BESCHLUSS DES RATES

vom 31. März 1992

auf dem Gebiet der Sicherheit von Informationssystemen

(92/242/EWG)

DER RAT DER EUROPÄISCHEN GEMEINSCHAFTEN —

gestützt auf den Vertrag zur Gründung der Europäischen Wirtschaftsgemeinschaft, insbesondere auf Artikel 235,

auf Vorschlag der Kommission (1),

nach Stellungnahme des Europäischen Parlaments (2),

nach Stellungnahme des Wirtschafts- und Sozialausschusses (3),

in Erwägung nachstehender Gründe:

Aufgabe der Gemeinschaft ist es, durch die Errichtung eines Gemeinsamen Marktes und die schrittweise Annäherung der Wirtschaftspolitiken der Mitgliedstaaten eine harmonische Entwicklung des Wirtschaftslebens innerhalb der Gemeinschaft, eine beständige und ausgewogene Wirtschaftsausweitung, eine größere Stabilität, eine beschleunigte Hebung der Lebenshaltung und engere Beziehungen zwischen den Mitgliedstaaten zu fördern.

Elektronisch gespeicherte, verarbeitete und übertragene Informationen spielen bei den wirtschaftlichen und sozialen Tätigkeiten eine immer wichtigere Rolle.

Mit der Einführung effizienter globaler Kommunikationsdienste und der immer weiter verbreiteten elektronischen Informationsverarbeitung wächst der Bedarf an angemessenen Schutzmaßnahmen.

Das Europäische Parlament hat in seinen Beratungen und Beschlüssen wiederholt auf die Bedeutung der Sicherheit von Informationssystemen hingewiesen.

Der Wirtschafts- und Sozialausschuß hat auf die Notwendigkeit hingewiesen, im Rahmen der Gemeinschaftsaktionen Fragen der Sicherheit von Informationssystemen zu behandeln, und zwar insbesondere angesichts der Auswirkungen der Verwirklichung des Binnenmarktes.

Aktionen auf nationaler und internationaler Ebene sowie auf Gemeinschaftsebene bilden hierfür eine gute Grundlage.

Es besteht eine enge Verbindung zwischen den Bereichen Telekommunikation, Informationstechnologie, Normung, Informationsmarkt und einer Politik der Forschung und technologischen Entwicklung (FTE) sowie der Arbeit, die die Europäische Gemeinschaft auf diesen Gebieten bereits geleistet hat.

Die Konzertierung der Maßnahmen sollte unter Zugrundelegung der laufenden Arbeiten auf nationaler und internationaler Ebene und durch Förderung der Zusammenarbeit zwischen den Hauptbeteiligten gewährleistet werden. Dies sollte im Rahmen eines in sich geschlossenen Aktionsplans geschehen.

Die Komplexität des Problems der Sicherheit von Informationssystemen erfordert die Entwicklung von Strategien, die den freien Informationsverkehr im Binnenmarkt ermöglichen und gleichzeitig die Sicherheit der Nutzung von Informatonssystemen in der gesamten Gemeinschaft gewährleisten.

Den einzelnen Mitgliedstaaten obliegt die Verantwortung, die durch Sicherheit und öffentliche Ordnung bedingten Zwänge zu berücksichtigen.

Die Verantwortlichkeit der Mitgliedstaaten auf diesem Gebiet bedingt einen konzertierten Ansatz, der auf einer engen Zusammenarbeit mit hohen Beamten der Mitgliedstaaten basiert.

Es ist eine Maßnahme erforderlich, die einen Aktionsplan für einen Anfangszeitraum von vierundzwanzig Monaten sowie die Einsetzung eines mit einem langfristigen Auftrag versehenen Ausschusses hoher Beamter zur Beratung der Kommission bei Maßnahmen auf dem Gebiet der Sicherheit von Informationssystemen beinhaltet.

Für die Durchführung der Maßnahme während eines Anfangszeitraums von vierundzwanzig Monaten wird ein Betrag von 12 Millionen ECU für notwendig erachtet. Der für 1992 im Rahmen der derzeitigen finanziellen Vorausschau für notwendig erachtete Betrag beläuft sich auf 2 Millionen ECU.

Die zur Finanzierung des Programms für die Zeit nach dem Haushaltsjahr 1992 zu bindenden Beträge müssen sich in den geltenden Finanzrahmen der Gemeinschaft einfügen —

BESCHLIESST:

Artikel 1

Im Bereich der Sicherheit von Informationssystemen wird eine Maßnahme beschlossen, die folgendes umfaßt:

— die Entwicklung umfassender Strategien auf dem Gebiet der Sicherheit von Informationssystemen (Aktionsplan) für einen Anfangszeitraum von vierundzwanzig Monaten und

— die Einsetzung einer mit einem langfristigen Auftrag versehenen Gruppe hoher Beamter zur Beratung der Kommission bei Maßnahmen auf dem Gebiet der Sicherheit von Informationssystemen, nachstehend „Ausschuß" genannt.

(1) ABl. Nr. C 277 vom 5. 11. 1990, S. 18.
(2) ABl. Nr. C 94 vom 13. 3. 1992.
(3) ABl. Nr. C 159 vom 17. 6. 1991, S. 38.

Artikel 2

(1) Die Kommission konsultiert den Ausschuß regelmäßig zu Fragen der Sicherheit von Informationssystemen der verschiedenen Gemeinschaftstätigkeiten und insbesondere bei der Festlegung von Arbeitsstrategien und -programmen.

(2) Der Aktionsplan gemäß dem Anhang sieht Vorarbeiten im Rahmen folgender Themenbereiche vor:

I. Entwicklung einer Rahmenstrategie für die Sicherheit von Informationssystemen

II. Ermittlung von Anforderungen der Benutzer und der Diensteanbieter zur Sicherheit von Informationssystemen

III. Lösungen für den kurz- und mittelfristigen Bedarf von Benutzern, Lieferanten und Diensteanbietern

IV. Entwicklung von Spezifikationen, Normung, Bewertung und Zertifizierung der Sicherheit von Informationssystemen

V. Technologische und funktionale Entwicklungen auf dem Gebiet der Sicherheit von Informationssystemen

VI. Maßnahmen auf dem Gebiet der Sicherheit von Informationssystemen.

Artikel 3

(1) Die für die Durchführung der Maßnahme während des Anfangszeitraums für erforderlich gehaltenen Mittel der Gemeinschaft belaufen sich auf 12 Millionen ECU, wovon im Rahmen der finanziellen Vorausschau 1988-1992 2 Millionen ECU auf 1992 entfallen.

Der Betrag für die restliche Laufzeit des Programms muß mit dem geltenden Finanzrahmen der Gemeinschaft in Einklang stehen.

(2) Die Haushaltsbehörde legt die für jedes einzelne Haushaltsjahr verfügbaren Mittel nach den Grundsätzen der Wirtschaftlichkeit der Haushaltsführung im Sinne von Artikel 2 der Haushaltsordnung für den Gesamthaushaltsplan der Europäischen Gemeinschaft fest.

Artikel 4

Die während des Anfangszeitraums erzielten Fortschritte werden für die Kommission von einer Gruppe unabhängiger Sachverständiger bewertet. Der Bericht dieser Gruppe wird zusammen mit etwaigen Bemerkungen der Kommission dem Europäischen Parlament und dem Rat vorgelegt.

Artikel 5

(1) Die Kommission ist für die Durchführung der Maßnahme verantwortlich. Sie wird von einem Beratenden Ausschuß unterstützt, der sich aus Vertretern der Mitgliedstaaten zusammensetzt und in dem der Vertreter der Kommission den Vorsitz führt.

(2) Der Aktionsplan wird entsprechend den in Artikel 2 festgelegten Zielen durchgeführt und ist erforderlichenfalls zu aktualisieren. In dem Aktionsplan werden im einzelnen die Ziele und Arten der zu treffenden Maßnahmen sowie die Finanzbestimmungen festgelegt. Die Kommission führt auf der Grundlage des Aktionsplans Ausschreibungen durch.

(3) Der Aktionsplan wird in Zusammenarbeit mit den Akteuren des Bereichs durchgeführt. In dem Aktionsplan werden die laufenden europäischen und internationalen Normungstätigkeiten auf diesem Gebiet berücksichtigt, gefördert und ergänzt.

Artikel 6

(1) Das Verfahren des Artikels 7 gilt für Maßnahmen im Zusammenhang mit der Gemeinschaftspolitik auf dem Gebiet der Sicherheit von Informationssystemen.

(2) Das Verfahren des Artikels 8 gilt für

— die Ausarbeitung und Aktualisierung des in Artikel 5 genannten Aktionsplans;

— den Inhalt von Ausschreibungen, die Bewertung der Vorschläge und den geschätzten Betrag des Gemeinschaftsbeitrags zu Maßnahmen, sofern dieser Betrag 200 000 ECU übersteigt;

— die Mitwirkung von Nichtgemeinschaftsorganisationen an Tätigkeiten im Rahmen dieses Beschlusses;

— Bestimmungen über die Verbreitung, den Schutz und die Auswertung der bei den Maßnahmen erzielten Ergebnisse;

— die Maßnahmen zur Bewertung der Aktion.

(3) Beläuft sich der Gemeinschaftsbeitrag zu den Maßnahmen auf höchstens 200 000 ECU, so hört die Kommission den Ausschuß zu den Maßnahmen an und unterrichtet ihn über das Ergebnis ihrer Nutzenabschätzung.

Artikel 7

Der Vertreter der Kommission unterbreitet dem Ausschuß einen Entwurf der zu treffenden Maßnahmen. Der Ausschuß gibt — gegebenenfalls nach Abstimmung — eine Stellungnahme zu diesem Entwurf innerhalb einer Frist ab, die der Vorsitzende unter Berücksichtigung der Dringlichkeit der betreffenden Frage festsetzen kann.

Die Stellungnahme wird in das Protokoll aufgenommen; darüber hinaus hat jeder Mitgliedstaat das Recht zu verlangen, daß sein Standpunkt im Protokoll festgehalten wird.

Die Kommission berücksichtigt soweit wie möglich die Stellungnahme des Ausschusses. Sie unterrichtet den Ausschuß darüber, inwieweit sie seine Stellungnahme berücksichtigt hat.

Artikel 8

Der Vertreter der Kommission unterbreitet dem Ausschuß einen Entwurf der zu treffenden Maßnahmen. Der Ausschuß gibt seine Stellungnahme zu diesem Entwurf innerhalb einer Frist ab, die der Vorsitzende unter Berücksichtigung der Dringlichkeit der betref-

fenden Frage festsetzen kann. Die Stellungnahme wird mit der Mehrheit abgegeben, die in Artikel 148 Absatz 2 des Vertrages für die Annahme der vom Rat auf Vorschlag der Kommission zu fassenden Beschlüsse vorgesehen ist. Bei der Abstimmung im Ausschuß werden die Stimmen der Vertreter der Mitgliedstaaten gemäß dem vorgenannten Artikel gewogen. Der Vorsitzende nimmt an der Abstimmung nicht teil.

Die Kommission erläßt die beabsichtigten Maßnahmen, wenn sie mit der Stellungnahme des Ausschusses übereinstimmen.

Stimmen die beabsichtigten Maßnahmen mit der Stellungnahme des Ausschusses nicht überein oder liegt keine Stellungnahme vor, so unterbreitet die Kommission dem Rat unverzüglich einen Vorschlag für die zu treffenden Maßnahmen. Der Rat beschließt mit qualifizierter Mehrheit.

Hat der Rat nach Ablauf von drei Monaten von der Befassung des Rates an keinen Beschluß gefaßt, so werden die vorgeschlagenen Maßnahmen von der Kommission erlassen, es sei denn, der Rat hat sich mit einfacher Mehrheit gegen die genannten Maßnahmen ausgesprochen.

Geschehen zu Brüssel am 31. März 1992.

Im Namen des Rates

Der Präsident

Vitor MARTINS

ANHANG

Übersicht über die Aktionslinien

LEITLINIEN FÜR EINEN AKTIONSPLAN AUF DEM GEBIET DER SICHERHEIT VON INFORMATIONSSYSTEMEN

EINLEITUNG

Ziel des Aktionsplans ist die Entwicklung umfassender Strategien mit dem Ziel, den Benutzern und Herstellern elektronisch gespeicherter, verarbeiteter oder übermittelter Informationen einen angemessenen Schutz der Informationssysteme gegen unabsichtliche oder vorsätzliche Gefährdung zu bieten.

Der Aktionsplan berücksichtigt und ergänzt die laufenden weltweiten Normungstätigkeiten auf diesem Gebiet.

Er umfaßt folgende Aktionslinien:

— Entwicklung einer Rahmenstrategie für die Sicherheit von Informationssystemen;

— Ermittlung von Anforderungen der Benutzer und der Diensteanbieter zur Sicherheit von Informationssystemen;

— Lösungen für den kurz- und mittelfristigen Bedarf von Benutzern, Lieferanten und Diensteanbietern;

— Entwicklung von Spezifikationen, Normung, Bewertung und Zertifizierung der Sicherheit von Informationssystemen;

— technologische und funktionale Entwicklungen auf dem Gebiet der Sicherheit von Informationssystemen;

— Maßnahmen auf dem Gebiet der Sicherheit von Informationssystemen.

Der Aktionsplan wird von der Kommission im engen Verbund mit ähnlichen Maßnahmen der Mitgliedstaaten und im Zusammenhang mit gleichgelagerten Forschungs- und Entwicklungsmaßnahmen der Gemeinschaft durchgeführt.

1. Aktionslinie I — Entwicklung einer Rahmenstrategie für die Sicherheit von Informationssystemen

1.1. *Problematik*

Die Sicherheit von Informationssystemen gilt unbestritten als eine Dimension, die in allen Bereichen der modernen Gesellschaft gewährleistet sein muß. Elektronische Informationsdienste erfordern eine sichere Telekommunikationsinfrastruktur, sichere Hard- und Software sowie eine sichere Benutzung und Verwaltung. Es muß eine Gesamtstrategie entwickelt werden, die alle Aspekte der Sicherheit von Informationssystemen berücksichtigt und somit ein aufgesplittertes Konzept vermeidet. Jegliche Strategie für die Sicherheit der elektronisch verarbeiteten Informationen muß den Wunsch der Gesellschaft berücksichtigen, effizient zu arbeiten und sich gleichzeitig in einem sich rasch wandelnden Umfeld zu schützen.

1.2. *Zielsetzung*

Es muß eine Rahmenstrategie geschaffen werden, um die gesellschaftlichen, wirtschaftlichen und politischen Ziele mit den technischen, operationellen und legislativen Optionen der Gemeinschaft in einem internationalen Kontext in Einklang zu bringen. Das empfindliche Gleichgewicht zwischen verschiedenen Anliegen, Zielen und Sachzwängen muß von den Akteuren des Bereichs ermittelt werden, die bei der Entwicklung einer gemeinsamen Sichtweise und einer abgestimmten Rahmenstrategie zusammenarbeiten. Dies sind die Voraussetzungen, um Interessen und Bedürfnisse sowohl im politischen Bereich als auch bei industriellen Entwicklungen zu vereinen.

1.3. *Derzeitiger Stand und Tendenzen*

Charakteristisch für die Lage ist das zunehmende Bewußtsein der Notwendigkeit zu handeln. In Ermangelung einer Konzertierungsinitiative ist es jedoch sehr wahrscheinlich, daß verstreute Maßnahmen in verschiedenen Bereichen ergriffen werden und damit in der Praxis eine widersprüchliche Situation entsteht, die nach und nach zu ernsthaften rechtlichen, gesellschaftlichen und wirtschaftlichen Problemen führt.

1.4. *Anforderungen, Optionen und Prioritäten*

Innerhalb eines solchen Rahmens wären Risikoanalyse und Risikomanagement zu behandeln und abzugrenzen; diese betreffen die Gefährdungen von Informationsdiensten, die Angleichung von Gesetzen und Regelungen im Zusammenhang mit dem Mißbrauch von Computern und Telekommunikationsdiensten, Verwaltungsinfrastrukturen einschließlich Sicherheitspolitiken und die Frage, wie sich diese in verschiedenen Industrien/Disziplinen effizient einführen lassen, und schließlich Bereiche des Gesellschaftslebens und der Privatsphäre (z. B. die Einführung von Plänen für Identifizierung, Authentifizierung, Nachweisbarkeit und gegebenenfalls Zugangsberechtigung in einem demokratischen Umfeld).

Es bedarf einer klaren Ausrichtung für die Entwicklung physischer und logischer Architekturen für sicher verteilte Informationsdienste, Normen, Leitlinien und Definitionen für Sicherheitsprodukte und -dienste, Pilotprojekte und Prototypen, um die Brauchbarkeit verschiedener Verwaltungsstrukturen auf den Bedarf spezifischer Bereiche ausgelegter Architekturen und Normen zu ermitteln.

Es muß ein Sicherheitsbewußtsein geschaffen werden, damit die Benutzer die Sicherheit in der Informationstechnologie (IT) zu ihrem eigenen Anliegen machen.

2. Aktionslinie II — Ermittlung der Anforderungen der Benutzer und Diensteanbieter an die Sicherheit von Informationssystemen

2.1. *Problematik*

Die Sicherheit von Informationssystemen ist die unerläßliche Voraussetzung für Integrität, die Zuverlässigkeit kommerzieller Anwendungen, den Schutz des geistigen Eigentums und die Vertraulichkeit der Daten. Dies führt unweigerlich zu einem empfindlichen Gleichgewicht und erfordert gelegentlich eine Wahl zwischen einem Engagement für den freien Handel und einem Engagement für den Schutz der Privatsphäre und des geistigen Eigentums. Diese Entscheidungen und Kompromisse müssen auf einer Gesamteinschätzung der Notwendigkeiten und der Auswirkungen möglicher Optionen auf dem Gebiet der Sicherheit von Informationssystemen basieren, um diesen Notwendigkeiten zu entsprechen.

Die Benutzeranforderungen umfassen die Sicherheitsfunktionen von Informationssystemen in Verbindung mit technologischen, operationellen und ordnungspolitischen Aspekten. Daher ist eine systematische Untersuchung der Anforderungen an die Sicherheit von Informationssystemen für die Entwicklung geeigneter und wirksamer Maßnahmen unerläßlich.

2.2. *Zielsetzung*

Ermittlung der Anforderungen (Art und Merkmale) der Benutzer und Diensteanbieter und ihre Beziehung zu Maßnahmen auf dem Gebiet der Sicherheit von Informationssystemen.

2.3. *Derzeitiger Stand und Tendenzen*

Bislang wurden keine konzertierten Maßnahmen ergriffen, um die sich rasch und ständig wandelnden Anforderungen der Hauptakteure an die Sicherheit von Informationssystemen zu ermitteln. Die Mitgliedstaaten der Gemeinschaft haben den Harmonisierungsbedarf der nationalen Tätigkeiten (insbesondere in bezug auf „Bewertungskriterien für IT-Sicherheit") festgelegt. Einheitliche Bewertungskriterien und Regeln für die gegenseitige Anerkennung der Bewertungszertifikate sind von grundlegender Bedeutung.

2.4. *Anforderungen, Optionen und Prioritäten*

Als Grundlage für eine kohärente und transparente Behandlung der fundierten Bedürfnisse der Akteure ist eine abgestimmte Klassifizierung der Benutzeranforderungen und ihrer Beziehungen zu den Maßnahmen zur Gewährleistung der Sicherheit von Informationssystemen zu entwickeln.

Ferner sind die Anforderungen an Rechts- und Verwaltungsvorschriften und Verfahrensregeln festzulegen. Dabei sind die aktuellen Trends der Dienstmerkmale und Technologien zu berücksichtigen, um alternative Strategien zur Erreichung der Ziele durch administrative, dienstspezifische, operationelle und technische Bestimmungen zu entwickeln. Des weiteren sind die Wirksamkeit, Benutzerfreundlichkeit und Kosten alternativer Optionen und Strategien der Sicherheit von Informationssystemen für Benutzer, Diensteanbieter und Netz-Betreiber einzuschätzen.

3. Aktionslinie III — Lösungen für den kurz- und mittelfristigen Bedarf von Benutzern, Lieferanten und Diensteanbietern

3.1. *Problematik*

Computer können heutzutage gegen unberechtigten externen Zugriff durch „Isolierung", d. h. konventionelle organisatorische und technische Maßnahmen, hinreichend geschützt werden. Dies gilt auch für die elektronische Kommunikation, die innerhalb einer geschlossenen Benutzergruppe über ein dediziertes Netz abgewickelt wird. Eine ganz andere Situation ergibt sich, wenn Informationen mehreren Benutzergruppen zur Verfügung stehen oder über ein öffentliches bzw. allgemein zugängliches Netz ausgetauscht werden. Hier stehen grundsätzlich weder die Technologien, Endgeräte und Dienste noch die entsprechenden Normen und Verfahren zur Verfügung, um eine vergleichbare Sicherheit von Informationssystemen zu gewährleisten.

3.2. *Zielsetzung*

Ziel ist es, kurzfristig Lösungen zu erarbeiten, die dem dringendsten Bedarf von Benutzern, Diensteanbietern und Herstellern gerecht werden. Dies schließt die Anwendung gemeinsamer IT-Sicherheitsbewertungskriterien mit ein. Sie sollten offen konzipiert sein, um auch künftige Anforderungen und Lösungen zu berücksichtigen.

3.3. *Derzeitiger Stand und Tendenzen*

Einige Benutzergruppen haben Techniken und Verfahren für ihre speziellen Anwendungen entwickelt, die insbesondere dem Bedarf an Authentifizierung, Integrität und Nachweisbarkeit gerecht werden. In der Regel werden Magnet- oder Chipkarten verwendet. Teilweise bedient man sich mehr oder weniger ausgefeilter Verschlüsselungstechniken. Hierzu sind häufig benutzergruppenspezifische „Instanzen" zu definieren. Eine allgemeine Anwendung dieser Techniken und Verfahren erweist sich angesichts der Anforderungen einer offenen Umgebung jedoch als schwierig.

Die ISO entwickelt derzeit eine OSI-Informationssicherheitsnorm (ISO DIS 7498-2), während der CCITT diese Frage im Zusammenhang mit dem X.400 bearbeitet. Eine Möglichkeit besteht darin, Sicherheitssegmente in die Nachrichten zu integrieren. Authentifizierung, Integrität und Nachweisbarkeit werden als Teil der Nachrichten (EDIFACT) und des Systems X.400 MHS behandelt.

Gegenwärtig befindet sich der rechtliche Rahmen für den elektronischen Datenaustausch noch in der Entwicklungsphase. Die Internationale Handelskammer hat einheitliche Verhaltensregeln für den Austausch von kommerziellen Daten über Telekommunikationsnetze veröffentlicht.

Mehrere Länder (z. B. Deutschland, Frankreich, das Vereinigte Königreich und die USA) haben Kriterien zur Bewertung der Vertrauenswürdigkeit von IT-Produkten und -Systemen sowie entsprechende Bewertungsverfahren entwickelt bzw. in Arbeit. Diese Kriterien wurden mit den nationalen Herstellern koordiniert und werden in zunehmendem Maße die Entwicklung zuverlässiger Produkte und Systeme, ausgehend von einfachen Produkten, ermöglichen. Dieser Trend wird durch die Einrichtung nationaler Organisationen unterstützt, die Bewertungen durchführen und Zertifikate erteilen.

Maßnahmen zur Wahrung der Vertraulichkeit werden von den meisten Benutzern für weniger dringend erachtet. Künftig wird sich diese Lage jedoch angesichts der allgemeinen Verbreitung moderner Kommunikationsdienste, insbesondere der Mobilfunkdienste, voraussichtlich ändern.

3.4. *Anforderungen, Optionen und Prioritäten*

Die Verfahren, Normen, Produkte und Werkzeuge zur Gewährleistung der Sicherheit von Informationssystemen als solchen (z. B. Computer und Peripheriegeräte) und von öffentlichen Kommunikationsnetzen müssen umgehend entwickelt werden. Hohe Priorität kommt dabei der Authentifizierung, Integrität und Nachweisbarkeit zu. Pilotprojekte sind durchzuführen, um die vorgeschlagenen Lösungen auf ihre Eignung zu prüfen. Lösungen für prioritäre Anforderungen im Bereich des elektronischen Datenaustausches werden mit dem Programm TEDIS angestrebt, das sich in den breiteren Rahmen dieses Aktionsplans einfügt.

4. Aktionslinie IV — Entwicklung von Spezifikationen, Normung, Bewertung und Zertifizierung der Sicherheit von Informationssystemen

4.1. *Problematik*

Anforderungen an die Sicherheit von Informationssystemen stellen sich in allen Bereichen; daher sind gemeinsame Spezifikationen und Normen unerläßlich. Solange keine abgestimmten Normen und Spezifikationen für die IT-Sicherheit vorliegen, können sich daraus wesentliche Hindernisse für den Fortschritt informationsgestützter Vorgänge und Dienste in der gesamten Wirtschaft und Gesellschaft ergeben. Es müssen auch Maßnahmen ergriffen werden, um die Entwicklung und den Einsatz von Technologien und Normen in verschiedenen zusammenhängenden Kommunikations- und Computernetzen zu beschleunigen, die für Benutzer, Industrieunternehmen und Verwaltungen von ausschlaggebender Bedeutung sind.

4.2. *Zielsetzung*

Es sind Maßnahmen zu treffen, um die Unterstützung und Durchführung spezieller Sicherheitsfunktionen in den allgemeinen Bereichen OSI, ONP, ISDN/IBC und Netzmanagement zu ermöglichen. In engem Zusammenhang mit der Normung und Spezifikation stehen die notwendigen Überprüfungstechniken und -konzepte, einschließlich der Zertifizierung zum Zwecke der gegenseitigen Anerkennung. Soweit möglich, sind international vereinbarte Lösungen zu unterstützen. Die Entwicklung und Anwendung von Computersystemen mit Sicherheitsfunktionen sollte ebenfalls gefördert werden.

4.3. *Derzeitiger Stand und Tendenzen*

Vor allem die USA haben größere Initiativen zur Frage der Sicherheit von Informationssystemen ergriffen. In Europa wird dieses Thema von ETSI und CEN/CENELEC im Zusammenhang mit der IT- und Telekommunikationsnormung als Vorbereitung der entsprechenden Arbeiten des CCITT und der ISO behandelt.

Da dieses Thema immer mehr in den Brennpunkt rückt, werden die Arbeiten in den USA zügig vorangetrieben; Lieferanten und Diensteanbieter verstärken ihre Bemühungen in diesem Bereich. In Europa haben Frankreich, Deutschland und das Vereinigte Königreich unabhängig voneinander ähnliche Tätigkeiten aufgenommen; ein gemeinsamer Verstoß wie in den USA zeichnet sich jedoch nur zögernd ab.

4.4. *Anforderungen, Optionen und Prioritäten*

Im Bereich der Sicherheit von Informationssystemen besteht zwangsläufig eine enge Verbindung zwischen ordnungspolitischen, operationellen, administrativen und technischen Aspekten. Bei den Normen sind die rechtlichen Vorschriften zu berücksichtigen; Maßnahmen zur Gewährleistung der Sicherheit von Informationssystemen müssen nachweislich den Normen und Vorschriften entsprechen. In mehrfacher Hinsicht erfordern Vorschriften Spezifikationen, die über den traditionellen Bereich der Normung hinausgehen, d. h. Verfahrensregeln beinhalten. Anforderungen an Normen und Verfahrensregeln gibt es in allen Bereichen der Sicherheit von Informationssystemen. Dabei ist zu unterscheiden zwischen den Schutzanforderungen, die den Sicherheitszielen entsprechen, und einigen technischen Anforderungen, mit deren Erfüllung die zuständigen europäischen Normungsgremien (CEN/CENELEC/ETSI) beauftragt werden können.

Spezifikationen und Normen müssen zahlreiche Bereiche der Informationssysteme abdecken; ihre Sicherheitsdienste (Authentifizierung von Personen und Unternehmen, Protokolle für die Nachweisbarkeit, rechtlich zulässige elektronische Belege, Berechtigungskontrolle), ihre Kommunikationsdienste (Schutz der Privatsphäre bei Bild-, Mobil- und Datenkommunikation, Schutz von Daten- und Bildbanken, Sicherheit integrierter Dienste), ihr Kommunikations- und Sicherheitsmanagement (öffentliche/private Schlüsselsysteme für offenen Netzbetrieb, Schutz des Netzmanagements, Schutz der Diensteanbieter) und ihre Zertifizierung (Kriterien und Stufen der Sicherheit, Verfahren zur Gewährleistung der Sicherheit für sichere Informationssysteme).

5. Aktionslinie V — Technologische und funktionale Entwicklungen auf dem Gebiet der Sicherheit von Informationssystemen

5.1. *Problematik*

Voraussetzung für die Entwicklung des Dienstemarktes und der Wettbewerbsfähigkeit der europäischen Wirtschaft insgesamt ist die systematische Erforschung und Entwicklung der Technologien, um wirtschaftlich rentable und operationell zufriedenstellende Lösungen für eine Reihe gegenwärtiger und künftiger Anforderungen an die Sicherheit von Informationssystemen zu erarbeiten.

Bei technologischen Entwicklungen im Hinblick auf die Sicherheit der Informationssysteme sind grundsätzlich Aspekte sowohl der Computersicherheit als auch der Kommunikationssicherheit zu berücksichtigen, da es sich bei den heutigen Systemen überwiegend um verteilte Systeme handelt und der Zugang über Kommunikationsdienste erfolgt.

5.2. *Zielsetzung*

Systematische Erforschung und Entwicklung der Technologien, um wirtschaftlich rentable und operationell zufriedenstellende Lösungen für eine Reihe gegenwärtiger und künftiger Anforderungen an die Sicherheit von Informationssystemen zu erarbeiten.

5.3. *Anforderungen, Optionen und Prioritäten*

Die Arbeiten im Bereich der Sicherheit von Informationssystemen betreffen Entwicklungs- und Implementierungsstrategien, Technologien, Integration und Überprüfung.

Die strategischen FuE-Arbeiten müssen theoretische Modelle für sichere Systeme (gesichert gegen Sicherheitsverletzungen, unberechtigte Änderungen und Dienstleistungsverhinderung), Modelle der Funktionsanforderungen, Risikomodelle und Sicherheitsarchitekturen abdecken.

Die technologischen FuE-Arbeiten müssen die Authentifizierung von Benutzern und Nachrichten (z. B. durch Stimmerkennung und elektronische Unterschriften), technische Schnittstellen und Protokolle für die Verschlüsselung, Zugriffskontrollmechanismen und Implementierungsverfahren für nachweislich sichere Systeme abdecken.

Integrations- und Überprüfungsprojekte dienen der Verifikation und Validierung der Sicherheit des technischen Systems und seiner Anwendbarkeit.

Über die Entwicklung und Konsolidierung von Sicherheitstechnologien hinaus sind eine Reihe von flankierenden Maßnahmen notwendig. Diese betreffen die Erstellung, Aktualisierung und konsequente Anwendung von Normen sowie die Validierung und Zertifizierung von IT- und Telekommunikationsprodukten in bezug auf ihre Sicherheitsmerkmale ; dazu gehören auch die Validierung und Zertifizierung von Verfahren zum Entwurf und zur Implementierung der Systeme.

Aufgrund des dritten FTE-Rahmenprogramms der Gemeinschaft können kooperative Projekte auf vorwettbewerblicher und pränormativer Ebene gefördert werden.

6. Aktionslinie VI — Maßnahmen zur Gewährleistung der Sicherheit von Informationssystemen

6.1. *Problematik*

Je nach Art der erforderlichen Sicherheitsmerkmale der Informationssysteme sind die Funktionen an verschiedenen Stellen des Informationssystems zu integrieren. Hierzu gehören Endgeräte/Computer/Dienste, Netzmanagement ebenso wie Verschlüsselungsgeräte, Chipkarten, öffentliche und private Schlüssel usw. Einige Funktionen können voraussichtlich vom Hersteller in die Hard- oder Software integriert werden, während andere Bestandteil verteilter Systeme sind (z. B. Netzmanagement), sich im Besitz des einzelnen Benutzers befinden (z. B. Chipkarten) oder von einer besonderen Organisation geliefert werden (z. B. öffentliche/private Schlüssel).

Sicherheitsprodukte und -dienste dürften überwiegend von Herstellern, Diensteanbietern oder Netz-Betreibern bereitgestellt werden. Für spezielle Funktionen, z. B. die Zuteilung öffentlicher/privater Schlüssel, Überwachung oder Berechtigungskontrolle, müssen gegebenenfalls entsprechende Organisationen bestimmt und beauftragt werden.

Gleiches gilt für die Zertifizierung, Bewertung und Überprüfung der Dienstqualität. Diese Aufgaben müssen von Organisationen wahrgenommen werden, die von den Interessen der Hersteller, Diensteanbieter und Netz-Betreiber nicht beeinflußt werden. Dies können private oder staatliche Organisationen sein oder solche, die eine staatliche Lizenz zur Ausübung bestimmter Funktionen besitzen.

6.2. *Zielsetzung*

Um die harmonische Entwicklung der Sicherheit von Informationssystemen in der Gemeinschaft im Hinblick auf den Schutz öffentlicher und geschäftlicher Interessen zu fördern, ist ein kohärentes Konzept für die Maßnahmen zu entwikkeln, mit denen die Sicherheit von Informationssystemen gewährleistet werden soll. Soweit damit unabhängige Organisationen beauftragt werden müssen, sind ihre Funktionen und Bedingungen festzulegen und abzustimmen und nach Bedarf in den ordnungspolitischen Rahmen zu integrieren. Ziel ist es, eine klar definierte und abgestimmte Verteilung der Zuständigkeiten unter den verschiedenen Akteuren auf Gemeinschaftsebene als Voraussetzung für die gegenseitige Anerkennung zu erreichen.

6.3. *Derzeitiger Stand und Tendenzen*

Zum gegenwärtigen Zeitpunkt sind Maßnahmen auf dem Gebiet der Sicherheit von Informationssystemen nur in bestimmten Bereichen durchorganisiert und beschränken sich auf spezielle Bedürfnisse. Die Organisation auf europäischer Ebene ist zumeist informell und die gegenseitige Anerkennung der Überprüfung und Zertifizierung, ausgenommen in geschlossenen Gruppen, noch nicht eingeführt. Mit der zunehmenden Bedeutung der Sicherheit von Informationssystemen wird die Festlegung eines kohärenten Konzepts für die Maßnahmen zur Gewährleistung der Sicherheit von Informationssystemen in Europa und international zu einem dringenden Anliegen.

6.4. *Anforderungen, Optionen und Prioritäten*

Angesichts der Zahl der betroffenen Akteure und des engen Zusammenhangs mit ordnungspolitischen und gesetzgeberischen Fragen muß in erster Linie eine Einigung über die Grundsätze erzielt werden, die für die Maßnahmen zur Gewährleistung der Sicherheit von Informationssystemen gelten sollen.

Bei der Entwicklung eines kohärenten Konzepts zu dieser Frage sind die Aspekte der Festlegung und Spezifikation von Funktionen zu prüfen, die unabhängige Organisationen (bzw. kooperierende Organisationen) erfordern. Dies gilt unter anderem für Funktionen wie die Verwaltung eines öffentlichen/privaten Schlüsselsystems.

Ferner sind zu einem frühen Zeitpunkt die Funktionen festzulegen und zu spezifizieren, die im öffentlichen Interesse unabhängigen Organisationen (bzw. kooperierenden Organisationen) übertragen werden müssen. Dazu könnten beispielsweise die Überwachung, Qualitätssicherung, Überprüfung, Zertifizierung und ähnliche Funktionen gehören.