KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 6.6.2001
KOM(2001)298 endgültig

MITTEILUNG DER KOMMISSION AN DEN RAT, DAS EUROPÄISCHE PARLAMENT, DEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz

MITTEILUNG DER KOMMISSION AN DEN RAT, DAS EUROPÄISCHE PARLAMENT, DEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Sicherheit der Netze und Informationen:
Vorschlag für einen europäischen Politikansatz

EXECUTIVE SUMMARY

I.

Sicherheit ist auf dem Weg, eine Priorität zu werden, weil Kommunikations- und Informationsinfrastrukturen ein wichtiger Faktor für wirtschaftliche und soziale Entwicklung geworden sind. Netze und Informationssysteme ermöglichen Dienstleistungen und übertragen Daten in einem Maße, in dem dies noch vor wenigen Jahren unvorstellbar war. Ihre Verfügbarkeit ist für andere Infrastrukturen wie etwa Wasser- oder Stromversorgung unerläßlich. Je mehr jedermann, ob Unternehmen, Bürger oder öffentliche Verwaltungen die Möglichkeiten der Kommunikationsnetze nutzen möchte, desto mehr wird die Sicherheit dieser Systeme zu einer Voraussetzung für weiteren Fortschritt.

Vor diesem Hintergrund hat der Europäischen Rat auf seiner Tagung vom 23.-24. März 2001 in Stockholm die Schlußfolgerung gezogen, daß *„der Rat in Zusammenarbeit mit der Kommission eine umfassende Strategie für die Sicherheit elektronischer Netze einschließlich praktischer Durchführungsmaßnahmen entwickeln wird. Diese Strategie sollte rechtzeitig für die Tagung des Europäischen Rates in Göteborg vorliegen.“* Die vorliegende Mitteilung stellt die Antwort der Europäischen Kommission auf diese Forderung dar.

II.

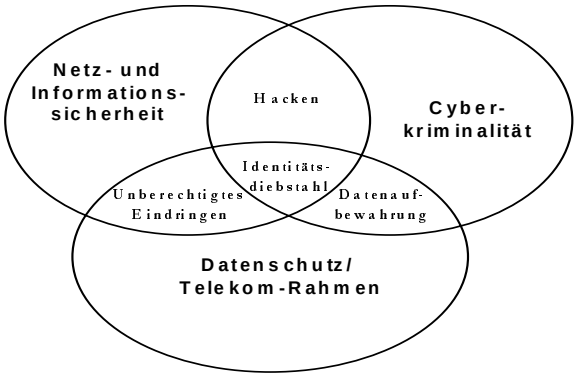
Sicherheit ist eine wichtige Herausforderung für die Politik geworden, doch wird das auffinden einer angemessenen Antwort immer komplexer. Kommunikationsdienste werden nicht mehr von öffentlichen Telekomverwaltungen angeboten, sondern im Wettbewerb zwischen vielen privaten Anbietern und Dienstleistungserbringern, und mehr und mehr auf europäischem und weltweitem Niveau. Die Netze konvergieren: sie können dieselben Dienste erbringen, sind zunehmend miteinander verbunden und benutzen teilweise dieselbe Infrastruktur.

Um ein minimales Sicherheitsniveau zu garantieren ist eine umfangreiche Gesetzgebung als Teil des Telekommunikationsrahmens und des Datenschutzrechts sowohl auf einzelstaatlicher als auch auf EU-Ebene geschaffen worden. Diese gesetzgeberischen Vorgaben müssen in einer sich schnell verändernden Umgebung effektiv angewandt werden. Sie müssen sich außerdem weiterentwickeln, wie man am bereits vorgeschlagenen neuen Regulierungsrahmen für elektronische Kommunikationen oder den Vorschlägen im Zusammenhang mit der Diskussion über die Cyber-Kriminalität sehen kann. Die Politik benötigt deshalb ein Verständnis der grundlegenden Sicherheitsthemen und ihrer Bedeutung bei der Verbesserung der Sicherheit.

Sicherheit ist eine Ware, die auf dem Markt gehandelt wird und Gegenstand vertraglicher Vereinbarungen zwischen verschiedenen Parteien ist. Normalerweise geht man implizit davon aus, daß der Preis die Kosten der Sicherheit mit den spezifischen Sicherheitsanforderungen in

Einklang bringt. Viele Sicherheitsrisiken bleiben jedoch als Ergebnis von Marktversagen ungelöst, oder werden verspätet gelöst. **Spezifische politische Maßnahmen können das Marktgeschehen verbessern und gleichzeitig das Funktionieren des rechtlichen Rahmens erleichtern.** Solche Maßnahmen müssen in einem Europäischen Ansatz aufgehen, um den Binnenmarkt zu sichern, von gemeinsamen Lösungen zu profitieren und auf globaler Ebene effektiv handeln zu können.

Die vorgeschlagenen politischen Maßnahmen in bezug auf Netz- und Informationssicherheit müssen im Zusammenhang der bestehenden Telekommunikations- und Datenschutzgesetzgebung sowie zur Bekämpfung der Cyberkriminalität gesehen werden. Eine Politik auf dem Gebiet der Netz- und Informationssicherheit wird die Lücke in diesem politischen Rahmen schließen. Die folgende Grafik zeigt die drei Politikansätze und ihre Wechselbeziehungen anhand einiger Beispiele:



III.

Die Netz- und Informationssicherheit kann verstanden werden als die Fähigkeit eines Netzes oder Informationssystems, mit einem vorgegebenen Niveau Störungen oder böswilligen Aktionen abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von gespeicherten oder übermittelten Daten und damit zusammenhängenden Diensten, die über dieses Netz oder Informationssystem angeboten werden bzw. zugänglich sind, beeinträchtigen. Solche Sicherheitszwischenfälle können wie folgt gruppiert werden:

- Elektronische Kommunikation kann abgehört und Daten können kopiert oder verändert werden. Dabei entsteht Schaden sowohl durch das Einringen in die Privatsphäre als auch durch die Verwertung der abgehörten Daten.

- Unberechtigter Zugang zu einem Computer oder einem Computernetz erfolgt zumeist in der böswilligen Absicht, Daten zu kopieren, zu verändern oder zu zerstören.

- Disruptive Angriffe auf das Internet sind inzwischen recht verbreitet, und die Telefonnetze könnten demnächst ebenfalls anfälliger werden.

- Bösartige software, z.B. ein Virus, kann Computer zerstören und Daten vernichten oder verändern. Einige der jüngsten Virus-Attacken waren sehr zerstörerisch und teuer.

- Eine Vortäuschung von Personen oder Körperschaften kann erheblichen Schaden verursachen. Kunden können bösartige Software von einer Webseite herunterladen, die als verläßliche Quelle maskiert ist. Vertrauliche Informationen können an die falsche Person herausgegeben, Verträge nicht anerkannt werden.

- Viele Sicherheitszwischenfälle gehen von unvorhergesehenen und unabsichtlichen Ereignissen aus, wie z. B. Naturkatastrophen (Überschwemmungen, Stürme, Erdbeben), Geräte- oder Softwareausfall, oder menschliches Versagen.

IV.

Die vorgeschlagenen Maßnahmen:

- **Sensibilisierung:** Eine öffentliche Informationskampagne sollte stattfinden, und die besten Lösungen sollten gefördert werden.

- **Ein europäisches Warn- und Informationssystem:** Die Mitgliedstaaten sollten ihre CERT verstärken und die Koordinierung untereinander verbessern. Die Kommission wird zusammen mit den Mitgliedstaaten untersuchen, wie die Datensammlung, Analyse und Planung von in die Zukunft gerichteten Antworten auf bestehende und neu entstehende Sicherheitsrisiken am besten organisiert werden kann.

- **Förderung des technischen Fortschritts:** Die Förderung von Forschung und Entwicklung im Bereich der Sicherheit sollte ein Hauptkomponent im 6. Rahmenprogramm sein und mit der umfassenden Strategie für verbesserte Netz- und Informationssicherheit verbunden werden.

- **Förderung von marktorientierter Standardisierungs- und Zertifizierung:** Die Europäischen Standardisierungsorganisationen werden aufgefordert, die Arbeiten über Kompatibiltät zu beschleunigen; die Kommission wird auch weiterhin elektronische Signaturen und die weitere Entwicklung von IPv6 und IPSec fördern; die Kommission wird die Notwendigkeit einer rechtlichen Initiative zur gegenseitigen Anerkennung von Zertifikaten überprüfen; die Mitgliedstaaten sollten alle betreffenden Sicherheitsstandards überprüfen.

- **Rechtlicher Rahmen**: Die Kommission wird eine Inventar einzelstaatlicher Maßnahmen erstellen, die im Einklang mit dem entsprechenden Gemeinschaftsrecht erfolgt sind. Die Mitgliedstaaten sollten den freien Verkehr von Verschlüsselungsprodukten fördern und Anreize für Investitionen in Sicherheitsprodukte schaffen. Die Kommission wird gesetzgeberische Maßnahmen gegen Cyber-Kriminalität vorschlagen.

- **Sicherheit bei der Anwendung durch staatliche Stellen:** Die Mitgliedstaaten sollten effektive und kompatible Sicherheitslösungen in ihre „Regierung am Netz“ und „elektronische Beschaffung“-programme integrieren. Sie sollten elektronische Signaturen für öffentliche Dienste einführen. Die Kommission wird die Sicherheitsvorkehrungen in ihrem Informations- und Kommunikationssytem verbessern.

- **Internationale Zusammenarbeit:** Die Kommission wird den Dialog über Netz- und Informationssicherheit mit internationalen Organisationen und Partnern verstärken.

V.

Als nächster Schritt müssen dieser Rahmen und die vorgeschlagenen Aktionen von den Mitgliedstaaten und dem Europäischen Parlament diskutiert werden. Der Europäische Rat könnte am 15./16. Juni in Göteborg die Richtung für das weitere Vorgehen aufzeigen.

Die Kommission schlägt vor, eine ausführliche Diskussion mit der Industrie und den Nutzern über die praktischen Einzelheiten der Durchführung der vorgeschlagenen Aktionen in Gang

zu bringen. Kommentare können bis Ende August 2001 an eeurope@cec.eu.int. Deshalb ist diese Mitteilung auch eine Aufforderung zur Stellungnahme der betroffenen Parteien im Hinblick auf die Definition eines endgültigen Maßnahmenkatalogs. Dieser könnte bis Ende 2001 zu einem Konzept entwickelt werden.

***

Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz

Inhaltsverzeichnis

1. Einführung

Mit der raschen Zunahme der Zahl der Netzbenutzer und dem zunehmenden Wert ihrer Transaktionen ist auch die Sicherheit von elektronischen Netzen zu einem immer wichtigeren Anliegen geworden. Sicherheit ist heute an einem Punkt angelangt, an dem sie eine Voraussetzung für das Wachstum des elektronischen Geschäftsverkehrs und das Funktionieren der Wirtschaft allgemein darstellt. Verschiedene Faktoren haben dazu beigetragen, daß die Sicherheit von Information und Kommunikation zu einem der wichtigsten politischen Anliegen der EU geworden ist:

- Die Regierungen haben erkannt, in welchem Maße ihre Bürger und ihre Wirtschaft auf effektiv funktionierende Kommunikationsnetze angewiesen sind, und einige von ihnen haben begonnen, ihre Sicherheitsvorkehrungen zu überprüfen.

- Durch das Internet ist eine weltweite Vernetzung entstanden, durch die Millionen von großen und kleinen Netzen und viele hundert Millionen PC sowie in zunehmendem Maße auch andere Geräte einschließlich mobiler Telefone) miteinander verbunden sind. Dadurch können Angreifer von überall mit deutlich geringerem Aufwand auf wertvolle Wirtschaftsinformationen zugreifen.

- Es hat bereits einige bekannte Fälle von ins Internet eingeschleusten Viren gegeben, die Informationen zerstört, das Netz blockiert und dadurch großen Schaden angerichtet haben. Solche Sicherheitsprobleme sind nicht auf einzelne Staaten begrenzt, sonder überqueren schnell die Grenzen.

- Beim Start des Aktionplans "*e*Europe 2002" wurde auf den Tagungen des Europäischen Rates in Lissabon und Feira anerkannt, daß das Internet einen Motor für die Produktivität der Volkswirtschaften innerhalb der EU darstellt.

Vor diesem Hintergrund hat der Europäischen Rat auf seiner Tagung vom 23.-24. März 2001 in Stockholm die Schlußfolgerung gezogen, daß *„der Rat in Zusammenarbeit mit der Kommission eine umfassende Strategie für die Sicherheit elektronischer Netze einschließlich praktischer Durchführungsmaßnahmen entwickeln wird. Diese Strategie sollte rechtzeitig für die Tagung des Europäischen Rates in Göteborg vorliegen.*" Die vorliegende Mitteilung stellt die Antwort der Europäischen Kommission auf diese Forderung dar.

Neue Rahmenbeingungen

Die Frage der Sicherheit der Netze ist zu einer wichtigen Herausforderung der Politiker geworden, die auch erkannt haben, daß die Erarbeitung einer angemessenen politischen Antwort eine zunehmend komplexe Aufgabe darstellt. Noch bis vor wenigen Jahren betraf die Frage der Netzsicherheit vorwiegend Staatsmonopole, die über öffentliche Netze Fachdienstleistungen, insbesondere Telefondienstleistungen anboten. Die Sicherheit von Computersystemen war ein Problem für große Organisationen und bestand hauptsächlich aus Zugangskontrollen. In diesem Kontext war die Ausarbeitung einer Sicherheitspolitik eine relativ unkomplizierte Angelegenheit. Heute hat sich die Lage aufgrund zahlreicher Entwicklungen im Kontext erweiterter Märkte, unter anderem durch Liberalisierung, Konvergenz und Globalisierung, deutlich geändert.

Die Netze sind heute vorwiegend in privatem Besitz und werden privat verwaltet. Kommunikationsdienstleistungen werden wettbewerbsorientiert angeboten, und auch Datensicherheit wird auf dem Markt angeboten. Dennoch täuschen sich viele Kunden über

das Ausmaß der Sicherheitsrisiken, denen sie ausgesetzt sind, wenn sie sich mit einem Netz verbinden, und treffen daher ihre Entscheidungen auf der Grundlage unvollständiger Information.

Die Netze und Informationssyteme konvergieren. Sie sind immer stärker untereinander verknüpft, bieten dieselbe Art von durchgehenden und personalisierten Dienstleistungen an und verwenden teilweise dieselbe Infrastruktur. Die Endgeräte (PC, Mobiltelefone usw.) sind zu aktiven Elementen der Netzarchitektur geworden und können an verschiedene Netze angeschlossen werden.

Netze sind international. Ein wichtiger Teil des heutigen Kommunikationsverkehrs überschreitet die Landesgrenzen oder durchquert Drittländer (manchmal ohne daß der Nutzer dies weiß), was bei Lösungen für die Sicherheitsrisiken berücksichtigt werden muß. Zur Erstellung von Netzen werden meist kommerzielle Produkte von internationalen Anbietern verwendet. Sicherheitsprodukte müssen daher mit internationalen Standards kompatibel sein.

Bedeutung für die Politik

Diese Entwicklungen engen die Möglichkeiten der Regierungen ein, auf das Sicherheitsniveau der elektronischen Kommunikation ihrer Bürger und Unternehmen Einfluß zu nehmen. Das bedeutet jedoch nicht, daß die öffentliche Hand keine Rolle mehr spielt, aus mehreren Gründen:

Zum einen **besteht eine Reihe von gesetzlichen Regelungen auf europäischer Ebene, mit spezifischen Auswirkungen auf die Netzsicherheit.** Insbesondere die europäischen Rechtsvorschriften im Bereich der Telekommunikation und des Datenschutzes beinhalten Bestimmungen für Betreiber und Dienstanbieter, durch die für ein den Risiken angemessenes Sicherheitsniveau gesorgt werden soll. Zum anderen besteht wachsende Sorge um die **nationale Sicherheit**, da die Informationssysteme und Kommunikationsnetze zu einem kritischen Faktor für andere Infrastruktur (z. B. Wasser- und Stromversorgung) sowie andere Märkte (z. B. die weltweiten Finanzmärkte) geworden sind.

Und schließlich gibt es gute Gründe, warum die Regierungen handeln müssen, um auf **Schwächen des Marktes** zu reagieren. Die Marktpreise spiegeln nicht immer Kosten und Nutzen von Investitionen in verbesserte Netzsicherheit wider und weder Anbieter noch Nutzer müssen immer für alle Folgen ihres Verhaltens geradestehen. Die Kontrolle über das Netz ist auf eine Vielzahl von Stellen verteilt, und Schwächen in einem System können für einen Angriff auf ein anderes ausgenutzt werden. Aufgrund der Komplexität der Netze ist es für die Nutzer nicht leicht, potentielle Gefahren richtig einzuschätzen.

Sie zielt darauf ab, die Rolle der öffentlichen Hand bezüglich spezieller Maßnahmen zur Verbesserung der Sicherheit der Kommunikationsnetze und Informationssysteme zu definieren.

In **Kapitel 2** wird Netzsicherheit definiert, es werden die wichtigsten Sicherheitsrisiken beschrieben und die heutigen Lösungen bewertet. Das Kapitel soll eine Wissensgrundlage über die Netz- und Informationssicherheit vermitteln, anhand der die vorgeschlagenen politischen Lösungen verstanden werden können. Es ist nicht beabsichtigt, einen umfassenden technischen Überblick über Sicherheitsfragen zu geben.

In **Kapitel 3** wird einen europäischen Politikansatz zur Verbesserung der Netzsicherheit vorgeschlagen. Grundlage ist eine Analyse des Bedarfs an einer Ergänzung der auf dem Markt vorhandenen Lösungen durch politische Maßnahmen. In diesem Kapitel wird eine Reihe von konkreten politischen Maßnahmen aufgeführt, wie es der Europäische Rat in Stockholm gefordert hat. Die vorgeschlagene Strategie sollte als integrales Element des bestehenden Rahmens für elektronische Kommunikationsdienste, Datenschutz und – in jüngster Zeit – Cyberkriminalität gesehen werden.

2. Analyse von Fragen der Netz- und Informationssicherheit

2.1. Was bedeutet Netz- und Informationssicherheit?

Netze sind Systeme, in denen Daten gespeichert oder verarbeitet werden und durch die Daten fließen. Sie bestehen aus Übertragungs- bzw. Hardware-Komponenten (Kabel, drahtlose Verbindungen, Satelliten, Router, Gateways, Switches usw.) und den dazu gehörigen Diensten (System von Bereichsnamen (DNS) einschließlich der Root-Server, Anzeige der Rufnummer des Anrufers, Authentifizierung usw.). Daran angeschlossen sind ein zunehmendes Spektrum von Anwendungen (e-mail, browser usw.) sowie Endgeräten (Telefonanlage, Server, PC, Mobiltelefone, ‚Personal Organizer', Haushaltselektronik, Industriemaschinen

Die allgemeinen Anforderungen an Netze und Informationssysteme können in Form der vier folgenden, miteinander verbundenen Merkmalen formuliert werden:

i) **Verfügbarkeit:** Die Daten sind verfügbar und die Dienste können unabhängig von möglichen Störungen wie Stromausfällen, Unfällen, Naturkatastrophen oder Angriffen benutzt werden bzw. sind funktionsfähig. Das ist besonders wichtig in Kontexten, in denen Störungen im Kommunikationsnetz dazu führen können, daß andere wichtige Netze wie der Luftverkehr oder die Stromversorgung zusammenbrechen.

ii) **Authentifizierung:** Die behauptete Identität von Körperschaften oder Nutzern wird bestätigt. Für verschiedene Anwendungen und Dienste wie zum Beispiel den Online-Abschluß von Verträgen, die Kontrolle des Zugangs zu bestimmten Daten und Diensten (z.B. bei Telearbeitern) und die Authentifizierung von Webseiten (z.B. bei Internetbanken) werden geeignete Authentifizierungsmethoden benötigt. Authentifizierung muß ebenfalls die Möglichkeit der **Anonymität** erlauben, da viele Dienstleistungen nicht die Identität der Nutzer, sondern nur einige Kriterien wie etwa die Zahlungsfähigkeit benötigen (sog. anonyme Referenzen).

iii) **Integrität:** Die Daten, die übermittelt, empfangen oder gespeichert werden, sind vollständig und unverändert. Das ist besonders wichtig in Bezug auf die Authentifizierung beim Abschluß von Verträgen, beispielsweise bei vielen geschäftlichen Transaktionen, und wo korrekte Daten unentbehrlich sind (medizinische Daten, industrielles Design)

iv) **Vertraulichkeit:** Hier geht es um den Schutz von Gesprächen oder gespeicherten Daten, so daß sie von unbefugten Personen nicht abgehört oder gelesen werden können. Er wird besonders für die Übertragung empfindlicher Daten gebraucht und ist eine Voraussetzung, um den Datenschutzanforderungen der Nutzer Rechnung zu tragen.

Alle möglicherweise die Sicherheit beeinträchtigenden Ereignisse müssen abgedeckt werden, nicht nur solche, die mit Absicht ausgelöst werden. Aus der Perspektive der

Nutzer sind Bedrohungen wie Umweltereignisse oder menschliches Versagen, die zu Netzzusammenbrüchen führen, möglicherweise ebenso kostspielig wie böswillige Angriffe.

Die Netz- und Informationssicherheit kann daher verstanden werden als die Fähigkeit eines Netzes oder Informationssystems, mit einem vorgegebenen Niveau Störungen oder böswilligen Aktionen abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von gespeicherten oder übermittelten Daten und damit zusammenhängenden Diensten, die über dieses Netz oder Informationssystem angeboten werden bzw. zugänglich sind, beeinträchtigen.

2.2. Überblick über die Sicherheitsrisiken

Unternehmen, die für den Verkauf oder zur Organisation ihrer Lieferungen ein Netz benutzen, können durch eine gezielte Überlastung ihres Servers lahmgelegt werden. Personenbezogene Daten und Finanzdaten können abgefangen und mißbraucht werden. Die nationale Sicherheit kann bedroht werden. Diese Beispiele vermitteln einen Eindruck von den Gefahren, die von einer unzureichenden Netzsicherheit ausgehen. Dabei wird eine Unterscheidung zwischen absichtlichen Angriffen (Unterabschnitte 2.2.1 bis 2.2.5) und unbeabsichtigten Schäden (Unterabschnitt 2.2.6) gemacht. Die möglichen Sicherheitsrisiken werden ausgeführt, um so als Grundlage für die Ausarbeitung eines politischen Rahmens zur Verbesserung der Sicherheit in Abschnitt 3 zu dienen.

2.2.1. Abhörung des Fernmeldeverkehrs

Elektronische Kommunikation kann abgehört und Daten können kopiert oder verändert werden. Die Überwachung kann auf verschiedenste Art und Weise erfolgen. Dazu gehören der physische Zugang zu den Netzleitungen, z. B. das Anzapfen von Telefonleitungen oder auch das Abhören von Funkübertragungen. Die anfälligsten Punkte für das Abhören des Datenverkehrs sind die Netzverwaltung und -steuerung, wie Router, Gateways, Switches und Netzserver.

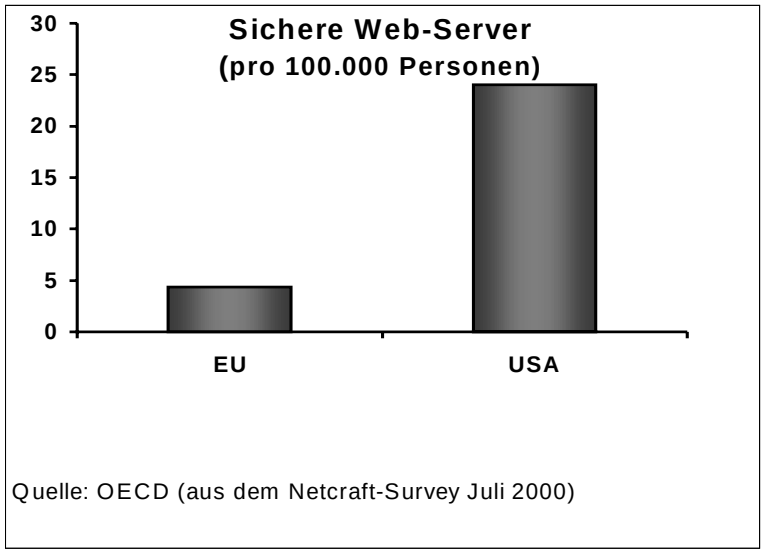
Eine Überwachung des Datenverkehrs, die in böser Absicht oder illegal erfolgt, muß von der rechtmäßigen Überwachung unterschieden werden. Das Abhören von Gesprächen aus Gründen der öffentlichen Sicherheit ist in bestimmten Fällen in begrenztem Rahmen in allen EU-Mitgliedstaaten erlaubt. Es besteht ein rechtlicher Rahmen, der es den Strafverfolgungsbehörden ermöglicht, eine gerichtliche Anordnung, bzw. in zwei Mitgliedstaaten eine von einem leitenden Minister persönlich genehmigte Anordnung zur Überwachung des Fernmeldeverkehr einzuholen.

Möglicher Schaden: Rechtswidriges Abhören von Datenübertragungen kann zum einen durch den Eingriff in die Privatsphäre und zum anderen durch die Nutzung von abgehörten Daten, wie etwa Paßwörtern oder Kreditkartenangaben, zu kommerziellen oder zu Sabotagezwecken Schaden verursachen. Dies wird als eines der größten Hemmnisse für den Durchbruch des elektronischen Geschäftsverkehrs in Europa betrachtet.

Mögliche Lösungen: Für den Schutz gegen ein Abhören der Datenübertragungen können sowohl die **Betreiber** sorgen, indem sie ihre Netze - unter anderem gemäß Richtlinie 97/66 EG[1] - sichern, als auch die **Nutzer**, indem sie die zu übermittelnden Daten verschlüsseln.

Für die **Betreiber** stellt der Schutz ihrer Netze gegen mögliches Abhören eine komplexe und kostspielige Aufgabe dar. Die Betreiber von herkömmlichen Fernsprechdiensten haben die Sicherheit ihrer Netze durch Kontrollen der physischen Anlagen und durch Leitlinien für ihre Beschäftigten gewährleistet. Der Datenverkehr wurde nur gelegentlich verschlüsselt. Wenn drahtlose Lösungen eingesetzt werden, sind die Betreiber verpflichtet, dafür zu sorgen, daß die Funkübertragungen angemessen verschlüsselt werden. Betreiber von Mobiltelefonnetzen verschlüsseln den Datenverkehr zwischen dem Mobiltelefon und der Bodenstation. In den meisten EU-Mitgliedstaaten wird nicht so stark verschlüsselt, wie es technisch möglich wäre, damit eine rechtmäßige Überwachung leichter ist. Aus dem gleichen Grund kann die Verschlüsselung von Funk-Bodenstationen an- und abgedreht werden, ohne daß der Nutzer es bemerkt.

Unabhängig von den Sicherheitsvorkehrungen des Netzes können die **Nutzer** selbst entscheiden, ob sie Daten oder Sprachsignale verschlüsseln oder nicht. Richtig verschlüsselte Nachrichten sind, selbst wenn sie abgefangen werden, für alle außer dem autorisierten Empfänger unverständlich. Verschlüsselungssoftware und –hardware ist für praktisch alle Kommunikationsarten überall erhältlich. [2] Spezielle Produkte sind in der Lage, Telefongespräche oder Übertragungen per Telefax zu verschlüsseln. E-Mails können mit spezieller Software oder mit der im Textverarbeitungsprogramm oder E-Mail-Programm vorhandenen Software verschlüsselt werden. Das Problem für den Nutzer besteht darin, daß der Empfänger in der Lage sein muß, die verschlüsselte E-Mail oder das verschlüsselte Telefonat zu verstehen. Daher müssen die entsprechende Hard- oder Software kompatibel sein. Für die Entschlüsselung müssen sie außerdem den Schlüssel kennen, d.h. es wird ein Verfahren benötigt, den Schlüssel einschließlich seiner Authentifizierung zu übermitteln. Die Kosten von Verschlüsselung, sowohl in Form von Aufwand als auch in Form von Geld, sind erheblich für die Nutzer, zumal sie häufig nicht die Informationen über Risiken und Vorteile besitzen, die ihnen eine optimale Entscheidung ermöglichen würden.



Quelle: OECD (aus dem Netcraft-Survey Juli 2000)

Ein im Internet häufig genutztes Sicherheitssystem nennt sich „Secure Socket Layer“ (SSL). SSL verschlüsselt die Kommunikation zwischen einem Web-Server und dem Web-Browser des Nutzers. Die restriktiven Exportvorschriften der USA in der Vergangenheit waren ein Hemmfaktor für einen Durchbruch dieser Technologie, vor allem ihrer

[1] Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (Amtsblatt L 24 vom 30.01.1998).

[2] Siehe Mitteilung der Kommission „Sicherheit und Vertrauen in elektronische Kommunikation“ vom 8. Oktober 1997, KOM (1997) 503 endg.

leistungsstärksten Version (128 Bit). Das Exportkontrollsystem der USA ist nach Verabschiedung der ‚dual-use'-Verordnung[3] in Europa, die ein liberaleres System für die Kontrolle von Exporten von Gütern und Technologien mit doppeltem Verwendungszweck errichtet, überarbeitet worden. Statistiken belegen, daß die Zahl der sicheren Web-Server in Europa weit hinter der in den USA liegt (siehe Abbildung).

Sowohl die **Betreiber** als auch die **Nutzer** stehen vor dem Problem von miteinander konkurrierenden und nicht-kompatiblen Standards. So konkurrieren beispielsweise im Bereich der sicheren E-Mail zwei Standards [4] um die Vorherrschaft auf dem Markt. In diesem Bereich war der Einfluß Europas bisher recht begrenzt. Das hat dazu geführt, daß es eine Vielzahl nicht-europäischer Produkte mit diesen diese Standards gibt, und der Zugang dazu für europäische Nutzer von der Exportkontrollpolitik der Vereinigten Staaten abhängt. Während bezüglich der Sicherheitsstufe vieler dieser Produkte einige Bedenken bestehen (vgl. Echelon[5]), beabsichtigen einige EU-Mitgliedstaaten, Software mit frei zugänglichem Quellcode einzusetzen, um das Vertrauen in Verschlüsselungsprodukte zu erhöhen. Diese Arbeit befindet sich allerdings erst in einer Versuchsphase[6], ist noch nicht koordiniert, und die Kräfte des Marktes werden sich möglicherweise als stärker erweisen als die Bemühungen einzelner Regierungen. Dieser Punkt kann durch eine umfassende Bewertung sowohl der kommerziellen Produkte als auch der Produkte mit frei zugänglichem Quellcode geklärt werden.

2.2.2. Unberechtigter Zugang zu Computern und Computernetzen

Unberechtigter Zugang zu einem Computer oder einem Computernetz erfolgt zumeist in der böswilligen Absicht, Daten zu kopieren, zu verändern oder zu zerstören. Technisch wird das als Einbruch bezeichnet, der auf vielerlei Arten und Weisen geschehen kann, z. B. indem Insider-Information genutzt wird, durch sog. Wörterbuchangriffe, ‚Brute-Force-Angriffe' (wobei die Tendenz ausgenutzt wird, daß viele Menschen vorhersehbare Paßwörter wählen), ‚social engineering' (wobei die Tendenz ausgenutzt wird, offenbar zuverlässigen Leuten Informationen zu geben) und durch das Abfangen von Paßwörtern. Dies geschieht häufig innerhalb derselben Organisation (interne Angriffe)

Möglicher Schaden: Manches unberechtigte Eindringen in Computernetze ist eher durch die intellektuelle Herausforderung als durch finanziellen Gewinn motiviert. Was aber als (oft als „Hacken" bezeichnete) Störtätigkeit begann, hat deutlich gemacht, wie anfällig Informationsnetze sind, und hat Personen mit kriminellen oder böswilligen Absichten motiviert. Es ist das Recht der Nutzer, sich gegen unerlaubten Zugang zu ihren vertraulichen Daten, insbesondere zu finanziellen Details, zu ihren Bankkonten und zu Informationen über ihre Gesundheit zu schützen. Für die öffentliche Hand und die Wirtschaft reichen die

---

3 Verordnung (EG) Nr. 1334/2000 des Rates vom 22. Juni 2000 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr von Gütern und Technologien mit doppeltem Verwendungszweck, (OJ L 159 vom 30.06.2000).

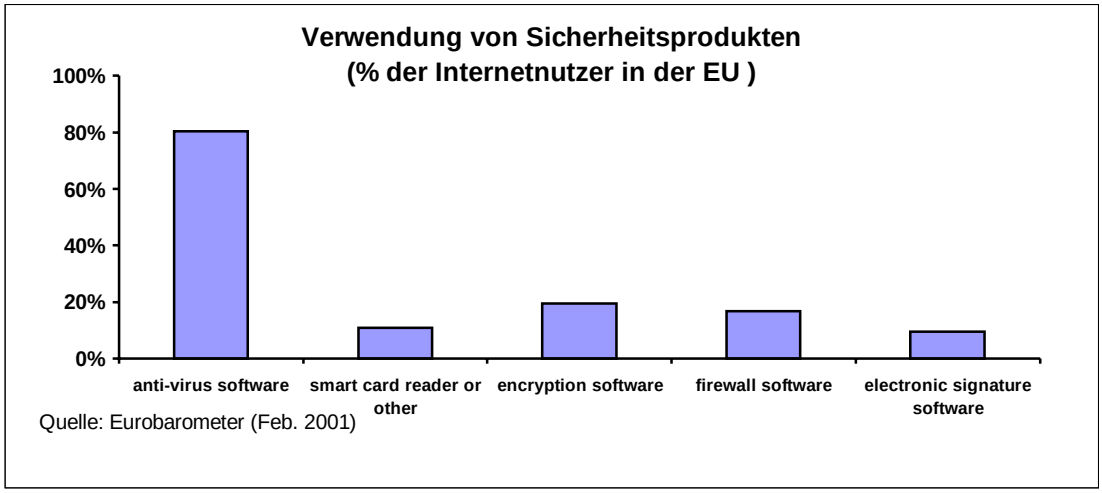
4 S-MIME (Secure Multiple Internet Mail Extensions) und OpenPGP (Pretty Good Privacy) sind beide Standards der IETF (Internet Engineering Task Force).

5 Das ECHELON-System wird anscheinend benutzt, um normale Kommunikation per E-Mail, Fax, Telex und Telefon in den weltweiten Telekommunikationsnetzen abzuhören. Siehe auch die Arbeit des Nichtständigen Ausschusses des Europäischen Parlaments über das Abhörsystem Echelon: http://www.europarl.eu.int/committees/echelon_home.htm

6 Die deutsche Regierung finanziert ein Projekt auf der Grundlage des OpenPGP-Standards mit der Bezeichnung GNUPG (http://www.gnupg.org).

Bedrohungen von Wirtschaftsspionage bis zur potentiellen Veränderung von internen oder öffentlichen Daten, wozu auch die Verfälschung von Webseiten gehört.

Mögliche Lösungen: Die am häufigsten angewandte Methoden, Netze gegen unerlaubten Zugriff zu schützen, sind Paßwortkontrollen und die Installation von ‚Firewalls'. Diese bieten allerdings nur begrenzten Schutz und müssen durch weitere Sicherheitsmaßnahmen ergänzt werden. Möglich wären: Erkennung eines Angriffs, Erkennung des Eindringens, und Überwachung auf Anwendungsebene (einschließlich intelligenter Chipkarten). Die Wirksamkeit dieser Kontrollen hängt davon ab, wie gut sie auf die Risiken der jeweiligen Umgebung eingestellt sind. Es muß eine Abwägung zwischen dem Schutz des Netzes und den Vorteilen, die ein freier Zugang bietet, stattfinden. Aufgrund der schnellen Entwicklungen



und entsprechender neuer Bedrohungen der Netze müssen die Sicherheitsmaßnahmen kontinuierlich unabhängig überprüft und weiterentwickelt werden.

Solange sich die Nutzer und Anbieter der Anfälligkeit ihrer Netze nicht voll und ganz bewußt werden, werden potentielle Lösungen unerforscht bleiben. Die obenstehende Abbildung gibt einen Überblick über den derzeitigen Einsatz von Sicherheitsprodukten in der Europäischen Union (die statistischen Zahlen stammen aus einer im Februar 2001 für das ‚Benchmarking' im Rahmen von *eEurope 2002* durchgeführten Erhebung).

2.2.3. Störung von Netzen

Netze sind weitestgehend digitalisiert und werden von Computern überwacht. In der Vergangenheit war die häufigste Ursache für eine Netzstörung ein Ausfall in dem Computersystem, das das Netz steuert, und Angriffe auf Netze waren sind im wesentlichen auf diese Computer gerichtet. Heutzutage nutzen die zerstörerischten Angriffe die Verwundbarkeit von Netzkomponenten (Betriebssysteme, Routingsysteme) aus.

Während Angriffe auf das Telefonsystem in der Vergangenheit kein besonders großes Problem darstellten, sind Angriffe auf das Internet recht verbreitet. Das liegt daran, daß beim Telefon die Steuersignale vom Kommunikationsverkehr getrennt verlaufen und geschützt werden können, während wichtige Knoten im Internet von jedermann erreicht werden können. Doch dürfte das Telefonnetz in Zukunft auch anfälliger werden, da es

Schlüsselelemente des Internets aufnehmen wird und seine Steuerebene für Dritte geöffnet wird.

Die Angriffe können verschiedene Formen annehmen:

- **Angriffe auf die Namenserver:** Das Internet stützt sich auf das System der Bereichsnamen (DNS), durch das benutzerfreundliche Namen (z. B. www.europa.eu.int) in abstrakte Netzadressen (z.B. IP-Nr. 147.67.36.16) übersetzt werden und umgekehrt. Wenn ein Teil des DNS ausfällt, können einige Web-Adressen nicht mehr lokalisiert werden und die E-Mail-Systeme können nicht mehr arbeiten. Die Störung von DNS-Root-Servern oder anderen wichtigen DNS-Servern könnte zu einem Netzzusammenbruch führen. Zu Beginn diesen Jahres wurde entdeckt, daß die Software, mit der die meisten Namenserver arbeiten, einige Schwächen aufweist. [7]

- **Angriffe auf die Router**: Das Routing im Internet erfolgt stark dezentralisiert. Jeder Router informiert in regelmäßigen Abständen seine benachbarten Router über die Netze, die er kennt und darüber, wie diese zu erreichen sind. Die Schwäche dieses Systems liegt darin, daß diese Information nicht überprüft werden kann, weil anlagebedingt jeder Router nur minimale Kenntnisse über die Netztopologie besitzt. Daher kann jeder Router sich selbst als besten Pfad zu jedem Bestimmungsort präsentieren und als Mittel dienen, den Datenverkehr zu diesem Bestimmungsort abzufangen, zu blockieren oder zu verändern.

- **‚Flooding' und ‚Denial of Service'**: Bei dieser Art von Angriffen werden Netze durch die Überschwemmung mit künstlichen Nachrichten gestört, die einen berechtigten Zugang unmöglich machen oder stark begrenzen. Das ist ähnlich, wie wenn Faxgeräte durch lange, wiederholte Nachrichten blockiert werden. Mit Flooding-Angriffen wird versucht, Web-Server oder die Umschlagskapazität der Anbieter von Internetdiensten (ISP) durch automatisch erzeugte Nachrichten zu überlasten.

Möglicher Schaden: Durch Störungen leidet das Ansehen renommierter Web-Adressen. Im Rahmen einiger Studien wurde berechnet, daß durch einen Angriff in jüngster Zeit zusätzlich zur unschätzbaren Beschädigung der Reputation mehrere hundert Millionen EURO Schaden entstanden sind. Die Unternehmen hängen bei ihrer Geschäftsabwicklung in immer stärkerem Maße von der Verfügbarkeit ihrer Webseiten ab, wobei Unternehmen, die das Internet für unmittelbare Lieferungen benötigen, besonders anfällig sind.

Mögliche Lösungen: Angriffen auf DNS-Server kann im Prinzip einfach dadurch begegnet werden, daß die DNS-Protokolle erweitert werden, beispielsweise durch die Verwendung sicherer DNS-Erweiterungen auf der Grundlage von öffentlichen Schlüsseln. Das bedeutet allerdings, daß auf den Client-Maschinen neue Software installiert werden muß, was bisher nur in geringem Umfang geschehen ist. Außerdem müßte der Verwaltungsprozeß, durch den das Vertrauen zwischen den DNS-Bereichen verbessert werden soll, effizienter werden.

Sich gegen Angriffe auf das Routing-System zu schützen, ist viel schwieriger. Das Internet wurde so gestaltet, daß beim Routing eine maximale Flexibilität gegeben ist. Dadurch wurde die Wahrscheinlichkeit reduziert, daß Dienste verloren gehen, wenn ein Teil der Netzinfrastruktur zusammenbricht. Es gibt kein effektives Mittel zur Sicherung der Routing-Protokolle, vor allem bei Backbone-Routern.

---

[7] Quelle: CERT/CC auf der Seite http://www.cert.org/advisories/CA-2001-02.html

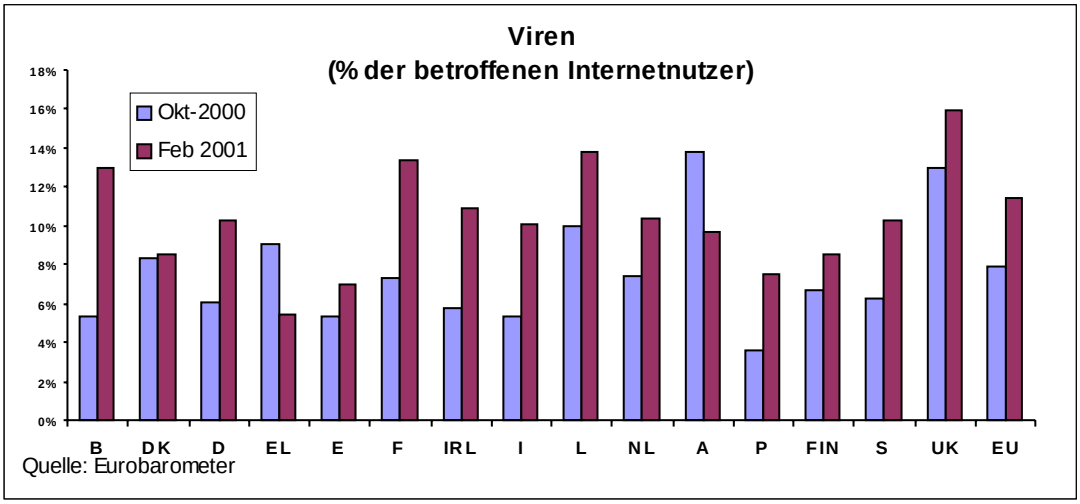
Das Volumen der übermittelten Daten erlaubt kein detailliertes Filtern. Eine eingehende Überprüfung würde die Netze zum Erliegen bringen. Aus diesem Grund führen die Netze nur einfache Filter- und Zugangskontrollfunktionen aus. Spezifischere Sicherheitsfunktionen (z.B. Authentifizierung, Prüfung auf Integrität, Verschlüsselung) sind am Rande der Netze angesiedelt, d.h. bei den Endgeräten und den Netzservern, die als Endpunkte fungieren.

2.2.4. Bösartige Software, die Daten verändert oder zerstört

Computer funktionieren nur mit Software. Unglücklicherweise kann Software auch dazu benutzt werden, einen Computer lahm zu legen oder Daten zu löschen oder zu verändern. Wie die obigen Beschreibungen zeigen, kann ein schlecht funktionierender Computer, der Teil des Netzmanagements ist, weitreichende Auswirkungen haben. Ein Virus ist eine Form bösartiger Software, die ihren eigenen Code reproduziert, indem es sich an andere Programme in einer Weise anheftet, daß immer, wenn das infizierte Programm ausgeführt wird, der Code des Virus ausgeführt wird.

Es gibt verschiedene andere Arten von bösartiger Software: manche schädigen nur den Computer, auf den sie kopiert wurden, andere verbreiten sich auf weitere vernetzte Computer. Beispielsweise gibt es auch Programme (dramatisch „logische Bomben“ genannt), die solange „schlafen“, bis sie durch ein Ereignis wie etwa ein bestimmtes Datum ausgelöst werden (Freitag, der 13., wird oft verwendet). Andere Programme scheinen gutartig zu sein, lösen aber, wenn sie ausgeführt werden, bösartige Angriffe aus (sie werden daher „Trojanische Pferde“ genannt). Wieder andere („Würmer“ genannt) infizieren keine anderen Programme, wie das die Viren tun, sondern kopieren sich selbst. Die Kopien kopieren sich immer weiter und überschwemmen unter Umständen das System.

Möglicher Schaden: Viren können sehr zerstörerisch sein, wie die hohen Kosten gezeigt haben, die durch einige der jüngsten Angriffe verursacht wurden (z.B. „I Love you“, „Melissa“ und „Kurnikova“). Die folgende Abbildung gibt einen Überblick (nach Mitgliedstaaten) über die Zunahme der Viren, die Internet-Nutzer in der EU zwischen Oktober 2000 und Februar 2001 registriert haben. Durchschnittlich hatten etwa 11 % der



europäischen Internet-Nutzer bereits einmal einen Virus auf ihrem PC zu Hause.

Mögliche Lösungen: In erster Linie wird zum Schutz Anti-Viren-Software eingesetzt, die in vielfältigen Formen verfügbar ist. Beispielsweise identifizieren Virenscanner und „Desinfektionsprogramme“ bekannte Viren und entfernen sie. Ihre wesentliche Schwäche

liegt darin, daß sie Schwierigkeiten mit neue Viren haben, selbst dann, wenn sie regelmäßig auf den neuesten Stand gebracht werden. Eine andere Möglichkeit ist ein Integritätsprüfer. Wenn ein Virus einen Computer infizieren will, muß er etwas in dessen System verändern. Bei einer Integritätsprüfung könnten solche Veränderungen aufgespürt werden, auch wenn sie von bis dato noch unbekannten Viren verursacht werden.

Trotz recht fortschrittlicher Schutz-Produkte haben die Probleme mit bösartiger Software zugenommen. Dafür gibt es im wesentlichen zwei Gründe. Zum einen ermöglicht die Offenheit des Internets es den Angreifern, voneinander zu lernen und Methoden zu entwickeln, mit denen sie die Schutzmechanismen umgehen können. Zum anderen wächst das Internet ständig und erreicht immer mehr Nutzer, von denen sich viele der Notwendigkeit, Schutzmaßnahmen zu ergreifen, nicht bewußt sind. Die Sicherheit wird davon abhängen, wie weitgehend Virenschutz-Software eingesetzt wird.

2.2.5. Täuschung/Irreführung des Benutzers („malicious misrepresentation“)

Wenn eine Netzverbindung hergestellt wird oder Daten empfangen werden, stellt der Nutzer auf der Grundlage des Kommunikationskontexts Annahmen über die Identität seines Kommunikationspartners an. Das Netz bietet dafür einige Hinweise. Die größte Gefahr geht von Angreifern aus, die den Kontext kennen, also von Insidern. Wenn ein Nutzer eine Telefonnummer wählt oder eine Internetadresse in seinen Computer eingibt, sollte diese das gewünschte Ziel erreichen. Das reicht für viele Anwendungen aus, nicht aber für wichtige geschäftliche Transaktionen, medizinische, finanzielle oder offizielle Transaktionen, die einen höheren Grad an Authentifizierung, Integrität und Vertraulichkeit erfordern.

Möglicher Schaden: Eine Täuschung von Personen oder Körperschaften kann in vielerlei Hinsicht Schaden verursachen. Kunden können bösartige Software von einer Webseite herunterladen, die als verläßliche Quelle maskiert ist. So können vertrauliche Informationen an die falsche Person herausgegeben werden. Es besteht auch die Möglichkeit von Täuschungen, die zur Nichtanerkennung von Verträgen oder ähnlichem führen. Der größte Schaden besteht aber möglicherweise darin, daß eine fehlende Authentifizierung potentielle neue Geschäftskunden zurückhält. Viele Studien haben darauf hingewiesen, daß Sicherheitsbedenken einen Hauptgrund dafür darstellen, daß Geschäfte nicht über das Internet abgewickelt werden. Wenn man sicher sein könnte, daß der Gesprächspartner im Internet auch derjenige ist, als der er sich vorstellt, würde das Vertrauen in Internet-Transaktionen zunehmen.

Mögliche Lösungen: Die Einführung einer Authentifizierung im Netz im Zusammenhang mit der Einführung von SSL ist bereits hilfreich, ein vorgegebenes Maß an Vertraulichkeit zu garantieren. Virtuelle Private Netze (VPN) nutzen SSL und IPsec, um ein gegebenes Sicherheitsniveau einzuhalten, auch wenn Mitteilungen durch unsichere Internet- und offene Kanäle laufen.

Der Nutzen dieser Lösungen ist jedoch begrenzt, da sie auf digitalen Zertifikaten beruhen und keine Garantie dafür besteht, daß diese Zertifikate nicht gefälscht wurden. Eine dritte Partei, die oft als „Zertifizierungsbehörde“ oder in der Richtlinie über elektronische Signaturen[8] als „Zertifizierungsdiensteanbieter bezeichnet wird, kann diese Garantie erbringen. Einer weiten

[8] Richtlinie 1999/93/EG vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. Nr. L 13 vom 19.1.2000, S. 12).

Verbreitung dieser Lösung steht ähnlich wie bei der Verschlüsselung das Problem der Kompatibilität und Schlüsselverwaltung entgegen. In einem VPN ist das kein Problem, da hier herstellereigene Standardlösungen entwickelt werden können. Bei öffentlichen Netzen ist es dagegen ein großes Hindernis.

Die Richtlinie über elektronische Signaturen verbessert die Rechtsgrundlage für die Sicherung einer einfacheren elektronische Authentifizierung in der EU. Sie bietet einen Rahmen, innerhalb dessen sich der Markt frei entwickeln kann, aber auch Anreize zur Entwicklung sicherer Signaturen, die rechtlich anerkannt werden können. Die Umsetzung der Richtlinie in einzelstaatliches Recht ist derzeit im Gange.

2.2.6. Risiken unabsichtlicher Handlungen und Umweltereignisse

Viele Sicherheitszwischenfälle gehen von unvorhergesehenen und unabsichtlichen Ereignissen aus, vor allem ausgelöst durch

- Naturkatastrophen (z. B. Stürme, Überschwemmungen, Brände, Erdbeben)
- Dritte ohne vertragliche Beziehungen mit dem Betreiber oder dem Nutzer (z.B. Dienstunterbrechung wegen Bauarbeiten)
- Dritte mit einer vertraglichen Beziehung zum Betreiber oder zum Nutzer (z.B. Geräte- oder Softwareausfall in gelieferten Komponenten oder Programmen)
- Menschliches Versagen oder schlechtes Management des Betreibers (einschließlich des Diensteanbieters) oder des Nutzers (z.B. Probleme in der Netzsteuerung, falsche Installierung von Software).

Möglicher Schaden: Umweltereignisse verursachen typischerweise Netzausfälle. Unglücklicherweise werden gerade während solcher Ereignisse funktionierende Telekommunikationsleitungen am dringendsten benötigt. Hardwareausfälle und schlechte Software schaffen Anfälligkeiten, die entweder durch Angreifer ausgenutzt werden oder von alleine zu Störungen führen. Schlechtes Management der Netzkapazität kann zu Verstopfung führen, die Kommunikationskanäle verlangsamt oder unterbricht.

In diesem Zusammenhang ist die Regelung der Haftung äußerst wichtig. In den meisten Fällen werden Nutzer keinerlei Verantwortung haben, aber sie können sich in einer Situation wiederfinden, in der sie keine oder nicht genügend Haftungsansprüche geltend machen können.

Mögliche Lösung: Die Betreiber von Telekommunikationsnetzen kennen solche Auswirkungen nur zu gut und haben Redundanzen und Infrastrukturschutz in ihre Netze eingebaut. Der zunehmende Wettbewerb auf dem Telekommunikationsmarkt könnte hier eine doppelschneidige Klinge sein. Auf der einen Seite könnten Preiserwägungen Betreiber veranlassen, Redundanzen abzubauen, auf der anderen Seite kann die Existenz von mehr Betreibern in einem Markt als Ergebnis der Liberalisierung Nutzer zum Wechsel zu einem anderen Betreiber veranlassen, wenn ein Netzausfall vorkommt (wie ein Fluggast auf eine andere Linie umgebucht wird, wenn ein Flug ausfällt). Gemeinschaftsrecht verlangt jedoch, daß Mitgliedstaaten alle erforderlichen Schritte unternehmen, um die Vefügbarkeit von öffentlichen Netzen im Falle von katastrophalen Netzausfällen oder Naturkatastrophen zu

sichern (siehe Zusammenschaltungsrichtlinie 97/33/EG[9] und die Richtlinie über Sprachtelefonie[10]). Insgesamt ist aufgrund der zunehmenden Anzahl verbundener Netze zu wenig über das generelle Sicherheitsniveau bekannt.

Der Wettbewerb zwischen Geräte- und Softwareproduzenten sollte dazu führen, daß sie die Sicherheit ihrer Produkte verbessern. Jedoch ist Wettbewerb nicht immer stark genug, um Sicherheitsinvestitionen zu begründen, zumal Sicherheit nicht immer eine große Rolle beim Kauf spielt. Sicherheitslücken werden häufig zu spät entdeckt, wenn der Schaden bereits erfolgt ist. Die Erhaltung fairen Wettbewerbs in den Märkten für Informationstechnologie wird bessere Sicherheitsbedingungen schaffen.

Das Risiko menschlichen Versagens und von Bedienungsfehlern kann durch verbesserte Ausbildung und erhöhtes Gefahrenbewußtsein verringert werden. Die Schaffung angemessener Sicherheitsregeln in den Unternehmen könnte diese Risiken reduzieren.

2.3 Neue Herausforderungen

Die Netz- und Informationssicherheit wird sich voraussichtlich zu einem Schlüsselfaktor für die Entwicklung der Informationsgesellschaft entwickeln, zumal Vernetzung einer immer größere Rolle im wirtschaftlichen und sozialen Leben spielt. Dabei sind zwei Themen zu betrachten: der potentielle Schaden wird immer größer und neue Technologien treten auf den Plan.

i. Netze und Informationssysteme transportieren mehr und mehr empfindliche Daten und wirtschaftlich wichtige Informationen, was die Anreize für Angriffe erhöht. Solche Angriffe können für die Allgemeinheit gering und relativ folgenlos sein – beispielsweise wenn eine private Webseite nicht mehr gelesen werden kann oder wegen eines Virus eine Festplatte neu formatiert werden muß. Solche Störungen können jedoch auch sehr viel kritischere Ausmaße annehmen, die bis zur Beeinträchtigung sehr empfindlicher Kommunikationen, größeren Stromausfällen oder deutlichen wirtschaftlichen Einbußen durch die gezielte Überlastung von Servern (Denial of service-Angriffe) oder Datenschutzverstöße reichen.

   Das genaue Ausmaß der tatsächlichen und potentiellen Schäden durch Einbrüche in die Netzsicherheit ist schwer zu messen. Es existiert kein systematisches Berichterstattungssystem, und viele Unternehmen geben Angriffe aus Angst vor Imageverlusten lieber nicht öffentlich zu. So sind die vorliegenden Informationen vorwiegend anekdotischer Art. Es entstehen nicht nur direkte Kosten (Einkommenseinbußen, Verlust wertvoller Informationen, Personalkosten für die Wiederherstellung des Netzes), sondern solche Angriffe verursachen auch umfangreiche immaterielle Kosten – insbesondere Imageverluste, die schwer abzuschätzen sind.

ii. **Die Netz- und Informationssicherheit ist ein dynamisches Problem.** Die Geschwindigkeit des technologischen Wandels bringt ständig neue Herausforderungen; die Probleme von gestern existieren nicht mehr und die Lösungen von heute sind morgen wertlos. Der Markt bietet fast täglich neue Anwendungen, Dienstleistungen und Produkte. Einige Entwicklungen werden jedoch mit Sicherheit die private und öffentliche Sicherheitspolitik vor erhebliche Herausforderungen stellen:

---

[9] ABl. L 99 vom 26.07.1997.
[10] ABl. L 101 vom 01.04.1998.

- Verschiedene digitale Objekte wie etwa Mulitmediaobjekte, herunterladbare Software oder mobile Agenten werden mit eingebauten Sicherheitsmerkmalen über die Netze übertragen werden. Der Begriff der Verfügbarkeit, der heute als die Fähigkeit, das Netz zu benutzen, verstanden wird, wird sich in Richtung der autorisierten Benutzung entwickeln, z.B. dem Recht ein Videospiel für eine bestimmte Zeit zu spielen oder eine einzelne Kopie einer Software zu erstellen.

- In Zukunft werden Betreiber von IP-Netzen die Sicherheit erhöhen wollen, in dem sie die Übertragungen ständig überwachen, um nur erlaubte Mitteilungen durchgehen zu lassen. Solche Maßnahmen sollten jedoch mit den Datenschutzregeln in Einklang stehen.

- Die Benutzer werden dazu übergehen, ihre Internet-Verbindung ständig aufrecht zu erhalten, wodurch sich Angreifern noch mehr Möglichkeiten bieten und ungeschützte Terminals angreifbar werden, da Angreifer noch leichter der Entdeckung entgehen können.

- In den Haushalten werden Netze, an die verschiedene Geräte angeschlossen sind, weite Verbreitung finden; damit werden sich neue Angriffsmöglichkeiten eröffnen, durch die die Benutzer stärker gefährdet werden (z.B. durch die Möglichkeit, Alarmanlagen ferngesteuert auszuschalten).

- Die großflächige Einführung drahtloser Netze (z.B. drahtloser Multimediazugang, drahtlose lokalen Netze, die dritte Generation des Mobilfunks) wird die effektive Verschlüsselung von über Funksignale übermittelten Daten erforderlich machen. Es wird daher zunehmend problematisch, per Gesetz eine schwache Verschlüsselung solcher Signale vorzuschreiben.

- Netze und Informationssysteme wird es überall geben; sie werden stationäre und drahtlose Geräte verbinden und eine „intelligente Umgebung" (*ambient intelligence*) bieten, d.h. selbstorganisierende Funktionen, die automatisch gestartet werden und vom Benutzer früher getroffene Entscheidungen reproduzieren. Die Herausforderung wird darin liegen, eine inakzeptable Verwundbarkeit zu verhindern und Sicherheit in die Architektur zu integrieren.

3. Ein europäischer Politikansatz

3.1. Grundlage einer politischen Strategie

Der Schutz von Kommunikationsnetzen gilt bei den politischen Entscheidungsträgern zunehmend als vorrangige Aufgabe, was vor allem mit nationaler Sicherheit, Datenschutz und dem Wunsch nach Förderung des elektronischen Geschäftsverkehrs zusammenhängt. Dies hat zu einer ansehnlichen Reihe von gesetzlichen Bestimmungen in der Richtlinie über Datenschutz und im Regulierungsrahmen für Telekommunikation geführt (wie in Abschnitt 3.6 ausgeführt). Dies Maßnahmen müssen jedoch in einer sich schnell verändernden Umgebung mit neuen Technologien, Wettbewerbsmärkte, Netzkonvergenz und Globalisierung angewandt werden. Diese Herausforderungen werden noch schwieriger gemacht dadurch daß der Markt aus den im folgenden analysierten Gründen eher zu wenig in Sicherheit investiert.

Netz- und Informationssicherheit ist eine Ware, die auf dem Markt gehandelt wird und Gegenstand vertraglicher Vereinbarungen zwischen verschiedenen Parteien ist. Der Markt für

Sicherheitsprodukte ist in den letzten Jahren erheblich expandiert. Einigen Studien zufolge hatte der Markt für Internet- Sicherheitssoftware Ende 1999 weltweit ein Volumen von etwa 4,4 Mrd. $ erreicht und wird pro Jahr 23% wachsen bis auf 8,3 Mrd $ im Jahr 2004[11]. In Europa wird der Sicherheitsmarkt für elektronische Kommunikationsmedien den Prognosen zufolge von 465 Mio. $ im Jahr 2000 auf 5,3 Mrd. $ im Jahr 2006[12] wachsen, der Sicherheitsmarkt für die Informationstechnologie wird voraussichtlich ein Wachstum von 490 Mio. $ im Jahr 1999 auf 2,74 Mrd. im Jahr 2006 verzeichnen[13].

Dabei geht man in der Regel davon aus, daß es durch den Preismechanismus zu einem Ausgleich zwischen Sicherheitskosten und dem spezifischen Sicherheitsbedarf kommen wird. Manche Benutzer werden einen höheres Sicherheitsniveau fordern, während andere sich mit einem geringeren Sicherheitsstandard begnügen werden. Der Staat wird allerdings möglicherweise für ein Mindestniveau an Sicherheit sorgen. Die Ansprüche der Kunden werden sich in diesem Fall im Preis widerspiegeln, die sie für Sicherheitsvorkehrungen zu zahlen bereit sind. Wie die Analyse in Abschnitt 2 zeigt, gibt es jedoch für viele Sicherheitsrisiken nach wie vor keine Lösungen oder aber diese werden aufgrund bestimmter Schwächen des Marktes erst langsam verfügbar.

(i). **Soziale Kosten und Nutzen:** Investitionen in eine Verbesserung der Netzsicherheit sind mit sozialen Kosten und Nutzen verbunden, die sich in den Marktpreisen nicht angemessen widerspiegeln. **Auf der Kostenseite** sind die Marktteilnehmer nicht für alle Folgen ihres Sicherheitsverhaltens verantwortlich. Benutzer mit niedrigem Sicherheitsniveau haften nicht für Schäden Dritter. Die Situation ist vergleichbar mit der eines unachtsamen Autofahrers, der für die Kosten des Verkehrsstaus, der durch seinen Unfall verursacht wird, nicht zur Verantwortung gezogen wird. In ähnlicher Weise sind im Internet die Folgen verschiedener Angriffe durch die schlecht geschützten Rechner relativ unbedachter Nutzer eskaliert. Der **Nutzen** der Sicherheit spiegelt sich ebenfalls nicht in vollem Umfang in den Marktpreisen wider. Wenn Betreiber, Lieferanten oder Dienstanbieter die Sicherheit ihrer Produkte verbessern, kommt ein erheblicher Teil des Nutzens aus dieser Investition nicht nur ihren Kunden, sondern all denjenigen zugute, die direkt oder indirekt mit elektronischer Kommunikation zu tun haben – letztendlich der gesamten Wirtschaft.

(ii). **Asymmetrie der Information:** Die Netze werden immer komplexer und erreichen einen größeren Markt, der viele Benutzer umfaßt, die über die Technologie oder ihre potentiellen Gefahren nur wenig wissen. Diese Benutzer sind sich nicht aller Sicherheitsrisiken bewußt, und für viele Betreiber, Händler oder Dienstanbieter ist es schwierig abzuschätzen, ob und wo Verwundbarkeiten existieren. Viele neue Dienste, Anwendungen und Softwareprodukte bieten attraktive Funktionen, doch gerade die sind oft eine Quelle neuer Risiken. (So ist beispielsweise der Erfolg des World Wide Web zum Teil auf das breite Spektrum leicht herunterladbarer multimedialer Anwendungen zurückzuführen, doch diese „Plug-ins“ bieten auch Möglichkeiten für das Eindringen von Angriffen). Während der Nutzen offensichtlich ist, sind die Risiken es nicht, und für die Anbieter bestehen mehr Anreize zur Bereitstellung neuer Funktionen als zur Erhöhung der Sicherheit.

---

11 IDC: Internet security market forecast and analysis, 2000-2004 Report #W23056 - Oktober 2000.

12 Frost&Sullivan: The European Internet communication security markets, report 3717 - November 2000.

13 Frost&Sullivan: The European Internet communication security markets, report 3847 - Juli 2000.

iii) **Das Problem kollektiven Handelns:** Die Betreiber übernehmen zunehmend den Internetstandard oder schließen ihre Netze in irgendeiner Form ans Internet an. Das Internet wurde jedoch nicht mit Blick auf die Sicherheit konzipiert, sondern im Gegenteil mit dem Ziel entwickelt, den Zugang zu Informationen zu ermöglichen und ihren Austausch zu erleichtern. Darauf beruht sein Erfolg. Das Internet ist zum globalen Netz der Netze geworden mit nie dagewesenen Reichtum an Inhalten und Varietät. Investitionen in die Sicherheit zahlen sich oft nur dann aus, wenn genügend Marktteilnehmer an einem Strang ziehen. Deshalb ist für die Entwicklung von Sicherheitslösungen **Zusammenarbeit** erforderlich. Zusammenarbeit funktioniert jedoch nur dann, wenn eine kritische Masse von Akteuren sich daran beteiligt, was schwer zu erreichen ist, da zum einen „Freibeuter-Gewinne" möglich sind. Interoperabilität von Produkten und Diensten wird für Wettbewerb zwischen Sicherheitslösungen sorgen. Es fallen jedocherhebliche Koordinierungskosten an, da globale Lösungen benötigt werden dürften und doch manche Akteure versucht sind, proprietäre Lösungen auf den Markt zu bringen. Da eine Vielzahl von Produkten und Diensten noch stets **proprietäre Lösungen** nutzen, bringt die Verwendung sicherer Standards, die nur dann zusätzliche Sicherheit bringen, wenn auch alle anderen sie anbieten, keinen Vorteil.

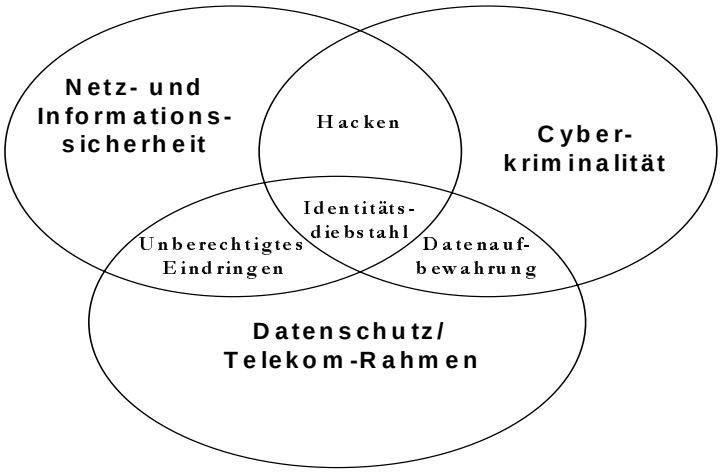
Als ein Ergebnis dieser Unzulänglichkeiten sieht der Telekommunikations- und Datenschutzrahmen bereits rechtliche Verpflichtungen für Betreiber und Diensteanbieter vor, um ein gewisses Sicherheitsniveau in Kommunikations- und Informationssystemen zu gewährleisten.

Die Begründung für eine europäische Politik der Netz- und Informationssicherheit kann wie folgt zusammengefaßt werden. Ersten müssen die gesetzlichen Bestimmungen der EU effektiv angewandt werden, wozu ein **gemeinsames Verständnis der Sicherheitsprobleme und der zu ergreifenden Maßnahmen** erforderlich ist. Der gesetzliche Rahmen muß sich außerdem weiterentwickeln, wie man am bereits vorgeschlagenen neuen Regulierungsrahmen für elektronische Kommunikationen oder den Vorschlägen im Zusammenhang mit der Diskussion über die Cyber-Kriminalität sehen kann. Zweitens führen einige Marktschwächen dazu, daß die Marktkräfte nicht alleine für genügend Investitionen in Sicherheitstechnik oder Sicherheitspraxis führen werden**. Politische Maßnahmen könne den Markt ergänzen und gleichzeitig das Funktionieren des gesetzlichen Rahmens verbessern**. Schließlich werden Kommunikations- und Informationsdienste über Grenzen hinweg angeboten. Deshalb ist ein europäischer Ansatz erforderlich, **um den Binnenmarkt für solche Dienste zu sichern, um von gemeinsamen Lösungen zu profitieren, und um effektiv auf globaler Ebene handeln zu können.**

Die vorgeschlagenen politischen Maßnahmen in bezug auf Netz- und Informationssicherheit müssen nicht nur im Zusammenhang der bestehenden Telekommunikations- und Datenschutzgesetzgebung gesehen werden, sondern auch im Zusammenhang mit den jüngsten Initiativen zur Bekämpfung der Cyber-Kriminalität. Die Kommission hat vor kurzem eine Mitteilung zur Computerkriminalität veröffentlicht[14], die untere anderem die Schaffung eines EU Forums über Cyber-Kriminalität vor, um das gegenseitige Verständnis und die Zusammenarbeit aller Beteiligten in der EU zu verbessern. Eine Politik auf dem Gebiet der Netz- und Informationssicherheit wird die Lücke in diesem politischen Rahmen schließen.

[14] Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, KOM (2000) 890, http://europa.eu.int/ISPO/eif/internetPoliciesSite/Crime/crime1.html

Die folgende Grafik zeigt die drei Politikansätze und ihre Wechselbeziehungen anhand einiger Beispiele:



3.2. Sensibilisierung

Zu viele (private/öffentliche) Nutzer sind sich der möglichen Risiken im Zusammenhang mit der Nutzung von Kommunikationsnetzen oder der bereits verfügbaren Lösungsmöglichkeiten nicht bewußt. Sicherheitsprobleme sind komplex, und die Risiken sind oft auch für Fachleute schwer abzuschätzen. Das Informationsdefizit ist eine der Schwächen des Marktes, die die Sicherheitspolitik angehen sollte. Es besteht die Gefahr, daß einige Nutzer von den vielen Berichten über Sicherheitsrisiken so abgeschreckt werden, daß sie den elektronischen Geschäftsverkehr ganz meiden. Andere, die entweder schlecht informiert sind oder das Risiko unterschätzen, werden wiederum zu unvorsichtig sein. Manche Unternehmen haben ein Interesse daran, potentielle Gefahren herunterzuspielen, da sie den Verlust von Kunden befürchten.

Paradoxerweise steht im Internet eine enorme Menge an Informationen über Netz- und Informationssicherheit zur Verfügung, und die Computerzeitschriften behandeln dieses Thema recht ausführlich. Das Problem besteht für die Nutzer darin, Informationen zu finden, die verständlich und aktuell sind und ihren speziellen Bedürfnissen gerecht werden. Die Autoindustrie bietet ein gutes Beispiel dafür, wie sich aus komplexen Sicherheitsspezifikationen ein wesentliches Marketingelement machen lässt. Zudem sind die Anbieter von öffentlichen Telekommunikationsdienstleistungen nach den EU-Rechtsvorschriften verpflichtet, die Teilnehmer über besondere Sicherheitsisiken auf ihrem Netz und mögliche Abhilfen einschließlich deren Kosten zu informieren (vgl. Art. 4 der Richtlinie 97/66/EG).

Ziel einer Sensibilisierungskampagne für Bürger, Verwaltungen und Unternehmen ist deshalb die Bereitstellung zugänglicher, unabhängiger und zuverlässiger Informationen über die Netz- und Informationssicherheit. Eine offene Diskussion über Sicherheit ist erforderlich. Ist das entsprechende Bewußtsein gewährleistet, können die Nutzer selbst entscheiden, welches Schutzniveau ihren Bedürfnissen entspricht.

Vorgeschlagene Aktionen:

- Die Mitgliedstaaten sollten eine öffentliche Informations- und Bildungskampagne starten und laufende Maßnahmen qualitativ aufwerten. In diesem Zusammenhang sollten eine

Kampagne in den Massenmedien sowie gezielte Aktionen für alle betroffenen Akteure stattfinden. Eine gut konzipierte und wirkungsvolle Informationskampagne ist nicht billig. Die Erarbeitung von Inhalten, in denen Risiken beschrieben werden, ohne den Menschen unnötig Angst zu machen und ohne potentielle Hacker anzuregen, erfordert eine sorgfältige Planung.

Die Europäische Kommission wird den Austausch vorbildlicher Praktiken erleichtern und auf EU-Ebene einen gewissen Grad an Koordinierung zwischen den verschiedenen nationalen Informationskampagnen gewährleisten, insbesondere, was die Substanz der anzubietenden Informationen angeht. Angelpunkt dieser Aktion wäre ein Web-Portal sowohl auf nationaler als auch auf europäischer Ebene. Eine Verknüpfung dieser Portale mit vertrauenswürdigen Web-Adressen internationaler Partner könnte ebenfalls in Erwägung gezogen werden.

- Die Mitgliedstaaten sollten den Einsatz beispielhafter Vorgehensweisen auf dem Gebiet der Sicherheit auf der Grundlage bestehender Maßnahmen wie etwa ISO/IEC DIS 17799 (Verhaltenskodex für das Management von Informationssicherheit, www.iso.ch) fördern. Kleine und mittlere Unternehmen sollten dabei gezielt angesprochen werden. Die Kommission wird die Mitgliedstaaten in ihren Bemühungen unterstützen.

- Das Bildungswesen in den Mitgliedstaaten sollte einen größeren Schwerpunkt auf Kurse legen, die sich vorwiegend mit Sicherheitsfragen beschäftigen. Die Entwicklung von Bildungsmaßnahmen auf allen Ebenen zu Themen wie beispielsweise den Sicherheitsrisiken offener Netze und wirksame Lösungen sollten mehr im Informatikunterricht an den Schulen vermittelt werden.

  Die Lehrkräfte müssen ihrerseits in ihrer eigenen Ausbildung mit Sicherheitsfragen vertraut gemacht werden. Die Europäische Kommission unterstützt die Entwicklung neuer Module für die einschlägigen Ausbildungspläne im Rahmen ihres Forschungsprogramms.

3.3. Ein europäisches Warn- und Informationssystem

Selbst wenn die Nutzer sich der Sicherheitsrisiken bewußt sind, müssen sie vor neuen Gefahren gewarnt werden. Es läßt sich kaum verhindern, daß böswillige Angreifer neue Schwachstellen finden, um selbst Schutzmaßnahmen auf dem neuesten Stand der Technik zu umgehen. Die Industrie entwickelt laufend neue Software-Anwendungen und Dienste und bietet verbesserte Dienstleistungen an, die das Internet attraktiver machen, doch dabei werden unbeabsichtigt auch neue Schwachstellen und Risiken geschaffen.

Selbst erfahrene Netztechniker und Sicherheitsfachleute sind vom innovativen Charakter mancher Angriffe überrascht. Deshalb sind ein Frühwarnsystem, mit dem alle Nutzer schnell gewarnt werden können, und die Möglichkeit einer schnellen und verlässlichen Beratung über den Umgang mit solchen Angriffen erforderlich. Außerdem brauchen Unternehmen ein vertrauliches Warnsystem, um Angriffe berichten zu können, ohne öffentliches Vertrauen zu verlieren. Ergänzend muß eine umfassendere zukunftsorientierte Sicherheitsanalyse stattfinden, in der Informationen zusammengetragen und die Risiken in einer weiter gefaßten Perspektive analysiert werden.

Viel Arbeit in diesem Bereich leisten öffentliche und private Computer-Notdienste (Computer Emergency Response Teams - CERT) und ähnliche Einrichtungen. So hat beispielsweise Belgien ein Virenwarnsystem eingerichtet, das es den belgischen Bürgern ermöglicht, innerhalb von zwei Stunden über Viren informiert zu werden. Die Arbeitsweise der

Computer-Notdienste ist jedoch in jedem Mitgliedstaat anders, wodurch die Zusammenarbeit kompliziert wird. Die bestehenden Computer-Notdienste sind nicht immer gut ausgerüstet, und ihre Aufgaben sind häufig nicht klar definiert. Die weltweite Koordination erfolgt durch das Koordinationszentrum CERT/CC, das teilweise von der US-Regierung finanziert wird, und die CERT in Europa sind von der Informationspolitik des CERT/CC und anderer Einrichtungen abhängig.

Aufgrund dieser komplizierten Struktur findet eine europäische Zusammenarbeit bisher nur in begrenztem Umfang statt. Die Zusammenarbeit ist entscheidend dafür, daß EU-weite Frühwarnungen durch den sofortigen Informationsaustausch über erste Anzeichen von Angriffen in einem Land gewährleistet werden können. Deshalb sollte die Zusammenarbeit mit den CERT-Systemen in der Europäische Union dringend verstärkt werden. Eine erste Aktion zur Verstärkung der Zusammenarbeit zwischen öffentlichen und privaten Stellen bezüglich der Verläßlichkeit von Informationsinfrastrukturen (einschließlich der Entwicklung von Frühwarnungssystemen) und zur Verbesserung der Zusammenarbeit zwischen CERT-Systemen ist bereits im Rahmen des eEurope-Aktionsplans erfolgt.

Vorgeschlagene Aktionen:

- Die Mitgliedstaaten sollten ihr CERT-System im Hinblick auf eine Verbesserung der Ausstattung und Kompetenz der bestehenden CERT überprüfen. Um die Anstrengungen auf einzelstaatlicher Ebene zu unterstützen, wird die Europäische Kommission einen konkreten Vorschlag zur Verbesserung der Zusammenarbeit in der europäischen Union ausarbeiten. Dieser wird einen Projektvorschlag innerhalb des TEN-Telekom-Programmes beinhalten, das eine effektive Vernetzung sowie die Konzipierung von Begleitmaßnahmen im IST-Programm zur Erleichterung des Informationsaustauschs vorsieht.
- Sobald das CERT-Netz auf europäischer Ebene eingerichtet ist, sollte es mit ähnlichen Einrichtungen in aller Welt, beispielsweise dem vorgeschlagenen G8-Ereignis-Meldesystem vernetzt werden.
- Die Kommission schlägt vor, mit den Mitgliedstaaten zu überprüfen, wie man auf europäischer Ebene am besten Daten sammeln und analysieren sowie zukunftsorientierte Gegenmaßnahmen für bestehende und neue Sicherheitsrisiken entwickeln kann. Die Organisationsform einer möglichen Struktur muß noch mit den Mitgliedstaaten diskutiert werden

3.4. Förderung des technischen Fortschritts

Die Investitionstätigkeit in Netz- und Informationssicherheitslösungen ist derzeit nicht optimal. Dies gilt sowohl für die Integration neuer Technologien als auch für die Erforschung neuer Lösungen. In einem Umfeld, in dem neue Technologien unweigerlich neue Risiken mit sich bringen, ist eine kontinuierliche Forschung unerlässlich.

Netz- und Informationssicherheit ist bereits Inhalt des Programms Technologien der Informationsgesellschaft (IST) im Rahmen des 5. Forschungsrahmenprogramms der EU (Mittelausstattung: 3.6 Mrd. € für vier Jahre), für das im Zeitraum 2001/2002 etwa 30 Mio. € für kooperative Forschungsarbeiten zu Sicherheitsfragen vorgesehen sind.

Die Forschung im Bereich der Verschlüsselung in Europa hat ein hohes Niveau. Der belgische Algorithmus „Rijndael“ hat die vom US-Standardisierungsinstitut NIST organisierte Ausschreibung für den Advanced Encryption Standard gewonnen. Das IST Projekt „NESSIE“ (New European Schemes for Signature, Integrity and Encryption) hat

einen erweiterten Wettbewerb für im Bereich von Multimediaanwendungen, mobilem Handel und intelligenten Chipkarten verwendbare Verschlüsselungsalgorithmen ausgeschrieben.

Vorgeschlagene Aktionen:

- Die Kommission schlägt vor, die Sicherheit in das geplante 6. Rahmenprogramm aufzunehmen, über das derzeit im Rat und im Parlament beraten wird. Um einen optimalen Einsatz dieser Mittel zu gewährleisten, sollten sie im Rahmen einer umfassenden Strategie zur Verbesserung der Netz- und Informationssicherheit gebunden werden. Gegenstand der von diesem Programm unterstützten Forschungsarbeiten sollten die wichtigsten Sicherheitsrisiken der „voll digitalisierten" Welt sein sowie die Aufgabe, die Rechte von Einzelnen und Gemeinschaften zu sichern. Im Mittelpunkt stehen grundlegende Sicherheitsmechanismen und deren Interoperabilität, dynamische Sicherheitsprozesse, moderne Verschlüsselungstechniken, Technologien zum Schutz der Privatsphäre, Technologien für den Umgang mit digitalen Vermögenswerten und Technologien zur zuverlässigen Unterstützung von Geschäfts- und Organisationsabläufen in dynamischen und mobilen Systemen.
- Die Mitgliedstaaten sollten aktiv die Nutzung von „einsteckbaren"[15] starken Verschlüsselungsprodukten fördern. Sicherheitslösungen auf der Grundlage einsteckbarer Verschlüsselung müssen als Alternative zu in Betriebssystemen eingebauten Lösungen erhältlich sein.

3.5. Förderung von marktorientierten Standardisierungs-, Bewertungs- und Zertifizierungsmaßnahmen

Wenn sicherheitsfördernde Lösungen wirksam sein sollen, müssen sie von den entsprechenden Marktteilnehmern gemeinsam umgesetzt werden und sollten am besten auf offenen internationalen Standards beruhen. Eines der größten Hindernisse für die Integration vieler Sicherheitslösungen, beispielsweise der elektronischen Signaturen, ist die mangelnde Interoperabilität verschiedener Umsetzungen. Wollen zwei Nutzer über verschiedene Umfelde hinweg sicher kommunizieren, müssen ihre Programme kompatibel sein.. Deshalb sollte die Verwendung standardisierter Protokolle und Schnittstellen, einschließlich der Anwendung von Konformitätstest sowie „Kompatibilitäts"-Veranstaltungen unterstützt werden. Offene Standards, am besten auf der Grundlage von Software mit frei zugänglichem Quellcode (Open Source Software) könnte zur schnelleren Fehlerkorrektur sowie zu größerer Transparenz beitragen.

Zudem kann eine Informationssicherheitsbewertung dazu beitragen, Vertrauen und Zuversicht der Benutzer zu stärken. Der Einsatz gemeinsamer Kriterien hat gegenseitige Anerkennung als Bewertungsmethode in vielen Ländern erleichtert[16], und diese Länder haben zudem eine mit den USA und Kanada eine Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten geschlossen.

Akkreditierte Zertifizierung von Geschäftsabläufen und Informationssicherheits-Managementsystemen wird durch den Leitfaden EA 7/03[17] der Organisation für die europäische Zusammenarbeit im Bereich der Akkreditierung (European co-operation for accreditation) unterstützt. Akkreditierung von Zertifizierungsstellen schafft Vertrauen in ihre

---

[15] Einsteckbar ('pluggable') bedeutet, dass eine Verschlüsselungssoftware einfach installiert wereden kann und parallel zu einem Betriebssystem funktioniert.

[16] Empfehlung des Rates 95/144/EG über gemeinsame Kriterien zur Bewertung von Informationssicherheitstechnologien (in der Mehrheit der Mitgliedstaaten umgesetzt).

[17] Europäische Zusammenarbeit über Akkreditierung zwischen Akkreditierungskörperschaften aus 25 EU, EFTA und Beitrittsländern.

Kompetenz und Unparteilichkeit, und erleichtert so die Akzeptanz ihrer Zertifikate im ganzen Binnenmarkt.

Zusätzlich zur Zertifizierung sollten auch Interoperabilitätstests durchgeführt werden. Ein Beispiel für diese Vorgehensweise ist die europäische Initiative zur Normung elektronischer Signaturen (EESSI), die Konsens-Lösungen zur Unterstützung der EU-Richtlinie über elektronische Signaturen entwickelt. Andere Beispiele sind die Initiative Intelligente Chipkarten in eEurope und die Initiative zur Umsetzung der Infrastrukturen für öffentliche Schlüssel (PKI) innerhalb des IDA-Programms zum Austausch von Daten zwischen Verwaltungen.

Es gibt keinen Mangel an Standardisierungsbemühungen, aber eine große Anzahl konkurrierender Standards und Spezifikationen führt zu einer Fragmentierung des Marktes und zu inkompatiblen Lösungen.

Darum brauchen die derzeitigen Standardisierungs- und Zertifizierungsmaßnahmen eine bessere Koordinierung, auch um mit der Einführung neuer Sicherheitslösungen besser Schritt zu können. Die Harmonisierung von Spezifizierungen wird zu erhöhter Kompatibilität führen und gleichzeitig schnelle Umsetzung durch die Marktteilnehmer ermöglichen.

Vorgeschlagene Aktionen:

- Europäische Normungsgremien sind aufgefordert, die Arbeit an der Interoperabilität von Sicherheitsprodukten und -diensten zu beschleunigen, nach einem festen und zügigen Zeitplan. Wo nötig sollten neue Verfahren und Testergebnisse benutzt werden, um die Arbeit zu beschleunigen und die Zusammenarbeit mit Verbraucherverbänden und das Engagement von Marktteilnehmern zu stärken.
- Die Kommission wird, insb. durch die IST- und IDA-Programme, den Einsatz elektronischer Signaturen, die Umsetzung nutzerfreundlicher PKI-Lösungen und die weitere Entwicklung von IPv6 und IPsec[18] (wie im eEurope 2002 Aktionsplan vorgesehen) fördern.
- Die Mitgliedstaaten werden aufgefordert, den Einsatz von Zertifikaten und Akkreditierungsverfahren nach allgemein akzeptierten europäischen und internationalen Standards, die gegenseitige Anerkennung erleichtern, zu fördern . Die Kommission wird die Notwendigkeit für eine rechtliche Initiative zur gegenseitigen Anerkennung von Zertifikaten bis Ende 2001 prüfen.
- Die europäischen Marktteilnehmer werden dazu angeregt, sich aktiver an europäischen (CEN, CENELEC, ETSI) und internationalen (Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C)) Normungsaktivitäten zu beteiligen.
- Die Mitgliedstaaten sollten alle relevanten Sicherheitsstandards überprüfen. Auswahlverfahren für europäische Verschlüsselungs und Sicherheitslösungen könnten organisiert werden in Zusammenarbeit mit der Kommission, mit der Perspektive, international anerkannte Standards zu stimulieren..

3.6. Rechtlicher Rahmen

[18] IPv6 ist ein Internetprotokoll, das die Zahl möglicher IP-Adressen vergrößert, das traffic routing von Nachrichten optimiert und die Möglichkeiten zum Einsatz von IPSec verbessert. IPSec ist ein anderes Internetprotokoll, das Vertraulichkeit anstrebt, die Einsicht von Paketen ausser durch den empfangenden host verhindert und Authentifizierung und Integrität bietet, um sicherzustellen, dass die Daten im Paket authentisch und vom korrekten Absender sind.

In Bezug auf die Sicherheit von Kommunikationsnetzen und Informationssystemen existieren verschiedene Rechtstexte. Am umfassendsten sind die rechtlichen Rahmenbedingungen für den Telekommunikationssektor. Aufgrund der Konvergenz der Netze sind im Hinblick auf Sicherheitsfragen die Vorschriften und Regulierungstraditionen verschiedener Sektoren von Belang. Dazu gehören der **Telekommunikationssektor** (einschließlich aller Kommunikationsnetze), der gleichzeitig reguliert und dereguliert wird, die weitgehend unregulierte **Computerindustrie**[19], das **Internet**, das nach dem „hands-off approach" weitgehend der Selbstregulierung durch die Anbieter überlassen wird, und der **elektronische Geschäftsverkehr**, für den zunehmend spezifische Vorschriften erlassen werden. Außerdem sind im Hinblick auf die Sicherheit Bestimmungen über Haftpflicht, Computerkriminalität, elektronische Signaturen, Datenschutz und Exportregelungen von Belang.

Von diesen verschiedenen Vorschriften sind die Datenschutzrichtlinie für den Telekommunikationssektor, der rechtliche Rahmen für den Telekommunikationssektor, und im Zusammenhang mit der Mitteilung zur Computerkriminalität noch andere rechtssetzende Initiativen von besonderer Bedeutung.

Der Schutz der Privatsphäre ist eine wichtiges Ziel der Politik in der Europäischen Union. In Artikel 8 der Europäischen Menschenrechtskonvention[20] wird er als Grundrecht anerkannt. In Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union [21]wird auch das Recht auf Achtung des Familien- und Privatlebens, der Wohnung und der Kommunikation sowie der personenbezogenen Daten festgeschrieben.

Nach den Datenschutzrichtlinien[22] und insbesondere gemäß Artikel 5 der Datenschutzrichtlinie für den Telekommunikationssektor[23] sind die Mitgliedstaaten verpflichtet, durch innerstaatliche Vorschriften die Vertraulichkeit in öffentlichen Telekommunikationsnetzen und öffentlich zugänglichen Telekommunikationsdiensten sicherzustellen. Außerdem sind nach Artikel 4 derselben Richtlinie im Hinblick auf die praktische Umsetzung von Artikel 5 die Betreiber öffentlich zugänglicher Dienste und Netze verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit ihrer Netze zu gewährleisten. Des weiteren müssen diese Maßnahmen nach diesem Artikel unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist. Alle Netzbetreiber sind demnach gesetzlich verpflichtet, den Fernmeldeverkehr vor widerrechtlicher Überwachung zu schützen. Die Tatsache, daß solche Dienste europaweit arbeiten, und der verstärkte grenzüberschreitende Wettbewerb werden dazu führen, daß die Forderung nach einer Harmonisierung dieser Bestimmungen laut wird.

Die allgemeine Datenschutzrichtlinie 95/46/EC verpflichtet in Artikel 17 Kontrolleure und für die Datenverarbeitung Verantwortliche dazu, ein angemessenes Sicherheitsniveau

---

19 Es gibt Sicherheitsbestimmungen für elektrische Bauteile von Computern, aber keine Vorschriften in Bezug auf die von einem Computer verarbeiteten Daten.

20 http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm#HD_NM_15

21 ABl. C 364 vom 18.12.2000, www.ue.eu.int/df/docs/de/CarteDE.pdf

22 Richtlinien 95/46/EG (ABl. Nr. L 281 vom 23.11.1995) und 97/66/EG (ABl. Nr. L 24 vom 30.1.1998) http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf

23 „Die Mitgliedstaaten stellen durch innerstaatliche Vorschriften die Vertraulichkeit der mit öffentlichen Telekommunikationsnetzen und öffentlich zugänglichen Telekommunikationsdiensten erfolgenden Kommunikation sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Kommunikationen durch andere Personen als die Benutzer, wenn keine Einwilligung der betroffenen Benutzer vorliegt, es sei denn, diese Personen seien gemäß Artikel 14 Absatz 1 gesetzlich dazu ermächtigt.

entsprechend den durch das Verarbeiten und die Natur der zu schützenden Daten gegebenen Gefahren zu gewährleisten, insbesondere wenn die Verarbeitung Datenübertragung über ein Netz einschließt. Sie müssen angemessene technische und organisatorische Maßnahmen treffen gegen ‚die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang - insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden, und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten

Diese Vorschriften haben Implikationen für die Sicherheitserfordernisse in Netzen und Informationssystemen, die von solchen Personen und Organisationen, wie zum Beispiel e-commerce-Anbietern genutzt werden. Der pan-europäische Charakter von Diensten und stärkerer grenzüberschreitender Wettbewerb führen zu einem wachsenden Bedürfnis nach Spezifizierung der anzuwendenden Mittel zur Beachtung dieser Vorschriften.

Der **rechtliche Rahmen der EU für Telekommunikationsdienste** beinhaltet verschiedene Vorschriften mit Bezug auf ‘die Sicherheit des Netzbetriebes’ (i.e. die Verfügbarkeit von Netzen im Notfall) und Netzintegrität (i.e. die Sicherstellung von normalem Betrieb von zusammengeschalteten Netzen).[24] Die Kommission hat im Juli 2000 einen neuen rechtlichen Rahmen für elektronische Kommunikationsdienste vorgeschlagen, der zur Zeit im Mitentscheidungsverfahren im Rat und im Europäischen Parlament diskutiert wird. Die Kommissionsvorschläge nehmen im wesentlichen – wenn auch mit Änderungen – die bestehenden Vorschriften zu Netzsicherheit und –integrität wieder auf.

Der bestehende rechtliche Rahmen betrifft daher also neben den spezifischen Punkten, die Gegenstand der jeweiligen Rechtstexte sind, auch bestimmte Aspekte von Netzen und Informationssystemen, die von der vorliegenden Mitteilung angesprochen werden.

Die Mitteilung über die **Computerkriminalität** hat in der Europäischen Union eine Diskussion über die angemessene Reaktion auf kriminelle Aktivitäten ausgelöst, die sich des Computers und elektronischer Netze bedienen. Die strafrechtlichen Bestimmungen der Mitgliedstaaten sollten den unberechtigten Zugang zu Computernetzen abdecken, einschließlich der Verletzung persönlicher Datensicherheit. Die Diskussion zwischen allen interessierten Parteien wird im Rahmen des EU-Forums, das in Kürze eingerichtet wird, wie in der Kommissionsmitteilung zu Computerkriminalität angekündigt, fortgesetzt. Derzeit findet in diesem Bereich keine Annäherung der Strafrechtsvorschriften auf EU-Ebene statt. Dies kann zu Problemen bei der Ermittlung gegen solche Straftaten führen, außerdem werden potentielle Hacker oder ähnliche Angreifer nicht ausreichend abgeschreckt. Eine Annäherung der Rechtsvorschriften bezüglich des Einbruchs in Computernetze ist deshalb wichtig, weil dadurch die Zusammenarbeit der Justizbehörden der Mitgliedstaaten erleichtert wird.

Die berechtigten Bedenken in bezug auf Computerkriminalität erfordern effiziente polizeiliche Ermittlungen. Diese rechtlichen Bedenken sollten jedoch keine Lösungen schaffen, bei denen rechtliche Erfordernisse zu einer Schwächung der Sicherheit von Kommunikations- und Informationssystemen führen

Vorgeschlagene Aktionen:

[24] Liberalisierungsrichtlinie der Kommission 90/388/EC, Zusammenschaltungsrichtlinie 97/33/EC, Sprach-Telefonierichtlinie 98/10/EC.

- Es ist eine allgemein anerkannte Definition der rechtlichen Implikationen von Sicherheit in elektronischer Kommunikation ist erforderlich. Zu diesem Zweck wird die Kommission ein Inventar nationaler Maßnahmen, die im Einklang mit dem relevanten Gemeinschaftsrecht getroffen worden sind, einrichten.

- Die Mitgliedstaaten und die Kommission sollten den freien Warenverkehr mit Verschlüsselungsprodukten und -diensten durch verstärkte Harmonisierung der Verwaltungsverfahren für den Export und durch eine weitere Erleichterung der Ausfuhrkontrollen fördern.

- Die Kommission wird eine legislative Maßnahme gemäß Titel VI des Vertrags über die Europäische Union zur Annäherung der Strafvorschriften der Mitgliedstaaten in Bezug auf Angriffe auf Computersysteme, einschließlich Hacking und der gezielten Überlastung von Servern vorschlagen.

3.7. Sicherheit bei der Anwendung durch staatliche Stellen

Mit dem Aktionsplan von *e*Europe 2002 wird das Ziel verfolgt, eine wirksame und effiziente Interaktion zwischen den Bürgern und der öffentlichen Verwaltung zu fördern. Da viele der Daten, die zwischen Bürgern und der Verwaltung ausgetauscht werden, personenbezogen oder vertraulich sind (Daten medizinischer, finanzieller, rechtlicher Art) ist die Sicherheit entscheidend dafür, daß solche Kommunikationsverfahren sich durchsetzen. Außerdem wird durch die Entwicklung elektronischer Behördendienste (*E-Government*) die öffentliche Verwaltung sowohl zum potentiellen Vorbild für wirksame und sichere Lösungen als auch zum Marktbeteiligten, der in der Lage ist, durch seine Beschaffungsentscheidungen die Entwicklungen zu beeinflussen.

Die öffentliche Verwaltung muß nicht nur Informations- und Kommunikationstechnologie-Systeme beschaffen, die den Sicherheitsanforderungen genügen, sondern auch eine Sicherheitskultur in ihren Organisationen schaffen. Dies läßt sich durch die Erarbeitung von „organisationsbezogenen Sicherheitsstrategien“ erreichen, die auf die Bedürfnisse der jeweiligen Einrichtung zugeschnitten sind.

Vorgeschlagene Aktionen:

- Die Mitgliedstaaten sollten wirksame und interoperable Informationssicherheits-Lösungen als wesentliche Anforderung in ihre Tätigkeiten im Bereich elektronischer Behördendienste und elektronischer Beschaffung aufnehmen.

- Die Mitgliedstaaten sollten elektronische Signaturen bei elektronischen Behördendiensten einführen.

- Im Rahmen der eKommission wird die Kommission eine Reihe von Maßnahmen ergreifen, um die Sicherheitserfordernisse in ihren Informations- und Kommunikationssystemen zu stärken.

3.8. Internationale Zusammenarbeit

Genau in dem Maße, wie Kommunikation, die die Netze benutzt, in Sekundenbruchteilen die Grenze überschreitet, tun dies auch die damit verbundenen Sicherheitsprobleme. Das Netz ist nur so sicher wie sein schwächstes Glied und Europa kann sich nicht vom Rest des globalen Netzes isolieren. Folglich erfordert das Angehen von Sicherheitsthemen internationale Zusammenarbeit.

Die Europäische Kommission beteiligt sich bereits an der Arbeit internationaler Foren wie beispielsweise G8, OECD und VN. Der privatwirtschaftliche Sektor beschäftigt sich in eigenen Organisationen wie dem *Global Business Dialogue* (www.GBDe.org) oder dem *Global Internet Project* (www.GIP.org) mit Sicherheitsfragen. Ein fortdauernder Dialog zwischen diesen Organisationen wird für die weltweite Sicherheit essentiell sein.

Vorgeschlagene Aktion:

- Die Kommission wird den Dialog mit internationalen Organisationen und Partnern über Netzsicherheit und insbesondere über die zunehmende Stabilität von elektronischen Netzen.

4. Die nächsten Schritte

In dieser Mitteilung wurde ein strategisches Rahmenkonzept für Maßnahmen auf diesem Gebiet entworfen. Dies ist lediglich ein erster Schritt und noch kein endgültiger Aktionsplan zur Förderung der Netzsicherheit in Europa. Es werden jedoch erste Aktionen vorgeschlagen, um einen Rahmen für einen gemeinsamen europäischen Ansatz zu schaffen.

Als nächster Schritt müssen dieser Rahmen und die vorgeschlagenen Aktionen von den Mitgliedstaaten und dem Europäischen Parlament diskutiert werden. Der Europäische Rat könnte am 15./16. Juni in Göteborg die Richtung für das weitere Vorgehen aufzeigen.

Die Kommission schlägt vor, eine ausführliche Diskussion mit der Industrie, den Nutzern und den Datenschutzbehörden über die praktischen Einzelheiten der Durchführung der vorgeschlagenen Aktionen in Gang zu bringen. Kommentare können bis Ende August 2001 an eeurope@cec.eu.int. Deshalb ist diese Mitteilung auch eine Aufforderung zur Stellungnahme der betroffenen Parteien im Hinblick auf die Definition eines endgültigen Maßnahmenkatalogs. Dieser könnte bis Ende 2001 zu einem Konzept entwickelt werden.

***