Stockholm am 23. und 24. März 2001, wonach der Rat in Zusammenarbeit mit der Kommission eine umfassende Strategie für die Sicherheit elektronischer Netze einschließlich praktischer Durchführungsmaßnahmen entwickeln wird;

UNTER HINWEIS AUF

1. die Entschließung des Rates vom 30. Mai 2001 „Aktionsplan *e*Europe 2002: Informations- und Netzsicherheit“;

2. die Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Sicherheit der Netze und Informationen: Vorschlag für einen Europäischen Politikansatz;

3. die Mitteilung der Kommission an den Rat und das Europäische Parlament „*e*Europe 2002: Auswirkungen und Prioritäten“;

4. den vom Europäischen Rat von Feira am 19. und 20. Juni 2000 gebilligten „*e*Europe“-Aktionsplan;

5. die Empfehlung 95/144/EG des Rates vom 7. April 1995 über gemeinsame Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik [1];

6. die Empfehlung des Rates vom 25. Juni 2001 über Kontaktstellen mit einem rund um die Uhr erreichbaren Dauerdienst zur Bekämpfung der Hightech-Kriminalität [2];

7. die Mitteilung der Europäischen Kommission über die Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität;

8. die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr [3];

9. die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [4];

10. die Richtlinie 97/33/EG des Europäischen Parlaments und des Rates vom 30. Juni 1997 über die Zusammenschaltung in der Telekommunikation im Hinblick auf die Sicherstellung eines Universaldienstes und der Interoperabilität durch Anwendung der Grundsätze für einen offenen Netzzugang (ONP) [5];

11. die 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 [6];

12. die Richtlinie 98/10/EG des Europäischen Parlaments und des Rates vom 26. Februar 1998 über die Anwendung des offenen Netzzugangs (ONP) beim Sprachtelefondienst und dem Universaldienst im Telekommunikationsbereich in einem wettbewerbsorientierten Umfeld [7];

[1] ABl. L 93 vom 26.4.1995, S. 27.

[2] ABl. C 187 vom 3.7.2001, S. 5.

[3] ABl. L 8 vom 12.1.2001, S. 1.

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

[5] ABl. L 199 vom 26.7.1997, S. 32.

[6] ABl. L 24 vom 30.1.1998, S. 1.

[7] ABl. L 101 vom 1.4.1998, S. 24.

13. die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen [1];

IN ERWÄGUNG NACHSTEHENDER GRÜNDE:

(1) Netze und Kommunikationssysteme sind ein entscheidender Faktor für die wirtschaftliche und gesellschaftliche Entwicklung geworden, und ihre Verfügbarkeit und Unversehrtheit ist für wesentliche Infrastrukturen und für die meisten öffentlichen und privaten Dienste und die Wirtschaft als Ganzes unabdingbar.

(2) In Anbetracht der immer wichtigeren Rolle, die elektronische Dienste in der Wirtschaft spielen, ist die Sicherheit von Netzen und Informationssystemen in zunehmendem Maße von öffentlichem Interesse.

(3) Die Sicherheit von Transaktionen und Daten ist nunmehr von wesentlicher Bedeutung für die Bereitstellung elektronischer Dienste, einschließlich des elektronischen Geschäftsverkehrs („e-commerce") und der online-Behördendienste, und ein geringes Vertrauen in die Sicherheit könnte die umfassende Einführung solcher Dienste hemmen.

(4) Es ist notwendig, dass Einzelpersonen, Unternehmen, Verwaltungen und andere Organisationen ihre eigenen Informations-, Daten- und Kommunikationssysteme — gegebenenfalls durch den Einsatz wirksamer Sicherheitstechnologie — schützen.

(5) Der Privatsektor bietet durch seine Einbindung in ein wettbewerbsorientiertes marktwirtschaftliches Umfeld und durch seine Innovationsfähigkeit eine Vielzahl von Lösungen, die an die wirklichen Marktbedürfnisse angepasst sind.

(6) Die Komplexität der Netz- und Informationssicherheit bedeutet, dass die Behörden bei der Entwicklung von politischen Maßnahmen in diesem Bereich eine Vielzahl politischer, wirtschaftlicher, organisatorischer und technischer Aspekte zu berücksichtigen haben und sich des dezentralen und globalen Charakters der Kommunikationsnetze bewusst sein müssen.

(7) Politische Maßnahmen können wirksamer angewandt werden, wenn sie Teil eines europäischen Ansatzes sind, das wirksame Funktionieren des Binnenmarktes wahren, auf einer verstärkten Zusammenarbeit zwischen den Mitgliedstaaten und auf internationaler Ebene beruhen, Innovation fördern und die internationale Wettbewerbsfähigkeit der europäischen Unternehmen begünstigen.

(8) Es gibt bereits einen umfangreichen Bestand an Rechtsvorschriften für Netz- und Informationssicherheit, insbesondere als Teil des Rechtsrahmens der Union für Telekommunikation, den elektronischen Geschäftsverkehr und elektronische Signaturen.

(9) Anbieter von Telekommunikationsdiensten werden gesetzlich dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit ihrer Dienste zu ergreifen; durch diese Maßnahmen wird ein Schutzniveau erreicht, das in einem angemessenen Verhältnis zu dem vorhandenen Risiko steht.

(10) Die internationale Norm ISO-15408 (Gemeinsame Kriterien) ist mittlerweile ein anerkanntes System zur Festlegung der Sicherheitsanforderungen für Rechner- und Netzprodukte und zur Beurteilung, ob ein bestimmtes Produkt diese Anforderungen erfüllt.

(11) Die internationale Norm ISO-17799 (Informationstechnologie — Verhaltenskodex für das Management von Informationssicherheit) und vergleichbare nationale Leitlinien werden zu einer anerkannten Praxis für Sicherheitsmaßnahmen in privaten und öffentlichen Organisationen.

(12) Die Internet-Infrastruktur sollte einen weit gehenden Zugang zu Netzen und Dienstleistungen ermöglichen und auf widerstandsfähige und sichere Weise — beispielsweise durch die Festlegung offener Normen und Internet-Sicherheitsprotokolle — verwaltet und betrieben werden.

IN DER ERWÄGUNG, dass es gemäß der Entschließung des Rates vom 30. Mai 2001 über den Aktionsplan „eEurope 2000: Sicherheit der Netze und Informationen" bei der Netz- und Informationssicherheit darum geht,

— die Verfügbarkeit von Diensten und Daten zu gewährleisten;

— die Störung und das unerlaubte Abhören des Kommunikationsverkehrs zu verhindern;

— die Vollständigkeit und Richtigkeit von übermittelten, erhaltenen oder gespeicherten Daten zu bestätigen;

— die Vertraulichkeit der Daten sicherzustellen;

— Informationssysteme gegen unerlaubten Zugriff zu schützen;

— Informationssysteme vor Angriffen unter Verwendung von Schadprogrammen zu schützen;

— eine zuverlässige Authentifizierung sicherzustellen —

ERSUCHT DAHER DIE MITGLIEDSTAATEN,

1. bis Ende 2002 Informations- und Schulungskampagnen zur Sensibilisierung für die Netz- und Informationssicherheit einzuleiten oder zu verstärken, diese Maßnahmen speziell auf Unternehmen, private Nutzer und öffentliche Verwaltungen auszurichten, diese Sensibilisierungsmaßnahmen in enger Zusammenarbeit mit dem Privatsektor, unter anderem unter Beteiligung der Internet-Diensteanbieter, zu entwickeln und Initiativen des Privatsektors zu fördern;

[1] ABl. L 13 vom 19.1.2000, S. 12.

2. die bewährten Praktiken im Bereich des Managements der Informationssicherheit insbesondere in kleinen und mittleren Unternehmen — gegebenenfalls auf der Grundlage von international anerkannten Normen — zu fördern;

3. bis Ende 2002 die Bedeutung der Sicherheitskonzepte als Teil der Computerbildung und -ausbildung zu vergrößern oder zu fördern;

4. bis Mitte 2002 die Wirksamkeit von nationalen Vereinbarungen über Computer-Notfalldienste, darunter gegebenenfalls Virenwarnsysteme, im Hinblick darauf zu überprüfen, dass erforderlichenfalls die Fähigkeit dieser Dienste bzw. Systeme verbessert wird, Störungen von Netzen und Informationssystemen und Angriffe darauf auf nationaler und internationaler Ebene wirksam zu verhindern, zu entdecken und zu bekämpfen;

5. für die Anwendung der Norm „Gemeinsame Kriterien" (ISO-15408) einzutreten und die gegenseitige Anerkennung der einschlägigen Zertifikate zu erleichtern;

6. bis Ende 2002 wichtige Schritte zur Ausarbeitung wirksamer und interoperabler Sicherheitslösungen, die nach Möglichkeit auf anerkannten Normen beruhen — darunter ggf. auch quell-offene Software —, für ihre netzgestützten Behördendienste und Beschaffungsdienste („e-government" und „e-procurement") sowie zur Einführung elektronischer Signaturen zu unternehmen, damit öffentliche Dienstleistungen, bei denen eine starke Authentifizierung erforderlich ist, auch online angeboten werden können;

7. im Falle der Einführung elektronischer und biometrischer Identifizierungssysteme für den öffentlichen oder amtlichen Gebrauch gegebenenfalls im Bereich der technologischen Entwicklungen zusammenzuarbeiten und die Möglichkeiten etwaiger Anforderungen an die Interoperabilität zu prüfen;

8. zur Erleichterung der Zusammenarbeit in der Gemeinschaft sowie der internationalen Zusammenarbeit gegenseitig und mit der Kommission Informationen über die Gremien auszutauschen, die in ihrem Gebiet an erster Stelle für Netz- und Informationssicherheit zuständig sind;

BEGRÜSST DIE ABSICHT DER KOMMISSION,

1. im Jahr 2002 einen Austausch der bewährten Praktiken in Bezug auf die Sensibilisierungsmaßnahmen zu erleichtern und eine erste Bestandsaufnahme der verschiedenen einzelstaatlichen Informationskampagnen durchzuführen;

2. im Jahr 2002 Vorschläge zu unterbreiten, um den Dialog und die Zusammenarbeit der Gemeinschaft mit Organisationen und Partnern auf internationaler Ebene über die Netzsicherheit, insbesondere über die Folgen der zunehmenden Abhängigkeit von elektronischen Kommunikationsnetzen, zu intensivieren und in diesem Rahmen bis Ende 2002 eine Strategie für einen stabileren und sicheren Betrieb der Internet-Infrastruktur vorzuschlagen;

3. bis Ende 2002 geeignete Maßnahmen zur Förderung der ISO-Norm 15408 (Gemeinsame Kriterien) im Hinblick auf die Vereinfachung der gegenseitigen Anerkennung von Zertifikaten und die Verbesserung des Verfahrens zur Evaluierung von Produkten, z. B. durch die Entwicklung angemessener Schutzprofile, vorzuschlagen;

4. bis Ende 2002 einen Bericht über die Technologien und Anwendungen elektronischer und biometrischer Systeme zur Authentifizierung der Identität mit dem Ziel auszuarbeiten, die Wirksamkeit dieser Systeme, insbesondere im Wege der Interoperabilität, zu verbessern;

5. bis Mitte 2002 nach Konsultation der Mitgliedstaaten und des Privatsektors Vorschläge für die Einrichtung eines Sonderstabs für Computer- und Netzsicherheit zu unterbreiten; dieser soll aufbauend auf den einzelstaatlichen Bemühungen die Netz- und Informationssicherheit sowie die Fähigkeit der Mitgliedstaaten, einzeln und gemeinsam erheblichen Problemen der Netz- und Informationssicherheit zu begegnen, verstärken;

6. bis Ende 2002 in Zusammenarbeit mit den Mitgliedstaaten unter Berücksichtigung der säulenübergreifenden Dimension der Netz- und Informationssicherheit die möglichen Mechanismen zu prüfen, anhand deren die Mitgliedstaaten und die Kommission Informationen und Erfahrungen in Bezug auf die Verwirklichung der mit dieser Entschließung verfolgten Ziele austauschen können, und zu untersuchen, wie der Privatsektor am besten an diesem Informations- und Erfahrungsaustausch beteiligt werden kann;

BEGRÜSST, dass die europäischen Forschungsarbeiten den Sicherheitsfragen eine größere Aufmerksamkeit widmen;

BETONT, dass weitere Forschungsarbeiten notwendig sind, insbesondere in Bezug auf Sicherheitsmechanismen und ihre Interoperabilität, Zuverlässigkeit und Schutz von Netzen, fortgeschrittene Kryptografie, Technologien zur Verbesserung des Vertraulichkeitsschutzes und Sicherheit drahtloser Kommunikation;

APPELLIERT

— an Lieferanten und Diensteanbieter, die Sicherheit als wesentlichen Bestandteil ihrer Produkte und Dienstleistungen zu verbessern;

— an die Lieferanten und Diensteanbieter des europäischen Privatsektors und die ihre Interessen vertretenden Verbände, sich aktiver an den Arbeiten der internationalen Normung zu beteiligen, und sich in Gremien zusammenzuschließen, in denen sie zur Verwirklichung der Ziele dieser Entschließung beitragen können.