Sicherheit im Netz – Was kann der Gesetzgeber tun? Europäische Ansichten und Aussichten.

Ernst Weiss

Montrichard, Frankreich
Verwaltungsdirektor i. R.
Former Chairman European Telecommunications Platform, Brüssel

1 Einführung

Dass Kommunikationsnetze in der Wissensgesellschaft, ähnlich den Nervensystemen in der Humanmedizin, eine außerordentlich wichtige Bedeutung haben, ist seit langem bekannt. Seit der Erfindung der Telegraphie existieren Regulierungsformen, die eine möglichst reibungslose Nutzung dieser Kommunikationsmittel sicherstellen sollen. Mit steigendem technologischem Fortschritt bekommt jedoch die Frage nach ihrer Sicherheit eine immer größere Bedeutung, aber auch einen immer größeren Umfang.

Die Frage nach der Verletzbarkeit der Kommunikationsnetze, vor allem hochsensibler Netze, wie sie für Forschung und Entwicklung betrieben werden, ist daher ja nicht so ganz neu. Noch vor ein paar Jahren war eine relative Sicherheit der Übertragungswege im Festnetz, bei Mietleitungen und in virtuellen Netzen mittels elektronischer Verschlüsselungssysteme wirtschaftlich machbar, aber es hatte doch einen mühsamen Weg globaler Vereinbarungen geben müssen, um eine vernünftige Ausbalancierung der Interessen nationaler Sicherheit mit den Anforderungen der Wirtschaft, Industrie und Forschung zu erreichen.

Während man bisher glaubte im Netz nur professionellen Angriffen, wie zum Beispiel Wirtschaftsspionage, Sabotage etc. , begegnen zu müssen, hat erst das Internet mit seinen offenen Strukturen auch die allgemeine Anfälligkeit moderner Übertragungstechnologien für fahrlässige oder mutwillige Verletzungen offen gelegt. Diese reichen von einfachen Belästigungen durch unerbetene Werbung (Spams) bis zur Zerstörung von Systemen und Anlagen durch Viren, Terrorismus und Naturkatastrophen

Über den Umfang der Schäden gibt es bisher wenig verlässliches Material. Eine Studie der Computer Intrusion Squad des amerikanischen FBI wurde jetzt im Jahresbericht 2001 zur Computerkriminalität in den USA veröffentlicht. Der Bericht befindet nach Befragen von 538 IT-Sicherheitsexperten aus Industrie und Verwaltung, dass die Bedrohung durch Computerkriminalität und kriminelle Verletzungen von IT Sicherheitssystemen unvermindert anhält und die finanziellen Schäden stetig anwachsen.

> 85 % der Befragten beklagten Verletzungen von Sicherheitsvorkehrungen in den letzten 12 Monaten.
> 64 % der Befragten bestätigten, finanzielle Verluste durch diese Straftaten erlitten zu haben, wovon 35 % sie auch quantifizieren konnten. Diese Angaben addierten sich zu einer Summe von 378 Milliarden US$

70 % der Befragten gaben Internetverbindungen als Schadensquelle an, während
30 % die Ursache in den eigenen internen Systemen sahen.
36 % der Befragten meldeten die Verletzungen den Strafverfolgungsbehörden.

Während man sich bis vor Kurzem auf den Schutz der Übertragungswege konzentrierte, wurde aber durch die Ereignisse der letzten Monate auch der Ruf nach geregeltem Schutz der Inhalte immer lauter.

2 Liberalisierung des Marktes und seine Sicherheit

Im Bestreben einen gemeinsamen Markt in und für Europa zu schaffen, haben sich daher auch die Gesetzgeber zu den Fragen der Sicherheit elektronischer Übertragungsformen Gedanken machen müssen, denn Sicherheit ist eine wichtige Herausforderung für die Politik geworden. Das Auffinden einer angemessenen Antwort wird aber 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 in den letzten Jahren bereits 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 zu treffenden politischen Maßnahmen zur Netz- und Informationssicherheit müssen daher im Zusammenhang der bestehenden Telekommunikations- und Datenschutz-Gesetzgebung, aber auch in bezug auf die Bekämpfung der Cyberkriminalität gesehen werden. Die Netz- und Informationssicherheit kann verstanden werden als die Fähigkeit eines Netzes oder Informationssystems, mit einem vorgegebenen Niveau Störungen oder böswilligen Aktionen abzuwehren, welche 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 Sicherheitsprobleme können wie folgt gruppiert werden:

- Elektronische Kommunikation kann abgehört und Daten können kopiert oder verändert werden. Dabei entsteht Schaden sowohl durch das Eindringen 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.
- 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 Sicherheitsprobleme gehen aber auch von unvorhergesehenen und unabsichtlichen Ereignissen aus, wie z. B. Naturkatastrophen (Überschwemmungen, Stürme, Erdbeben), Geräte- oder Softwareausfall, oder menschliches Versagen.

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 eine Hauptkomponente im kommenden Rahmenprogramm werden.
- **Förderung von marktorientierter Standardisierungs- und Zertifizierung:** Die Europäischen Standardisierungsorganisationen werden aufgefordert, die Arbeiten über Kompatibilität 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 und wo erforderlich, Wettbewerbe für Europäische Verschlüsselungs- und Sicherheitslösungen ausschreiben..
- **Rechtlicher Rahmen:** Die Kommission wird ein 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 öffentlichen IT-Systeme integrieren. Sie sollten elektronische Signaturen für öffentliche Dienste einführen.
- **Internationale Zusammenarbeit:** Die Kommission wird den Dialog über Netz- und Informationssicherheit mit internationalen Organisationen und Partnern verstärken.

Es wird allgemein gefolgert, dass zur Lösung der Probleme eine bessere Zusammenarbeit erforderlich ist und es wird eine Reihe konkreter Maßnahmen vorgeschlagen, die zur Zeit von den Mitgliedstaaten und dem Europäischen Parlament diskutiert werden.. Darüber hinaus schlägt die Kommission vor, eine ausführliche Diskussion mit der Industrie und den Nutzern über die praktischen Einzelheiten der Durchführung der vorgeschlagenen Aktionen in Gang zu bringen.

3 Maßnahmen zur Sicherung des IT-Marktes

3.1 Die Cybercrime Konvention

Der EU Ministerrat hatte bereits im Jahre 1997 eine Expertengruppe eingesetzt, um bindende rechtliche Maßnahmen auszuarbeiten, die einen ausreichenden Schutz bei den vielfältigen Vorkommnissen im Cybercrime ermöglichen können. Im April 2000 wurde ein Entwurfstext im Internet veröffentlicht und im Juni 2001 der letzte Entwurf beendet.

Offensichtlich beschleunigt durch die Ereignisse des 11. Septembers in New York hat der Europarat am 19. September den letzten Entwurf angenommen und ihn am 8. November der Tagung des Rates der Außenminister vorgelegt. Diese **Convention on Cybercrime** wurde am 23. November 2001 von 31 Staaten unterzeichnet, darunter auch von drei nichteuropäische Staaten, nämlich USA, Kanada und Japan. Das Vertragswerk tritt in Kraft, wenn es von mindestens 5 Staaten ratifiziert wurde, davon müssen 3 Staaten Mitglied der EU sein.

In der Präambel des Vertrages wird als Ziel die gemeinsame Durchführung einer allgemeinen Kriminalpolitik genannt, die zum Schutz der Gesellschaft gegen Cybercrime, geeignete Rechtsformen schaffen und die internationale Zusammenarbeit fördern soll. Im Einzelnen beinhaltet der Vertrag folgende Themen:

Kapitel I Begriffsbestimmungen

Kapitel II Maßnahmen die auf nationaler Ebene zu treffen sind

Abschnitt 1 Materielles Strafrecht

Titel 1 Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und – systemen.

Titel 2 Computerstraftaten

Titel 3 Inhaltsbezogenen Straftaten

Titel 4 Straftaten im Zusammenhang mit Verletzungen des Urheberrechtes und verwandter Schutzrechte

Titel 5 Nebenformen der Verantwortlichkeiten und Sanktionen

Abschnitt 2 Verfahrensrecht

Abschnitt 2 Gerichtsbarkeit

Kapitel III Internationale Zusammenarbeit

Diese sogenannte „Budapester Konvention“ gilt als erstes internationales Vertragswerk, das jene Vergehen definiert, die mit Hilfe des Internet verübt werden können. Das Cybercrime-Abkommen sieht dafür erweiterte Befugnisse zum Abhören der Internetkommunikation und zum grenzüberschreitenden Datenaustausch vor. Internetkommunikation soll in Echtzeit abgehört werden können, und es müssen Vorkehrungen getroffen werden, die Verkehrsdaten zu speichern.

Neben der strafrechtlichen Einordnung von illegalem Abhören, dem Eindringen und Stören von Computersystemen, dem Stehlen, Manipulieren oder Löschen von Daten stellt das Abkommen auch Vergehen gegen das Copyright, das Umgehen von Kopierschutzsystemen, das Herstellen, Verbreiten und Verfügbarmachen von Kinderpornographie sowie Verbrechen, die unter Ausnutzung von Computer-Netzwerken begangen werden können (Betrug, Geldwäsche, Vorbereitung terroristischer Akte), unter Strafe.

Die Konvention verpflichtet die Unterzeichner, diese Straftatbestände und ihre Ahndung in ihre nationale Gesetzgebung aufzunehmen. Sie sieht auch grenzüberschreitende Verfahren und Mechanismen bei der Strafverfolgung vor. Polizeibehörden eines Landes sollen Kollegen eines anderen Landes gegebenenfalls zu rascher Amtshilfe auffordern können. Zu diesem Zweck soll ein rund um die Uhr tätiges internationales Kontaktnetzwerk eingerichtet werden, Internet-User oder Domain-Besitzer sollen grenzüberschreitend identifiziert werden und Web-Seiten, deren Inhalte gegen die Konvention verstoßen, sollen aus dem Web entfernt werden können.

Keinen Eingang in die Straftatbestandsliste der Konvention fand die Verbreitung rassistischer und fremdenfeindlicher Inhalte. Dies hätte keine Zustimmung seitens der USA gefunden, wo die Redefreiheit verfassungsmäßig weiter gespannt ist. Ein Zusatzprotokoll soll sich zu einem späteren Zeitpunkt dieser Thematik annehmen. Um Rechtsextremisten die Möglichkeit zu verbauen, ihre Seiten auf Server in einem anderen Land zu legen, das weniger strenge Gesetze hat oder in dem auch solche Meinungen durch die Verfassung geschützt sind (wie z. B. in den USA), soll in diesem Zusatzprotokoll etwa der Tatbestand des „illegalen Hosting“ eingeführt werden.

Wie zu erwarten, blieb das Cybercrime-Abkommen von Kritik nicht verschont. Die Konvention stärke die Behörden und nehme wenig Rücksicht auf die private Sphäre der Internet-Bürger, beklagten britische Bürgerrechtsgruppen, wie auch verschiedene politische Gruppierungen in Deutschland. Hier sollte man aber bedenken, dass es ausschließlich um die Verfolgung strafrechtlich relevanter Tatbestände geht, für die es eine Reihe geltender Europarats-Konventionen gibt, welche die Rechtsstaatlichkeit von Strafverfahren und die Achtung der Menschen- und Bürgerrechte sowie des Datenschutzes sichern.

3.2 Weitere Maßnahmen der EU im Bereich der Netz- und Informations-Sicherheit

Unter Hinweis auf die bestehenden Richtlinien für die Sicherheit elektronischer Netze und in Erwägung der Gründe für eine verstärkte Maßnahme zur Sicherung der Netze und Informationen, hat der EU Rat am 28. Januar 2002 in einer **Entschließung zu einem gemeinsamen Ansatz und spezifische Maßnahmen im Bereich der Netz- und Informationssicherheit** die Mitgliedstaaten unter anderem ersucht:

- bis Ende 2002 Initiativen für die Sensibilisierung der Netz- und Informationssicherheit einzuleiten
- bewährte Praktiken zu fördern,
- bis Ende 2002 die Bedeutung der Sicherheitskonzepte als Teil der Computerausbildung zu fördern
- bis Mitte 2002 die Wirksamkeit nationaler Vereinbarungen über Computer-Notfalldienste (Virenwarnsysteme) auf ihre Wirksamkeit zu überprüfen
- bis Ende 2002 wirksame Sicherheitslösungen für netzgestützte Behörden- und Beschaffungsdienste zu finden

Auf der Basis der Cybercrime Konvention von 2001 hat die EU Kommission am 19. April 2002 einen Vorschlag für einen **Rahmenbeschluss des Rates über Angriffe auf Informationssysteme** beschlossen und dem EU Parlament und dem EU-Rat zur Beschlussfassung zugeleitet. In der Begründung wird angeführt, dass die Mitgliedstaaten nicht ausreichend dafür sorgen können, dass Angriffe auf Informationssysteme in allen Mitgliedstaaten mit wirksamen, angemessenen und abschreckenden Strafen geahndet werden. Hierzu bedürfe es gemeinsamer, miteinander zu vereinbarender Regeln, die von der EU in Übereinstimmung mit dem Subsidiaritätsprinzip beschlossen werden können.

Der Rahmenbeschluss stellt darauf ab, durch Angleichung der einzelstaatlichen Strafrechtsvorschriften für Angriffe auf Informationssysteme die Zusammenarbeit zwischen den zuständigen Behörden der Mitgliedstaaten zu verbessern. Erfasst werden die Tatbestände

- Rechtswidriger Zugang zu Informationssystemen (Artikel 3)
- Rechtswidriger Eingriff in Informationssysteme (Artikel 4)
- Anstiftung, Beihilfe und Versuch (Artikel 5)

Darüber hinaus wird zum Zwecke des Informationsaustausches (Artikel 12) die Einrichtung operativer Kontaktstellen bei den Mitgliedstaaten vorgeschlagen, die rund um die Uhr an allen Tagen erreichbar sein sollen.

4 Datenschutz und elektronische Kommunikation

Der Entwurf einer **Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation** war Bestandteil eines Paketes von Richtlinien, die einen neuen Rechtsrahmen für die Regulierung der Telekommunikation in Europa darstellen. Der Entwurf soll die derzeitige Richtlinie 95/46/EC um die technologische Neutralität aktualisieren und die Einbeziehung neuer Kommunikationsdienste, wie das Internet; gewährleisten.

Während man bisher nur von “leitungsvermittelten Anrufen” ausgeht, versteht man jetzt, um den Umfang auch auf Internet-Protokoll- und andere verbindungslose Netze auszuweiten., unter “Verkehrsdaten” jegliche Daten, die im Zuge oder zum Zweck der Übertragung einer Nachricht über ein elektronisches Netz verarbeitet werden

Die Artikel 7 und 8 befassen sich mit Vertraulichkeit bei Einzelgebührennachweisen und Anrufer-Identifizierung, wobei relativ lapidar ausgeführt wird, dass Vertraulichkeit zu

wahren ist und dass es den Mitgliedstaaten überlassen ist, geeignete innerstaatliche Maßnahmen zu treffen.

Das hier behandelte Problem unerbetener Nachrichten (Spams) ist außergewöhnlich komplexer Natur, es gibt viele feste Meinungen und wenig Verständigung. Ein großes Problem unerwünschter Kommunikation ist, dass viele dieser Anrufe in anderen Ländern ihren Ursprung haben. Folglich wird es notwendig sein, globale Lösungen zu finden. Die Kommission sollte verstärkt mit anderen Staaten zusammenarbeiten, besonders mit den USA:

Das Vorschlagspaket der TK-Rahmenrichtlinien war nach einem Kompromissvorschlag der belgischen Präsidentschaft im Dezember 2001 verabschiedet worden. Um die Verabschiedung des Paketes jedoch nicht zu gefährden, hat man den Entwurf für die neue Datenschutzrichtlinie für elektronische Kommunikation ausgeklammert, da es zu Kontroversen bei der Forderung nach Aufbewahrung von Berechnungsunterlagen durch die Betreiber gekommen war. Dieses war von den Mitgliedstaaten aus Gründen nationaler Sicherheit verlangt worden, aber Parlament und Kommission wollen dieses Recht nur sehr limitiert zugestehen. Mit einer Verabschiedung der Verordnung ist aber in den nächsten Tagen zu rechnen.

5 Sicherheit im Internet

Die EU engagiert sich nach Verabschiedung des neuen TK Regulierungspaketes verstärkt um die Frage der Online-Sicherheit: Die Kommission hat, den Empfehlungen des eEuropa Benchmarking Reports 2002 folgend, den Aktionsplan zur sichereren Nutzung des Internet um zwei Jahre verlängert und zusätzliche 13,3 Milliarden Euro bereit gestellt. Dieser Verlängerung hat der Rat der TK-Minister am 25. März 2002 zugestimmt. Der zuständige EU-Kommissar Erkki Liikanen erklärte, man wolle sich nun vor allem darauf konzentrieren, das Bewusstsein der Anwender für Fragen der Sicherheit im Netz zu schärfen.

Konkret sollen neue Filter- und Bewertungssysteme für Inhalte entwickelt werden, um so etwa rechtsradikalen Inhalt auszusondern. Außerdem plant die Kommission die Errichtung eines Netzes von Meldestellen in Europa sowie Maßnahmen zur Förderung der Selbstkontrolle. Ursprünglich wäre der Aktionsplan im Jahr 2002 ausgelaufen, der Finanzrahmen sollte 25 Millionen Euro nicht überschreiten.

Diese Entscheidung hat in Mitgliedstaaten der EU, vor allen in Deutschland, sehr unterschiedliche Reaktionen ausgelöst. Security-Unternehmen und Forscher haben die Entscheidung der EU-Kommission, den Aktionsplan zur sicheren Nutzung des Internet zu verlängern und weitere Geldmittel dafür bereitzustellen, mit großer Skepsis aufgenommen. Vor allem die neuen Erweiterungen stoßen auf Kritik. Die vorgeschlagene Europäische Meldestelle für „gefährliche Inhalte“ wird von manchen Branchenkennern als Anstiftung zur Denunziation betrachtet, da eine Definition so genannter “übler” Inhalte nahezu unmöglich sei.

Dieses Argument wird auch von anderen aufgenommen, denn man könne sich nicht vorstellen, dass eine Art Web-Polizei bestimmt, was gut und richtig ist für alle. Außerdem sei die länderübergreifende Regelung, welche Inhalte strafbar sind, noch ausständig

Hierbei wird aber übersehen, dass das Bundes-Innenministerium bereits im Februar 2000 den Arbeitsstab "Sicheres Internet" eingerichtet hat. "Hier sollen alle rechtlichen und technischen Möglichkeiten geprüft werden, um mit modernsten und schnellen Maßnahmen vorgehen zu können", erklärte Bundesinnenminister Otto Schily (SPD). Die Regierung wolle ferner internationale Mindeststandards fordern, um Volksverhetzung und Aufruf zum Rassenhass im Internet unter Strafe stellen zu können.

6 Der Regulierer in Europa und die Sicherheit im Netz

Aber es geht hier ja nicht nur um Inhalte, sondern um die Sicherheit der Information allgemein. Wie es scheint wird uns dieses Thema in den nächsten Monaten noch sehr beschäftigen, denn es wird auf der Tagesordnung des kommenden EU Gipfels in Sevilla zum Abschluss der spanischen Präsidentschaft stehen.

Wie auch aus Dänemark verlautet, wird Sicheres Internet ein Prioritätsthema im Programm der kommenden Präsidentschaft ab Juli 2002 sein. Und so kam es nicht von ungefähr, dass Anfang April in Kopenhagen von der Independent Regulators Group IRG, der Interessengemeinschaft der nationalen Regulierungsbehörden, ein Seminar zum Thema IT Sicherheit veranstaltet wurde und es ist wahrscheinlich interessant, diese Problematik aus der Sicht des Regulierers zu sehen.

Hier wurde festgehalten, dass in der Verantwortung der Regierungen vorrangig liegt, öffentliche Werte zu schützen und nicht nur für das Funktionieren der Kräfte des Marktes zu sorgen, aber die Erfahrung zeigt, dass der Markt kaum interessiert ist, in aufwendige Sicherheits-Systeme zu investieren. Besonders Verbraucher und kleinere Unternehmen sind eher geneigt, unsichere Betriebssysteme und Software zu akzeptieren, vielleicht wird mal gerade etwas kostenlose Antivirus-Software oder ein Firewall-System heruntergeladen und es besteht wenig Interesse, sich eingehender mit der vorhandenen Software zu befassen, um sie sicherer zu machen. Internationale Service Provider (ISP) gibt es wie Sand am Meer, aber keiner von ihnen hat bisher ein Sicherheitspaket angeboten, welches nicht nur vor Viren und Hackern schützt, sondern auch in der Lage ist, unerwünschtes Email (Spams) auszufiltern. Das ist für ISPs zur Zeit noch kein Markt, weder in Europa noch anderswo, aber das kann sich schnell ändern. Ergo wird der Ruf nach dem Regulierer immer lauter.

Hinsichtlich internationaler Zusammenarbeit gab es kaum ein Argument, sowohl zwischen Regierungen, als auch zwischen Regulierern, oder privaten Organisationen. Das Problem liege nur in der Möglichkeit, oder Unmöglichkeit, sie in Internet-Zeit zu bewältigen.

Folgende weitere Themen wurden in diesem Seminar angesprochen:

Harmonisierung von Sicherheitsmassnahmen.

Am Nutzen internationaler Harmonisierung aller Sicherheitsmaßnahmen in der elektronischen Kommunikation besteht kein Zweifel. Die Teilnehmer des Seminars bestätigten auch, dass in allen Ländern gleiche Anforderungen und gleiche Probleme bestehen. Die Problemstellung der IT Sicherheit ist auch von großen Organisationen, wie der G8, der

OECD, vom Europa-Rat und der Europäischen Gemeinschaft erkannt worden und grenzüberschreitende Kooperation ist gefordert. Überall werden die gleichen Diskussionen geführt, aber es ist wichtig, dass alle in die gleiche Richtung ziehen und dafür Sorge tragen, dass alle Maßnahmen und Lösungen auch überall konsistent durchgeführt werden, denn für den Nutzer ist es im internationalen Betrieb ein Alptraum mit 15 verschiedenen Betriebssystemen und Software in jedem der 15 Mitgliedstaaten arbeiten zu müssen.

Widersprüchliche Sicherheitsprobleme

Es scheint offensichtlich, das Sicherheitsprobleme der Nutzer anders gesehen werden, als Sicherheitsprobleme, bei denen es um das Recht geistigen Eigentums von Herstellern und Anbietern geht. Während auf der einen Seite Software-Konfigurationen angeboten werden, die nicht einmal ein Mindestmaß an Sicherheit bieten, werden auf der anderen Seite nicht kopierbare CDs und DVDs angeboten. Im amerikanischen Kongress ist ernsthaft erwogen worden, die Kopierfunktionen bei Computer Hardware und Software gesetzlich zu verbieten. Wenn es verboten ist, Software zu kopieren in der alle Sicherheitsvorkehrungen unbrauchbar sind, liegt der Widerspruch auf der Hand,

Verfahrensweisen Sicherheitsprobleme zu lösen

Abläufe, die Sicherheitssysteme betreffen, sind nicht schnell zu verändern. Wenn man noch die Zeit für Umstellung und Umgewöhnung bei Menschen und Betrieben berücksichtigt, muss man für eine Umstellung im Netzbereich mit einem Zeitraum von zwei bis drei Jahren rechnen.

Hierbei müssen auch die peripheren Geräte berücksichtigt werde, wie z.b.: PCs, Telefonanlagen, Set.top Boxes, Spielgeräte und sogar Haushaltsgeräte.

> Ein Hersteller aus Südkorea bietet bereits einen Kühlschrank an, der selbsttätig über das Internet Ihren Lebensmittelbedarf bestellt. Können Sie sich vorstellen dass ein Hacker Ihren Kühlschrank abstellt, oder ein Kilo Kaviar und ein Dutzend Austern bestellt, oder ein Kilo Kalbfleisch für einen Vegetarier?

Aber auch die ganze Palette der Hersteller und Anbieter muss berücksichtigt werden und es ist fraglich, ob NRBs für alle zuständig sind und ob die Nichtzuständigen, wie z.b die ISPs, bereit sind, Anweisungen zu folgen. Wir müssen uns auch fragen, ob die NRBs über die genügenden Ressourcen verfügen, dieser Aufgabe gerecht zu werden, ohne ihre eigentlichen Aufgaben zu vernachlässigen.

Man war sich einig, dass sich über den Umfang neuer Sicherheitsmassnahmen zum gegenwärtigen Zeitpunkt noch wenig sagen lässt, während man sich über den Wert von Aufklärung und Forschung aber durchaus klar war. Ein beträchtlicher Mangel geeigneter Statistiken ist ein weiteres Problem.

Robert Verrue, Generaldirektor der EU Kommission Informationsgesellschaft, gab einen Überblick über das komplexe Angebot von Initiativen der EU Kommission und verschiedene Male wurde auf die Konvention gegen Cybercrime des Europa-Rates hingewiesen. Auch der OECD Leitfaden für Sicherheit von Informations-Systemen wurde als sehr nützlich angesehen. Alles in allem gebe es genügend Impulse, aber es mag die Überlegung gestattet sein, ob nicht zu viele Köche den Brei verderben.

Für den Beobachter scheint jedoch ein Mangel an praktischer und pragmatischer Hilfe für Personen und Unternehmen zu bestehen, geeignete Sicherheits-Systeme zu erwerben oder selbst zu konfigurieren. Wenn man die Risiken kennt, sollte man in der Lage sein, etwas dagegen zu tun, ohne gleich einen 3-Tage -Trainingskurs besuchen zu müssen

Standards für Sicherheitssysteme?

Robert Verue kam in seiner Rede auf den "unsportlichen Geist" mancher Marktteilnehmer zu sprechen. Gemeint waren damit wohl Aktivitäten, die leicht am Rande der Legalität stehen. Wir haben Beispiele hierfür im GPRS erlebt, wenn Mobilfunkbetreiber aus "Sicherheitsgründen" Firewall-Systeme installieren, sich aber in Wirklichkeit abschotten gegen Dritt-Party-Aktivitäten ihrer Kunden. Netz-Integrität hat eine ellenlange Geschichte des Missbrauches durch dominante Betreiber. Die Entbündlung der Ortsnetze hat in letzter Zeit viele Beispiele einfallsreicher, um nicht zu sagen "bizarrer", Taktiken dominanter Betreiber gezeigt, mit denen Wettbewerber behindert oder verzögert werden. Daher scheint die Schaffung technischer Standards für die Sicherheit von IT Systemen für einen fairen Wettbewerb im Markt kontraproduktiv zu sein. Kennzeichnung wäre eine nützlichere Methode, die für den Wettbewerb weitaus weniger schädlich ist.

Was folgert hieraus aus der Sicht des Regulierers ?

Im Seminar wurde über sicheres Internet gesprochen, aber es mangelt an Beweisen, dass Unsicherheit ein ernsthafter Faktor für die Nutzung des Internets ist.. Es wurde vorgebracht, dass Unsicherheit ein Hindernis im Umgang mit dem e-Commerce ist, was aber ebenso schwer nachzuweisen ist. Es wurden Vergleiche zur Sicherheit beim Autofahren gebracht, aber wir wissen, dass man sich derzeit mehr Gedanken um die Sicherheit von Fußgängern macht, die möglicherweise von Autos angefahren werden. Es ist eben alles eine Frage der Angleichung von Aufwand und Nutzen, aber man sollte das Kind nicht mit dem Bade ausschütten!

Einig war man sich natürlich über die Notwendigkeit, Fehler in IT-Systemen abzustellen, die Dritten Schaden zufügen können. Beunruhigend wurde der Mangel an Kontrolle und Aufsicht über IT Systeme empfunden. Es bedürfe wesentlich mehr Sicherheitsbewusstsein, mehr Austausch von Informationen und bessere Anleitungen für Anwender.

Internet Literatur zum Thema Netzsicherheit:

Convention on Cybercrime, Budapest, 23.XI.2001
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
http://conventions.coe.int/Treaty/EN/cadreprincipal.htm

Vorschlag für einen Rahmenbeschluss über Angriffe auf Informationssysteme.
KOM(2002)173 endgültig vom 19.04.2002:
http://europa.eu.int/eur-lex/de/com/pdf/2002/com2002_0173de01.pdf

Entschließung des Rates vom 28. Januar 2002 zu einem gemeinsamen Ansatz und spezifischer Maßnahmen im Bereich der Netz- und Informationssicherheit
OJ 43/2 vom 16.2.2002.
http://europa.eu.int/eur-lex/pri/de/oj/dat/2002/c_043/c_04320020216de00020004.pdf

Sicherheit der Netze und Informationen. Vorschlag für einen europäischen Politikansatz.
EU Kommission 6. Juni 2001
http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsec_de.pdf

Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsstrukturen und Bekämpfung der Computerkriminalität
KOM(2000) 890 endgültig vom 26.01.2001
http://europa.eu.int/eur-lex/de/com/cnc/2000/com2000_0890de01.pdf

Aktionsplan der Gemeinschaft zur Förderung einer sicheren Nutzung des Internet durch die Bekämpfung illegaler und schädigender Inhalte in globalen Netzen . Arbeitsprogramm 1999-2002.
http://europa.eu.int/information_society/programmes/iap/docs/pdf/programmes/workprgm/workde.pdf

Mitteilung der Kommission KOM (2002)152 endgültig vom 22.03.2002.
Folgemaßnahmen zum Aktionsplan 1999-2002.
http://www.europa.eu.int/eur-lex/de/com/pdf/2002/de_502PC0152.pdf

Pressemitteilung 23. 04.2002:
Kommission verabschiedet Vorschlag zur Bekämpfung von Computerkriminalität:
http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/02/601$l0|RAPID&lg=DE&display=

Pressebericht: 7. Mai 2002
Deutschland Nummer 1 beim Cybercrime
http://de.news.yahoo.com/020507/272/2r85u.html

Deutscher Datenschutz, Berlin 15.01.2000

Ministerkonferenz der G8 zur Bekämpfung transnationaler organisierter High-Tech Kriminalität, Moskau 19. und 20. Oktober 1999

http://de.news.yahoo.com/020507/272/2r85u.html