(Un–)Sicherheit im Internet

Wege zu einem besseren Schutz für Unternehmen und private Nutzer

Eine Veranstaltung der Friedrich-Ebert-Stiftung am 17. Juni 2002 in Hamburg

Herausgegeben vom
Wirtschafts- und sozialpolitischen Forschungs- und
Beratungszentrum der Friedrich-Ebert-Stiftung
Abt. Wirtschaftspolitik
Godesberger Allee 149, D-53170 Bonn
Umschlag: Pellens Kommunikationsdesign Bonn
Foto: Stefan Nicolay
Druck: Thenée Druck Bonn
Oktober 2002
ISBN 3-89892-120-4

Über das Projekt „Internetökonomie“ der Friedrich-Ebert-Stiftung

Das Projekt „Internetökonomie“ der Abteilung Wirtschaftspolitik im Wirtschafts- und sozialpolitischen Forschungs- und Beratungszentrum widmet sich seit Mitte 2000 den vielfältigen Facetten der wirtschaftlichen, politischen und gesellschaftlichen Veränderungen, die mit der Ausbreitung und Anwendung neuer Informations- und Kommunikationstechnologien zu erwarten sind bzw. bereits stattfinden.

Die im Themenraum „Neue Ökonomie – Wissens- und Informationsgesellschaft“ betrachteten Einzelaspekte sollen einen strategischen Bereich eingehender betrachten, dem noch vor wenigen Jahren sowohl in Politik als auch in Wirtschaft und Wissenschaft wenig Beachtung zuteil wurde.

In seiner Analyse und Diskussion der Prozesse will sich das Projekt bewusst nicht auf den deutschen Raum beschränken, sondern strebt an, den europäischen Blickwinkel zu erhalten. Das Projekt möchte mit Expertengesprächen und Publikationen seinen Beitrag leisten, zu einem tieferen Verständnis der allgegenwärtigen Transformationsprozesse beizutragen und damit letztlich Gestaltungsmöglichkeiten und Handlungsalternativen für politische Entscheidung8träger wie auch wirtschaftliche Akteure aufzuzeigen.

Eine Dokumentation der Projektaktivitäten findet man außerdem im Internet unter:

www.fes.de/internetoekonomie

Inhaltsverzeichnis

Vorwort

Zusammenfassung 1

1. Unternehmen im Visier von konkurrierenden Firmen und Hackern

1.1. Risikofaktoren für Unternehmen im Inter- und Intranet: Gefährdungspotenziale, Erscheinungsformen, Erkennungs- und Zugriffsmöglichkeiten 7

Prof. Dr. rer. nat. Dipl.-Phys. Klaus Brunnstein
Universität Hamburg, Fachbereich Informatik

1.2. Sicherheits- und Risikofaktor Provider? 14

Stefan Kratzer
Projektmanager Security, eco Electronic Commerce Forum e.V.

1.3. Forderungen an Politik und Gesetzgebung 17

Peter Schaar
Stellvertretender Datenschutzbeauftragter der Freien Hansestadt Hamburg

1.4. Maßnahmen der Bundesregierung für mehr Sicherheit im Internet aus Sicht des Wirtschaftsministeriums 19

Dr. Ulrich Sandl
Referatsleiter IT-Sicherheit, Bundesministerium für Wirtschaft und Technologie

1.5. Maßnahmen der Bundesregierung für mehr Sicherheit im Internet aus Sicht des Innenministeriums 22

Christoph Verenkotte
Referatsleiter Sicherheit in der Informationstechnik, Bundesministerium des Innern

2. Private Nutzer im Visier von Unternehmen und dubiosen Geschäftemachern

2.1. Gefahrenpotenziale und Missbrauchsziele: Von der elektronischen Signatur, systematischen Datenauswertung bis hin zu Viren und Trojanern 26

Jens Ohlig
Sprecher des Chaos Computer Clubs

2.2. Teure Dialer – Unseriöse Anbieter und ihre Tricks 33

Sascha Borowski
Journalist, Betreiber der Internetseiten www.dialerschutz.de

2.3. Produkte für mehr Sicherheit im Internet 37

Björn Dehms
Bundesamt für Sicherheit in der Informationstechnik (BSI)

2.4. Forderungen der Verbraucherschutzverbände und Antworten von Politik und Gesetzgebung: Statements

2.4.1. Verbraucherschutzpolitische Forderungen 43

Edda Castello
Leiterin der Rechtsabteilung der Verbraucher-Zentrale Hamburg

2.4.2. Rechtspolitische Problemfelder 48

Prof. Dr. Thomas Hoeren
Institut für Informations-, Telekommunikations- und Medienrecht, Westfälische Wilhelms-Universität Münster

2.4.3. Antworten von Politik und Gesetzgebung 51

Jella Teuchner, MdB
Verbraucherpolitische Sprecherin der SPD-Bundestagsfraktion

3. Diskussion und Ausblick 53

Moderatoren, Referenten und Teilnehmer/-innen an der Podiumsdiskussion, Tagungskonzeption und –organisation, Verfasser der Broschüre 71

Vorwort

Das Internet hat unwiderruflich Einzug in nahezu jedes Unternehmen und in die meisten Haushalte gefunden. Aus unserer heutigen virtuellen wie realen Welt ist es nicht mehr wegzudenken. Es gehört zu den treibenden Faktoren des gravierenden technologischen und gesellschaftlichen Wandels, den wir derzeit erleben.

Das neue Medium bietet enorme Chancen, aber auch immense Gefahrenpotenziale sowohl für Unternehmen als auch für private Nutzer. Diese Sicherheitsrisiken nehmen in rasanter Weise zu. Die Zahl der Internet-Nutzer, die mit Viren-Attacken zu kämpfen hat, steigt von Jahr zu Jahr. Ganze Datennetze werden lahmgelegt. E-Mails und Passwörter werden missbraucht, um Daten auszuspähen und zu manipulieren. Viele Nutzer wurden in der Vergangenheit Opfer von für sie nicht erkennbaren Web-Dialern, die unbemerkt teure 0190-Nummern anwählten und ihnen Telefonrechnungen in ungeahnter Höhe bescherten. Aber auch die Fehlbedienung von Computern und Programmen führt zu zusätzlichen Sicherheitsproblemen.

Generell gilt: Wer online geht, ist für andere sichtbar. Damit stellen sich völlig neue Herausforderungen an den Datenschutz bzw. den Verbraucherschutz. Es sind nicht nur die bekannten spektakulären Angriffe von jungen Hackerfreaks, die zeigen, wie verwundbar die Server von Unternehmen und anderen Institutionen sein können. Gefährlich sind auch die digitalen Einbrüche, die in die Rubrik Wirtschaftsspionage und Wirtschaftssabotage fallen. Von diesen gelangen erklärlicherweise nur die wenigsten Fälle an die Öffentlichkeit. Der materielle Schaden für die Unternehmen kann immens sein. Auch die Möglichkeit, dass Mitarbeiter als Innentäter gegen die Interessen des Arbeitgebers tätig werden, ist eine weitere Gefahrenquelle.

Die Sicherheit in dieser Informationstechnik entwickelt sich darüber hinaus zu einer Schlüsselfrage für die Wettbewerbsfähigkeit unserer gesamten Wirtschaft. Denn das erhoffte Wachstum des e-commerce und der IT-Branche ist nur zu realisieren, wenn die Unternehmen Verbraucherbedürfnisse in den Mittelpunkt ihrer Geschäftspolitik stellen. Wenn die Kunden aufgrund von Sicherheitslücken im Internetgeschäftsverkehr das Vertrauen in die Datensicherheit und damit auch das Vertrauen in den Geschäftspartner verlieren, ist eine grundlegende Voraussetzung für die Geschäfts-

beziehung gestört. Betroffene Unternehmen oder sogar ganze Sektoren können neben materiellen Schäden irreparable Imageverluste erleiden.

Unternehmen jeder Größe wie auch private Haushalte müssen sich der Bedeutung des Themas Sicherheit im Internet bewusst werden. Die wachsende Angriffsgefahr aus dem Internet wird allerdings vielfach ignoriert. Bisweilen bremst das Top-Management sogar häufig notwendige Sicherheitsmaßnahmen. Private Nutzer sind sich der Risiken durch unseriöse oder kriminelle Unternehmen, aber auch der quasi legalen Möglichkeiten des Missbrauchs ihrer Daten häufig nicht einmal bewusst.

Vor diesem Hintergrund veranstaltete die Friedrich-Ebert-Stiftung am **17. Juni 2002** in **Hamburg** die Tagung: **„(Un-)Sicherheit im Internet - Wege zu einem besseren Schutz für Unternehmen und private Nutzer**“, auf der Experten aus Wissenschaft, Wirtschaft, Verwaltung, Politik, Daten- und Verbraucherschutz sowie weitere relevante Akteure ihre Positionen darstellten und mit den Teilnehmern diskutierten.

Die Veranstaltung verfolgte zwei Anliegen: Zum einen sollte über die Risiken und Gefahrenpotenziale des Mediums Internet und dessen vielfältige Erscheinungsformen informiert werden. Zum anderen sollte über einen wirksameren Schutz für die Internet-Nutzer beraten und debattiert werden. Dabei wurden bereits bestehende Sicherheitsregelungen und -konzepte politischer, rechtlicher Art sowie technische Schutzmöglichkeiten vorgestellt und bewertet und auf dieser Grundlage der Handlungsbedarf und die Handlungsmöglichkeiten für einen verbesserten Nutzerschutz abgesteckt.

In der vorliegenden Broschüre werden die auf der Konferenz gehaltenen Referate und die Diskussion wiedergegeben. Für Konzeption und Durchführung der Veranstaltung war Diplom-Ökonomin Hannelore Hausmann mit Unterstützung von Diplom-Politologen Oliver Dalichau, für das Sekretariat Margit Durch vom wirtschafts- und sozialpolitischen Forschungs- und Beratungszentrum der Friedrich-Ebert-Stiftung, Abteilung Wirtschaftspolitik, verantwortlich.

Den Tagungsbericht erstellten Dr. Jürgen Malley und Diplom-Biologin Maria Rieping aus Mainz.

Hannelore Hausmann Oktober 2002

Zusammenfassung

„(Un-)Sicherheit im Internet“, so lautet der Titel der Tagung der Friedrich-Ebert-Stiftung, und diese Formulierung spiegelt treffend die Einschätzung der Referenten wider: Es herrscht Einigkeit dahingehend, dass die Nutzung des Internet Risiken mit sich bringt. Bezüglich des Maßes an Unsicherheit und den daraus zu ziehenden Konsequenzen sind die Einschätzungen jedoch breit gefächert.

Folgende wesentliche **Risiken** für private Nutzer und Unternehmen wurden benannt:

- Zerstörung von Daten und Programmen durch Viren, Würmer, Trojanische Pferde bzw. generell durch Hacker-Angriffe
- Verändern von Daten, bspw. Webseiten (sog. Defacement)
- Manipulation der Kommunikation, bspw. durch Missbrauch fremder e-mail-Adressen, Fälschung von Daten bei Überweisungen oder Bestellungen, Missbrauch von Passwörtern
- Abfangen und Ausspähen von Daten zur kriminellen Nutzung (bspw. Wirtschaftsspionage), Anlage von Datensammlungen außerhalb der deutschen Datenschutzgesetzgebung (Data Mining); Veröffentlichung von vertraulichen Daten, Ausspähen sensitiver Daten durch Spyware oder Trojanische Pferde.
- Unfreiwillige Preisgabe von Daten durch die Nutzer der neuen Medien bei nicht sachgerechtem Einsatz technischer Hilfsmittel, bspw. durch den ungeschützten Einsatz drahtloser Funknetzwerke oder zukünftig durch Bluetooth-Systeme
- Missbrauch bei Web-Dialern, der zu immensen Telefonrechungen führen kann
- Dienstverweigerungsangriffe (sog. Denial-of-Service-Attacken, kurz DoS-Attacken), Mailbombing
- Fehlfunktionen, die der nicht auf Sicherheit angelegten, komplexen Internet-Technologie inhärent sind
- Überwachung der Bewegung der Internet-Nutzer im Netz durch legalen Zugriff von interessierten Wirtschaftsunternehmen oder Sicherheitsbehörden

Folgende **Gegenmaßnahmen** wurden diskutiert:

Technische Maßnahmen:

- Schutz vor Dialer-Missbrauch durch Sperrung der 0190-Nummern für den eigenen Anschluss, Internet-Zugang über DSL, Installierung von Dialer-Schutzprogrammen
- Schutz des Rechners durch Anti-Virenprogramme, Firewalls, Intrusion Detection Systeme, Public Key Infrastrukturen (PKI)
- Schutz von Daten durch Anti-Spyware, Web-Filter und Verschlüsselung von sicherheitsbedürftiger Kommunikation
- Erhöhung der Sicherheits-Standards der Provider, auch durch die Einbindung eines Sicherheits-Verantwortlichen in die Betriebsprozesse, Implementierung besonderer Sicherheitsmaßnahmen beim Provider für transportierte und gespeicherte Daten
- Nutzung von Open-Source-Software (OSS) zur Erhöhung der Transparenz von Sicherheitsrisiken
- Aufbau eines neuen Netzes, das im Gegensatz zum offenen Internet spezifisch für sicherheitsbedürftige Kommunikation gestaltet wird

Maßnahmen der Aufklärung und Information:

- Awareness-Kampagne der Bundesregierung zur Sensibilisierung für die Risiken der Internet-Nutzung, Stärkung des „Selbstschutzes“, insbesondere auch für bisher nicht informierte Zielgruppen, bspw. Mittelstand, Information auch über Kosten für Sicherheitsmaßnahmen; in diesem Bereich soll auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine maßgebliche Rolle spielen
- Aufklärung der Kunden über die von ihrem Provider durchgeführten Sicherheitsmaßnahmen
- Information der Verbraucherverbände über Risiken im Netz, insbesondere bzgl. der Dialer-Problematik

- Aufklärung durch Software-Hersteller über die Sicherheitsrisiken ihrer Produkte
- Durchführung von Internet-(Verkehrs-)erziehung

Organisatorische Maßnahmen:

- Einrichtung der Task Force Sicheres Internet unter Federführung des BMI
- Einrichtung von Computer Emergency Response Teams (CERT), bspw. M-CERT für den Mittelstand, welches mit staatlicher Unterstützung realisiert wird.
- Angebot von Security-Beratung und konkreter Unterstützung im Problemfall durch den/ die Provider
- Aufbau eines ISI-PART (Internet Security Incident Prevention and Response Team) seitens der deutschen Internet-Industrie für reaktive Sicherheitsdienste (bspw. Incident Response, Advisory-Dienste, Quick-Fixes, Unterbrechung von DoS bzw. DDos-Attacken) sowie weitere präventive und pro-aktive Dienste (Früherkennungssysteme, regelmäßige Scans, Security-Beratung und -Training, Expertenanalysen, Empfehlungen)
- Einrichtung von „Spielwiesen“ für Hacker, stärkere Einbindung des immensen Know-Hows und Potenzials dieser Gruppe
- Stärkung des Potenzials der Verbraucherverbände zu Abmahnungen; Aufruf zum Zahlungsboykott gegen 0190-Betrüger
- Entwicklung einer Verbraucherschutzkonzeption, die eine bessere finanzielle und kompetenzbezogene Ausstattung der Verbraucherverbände beinhaltet, damit diese erweiterte Aufgaben im Dienste des Verbraucherschutzes bewältigen können
- Einrichtung einer Technikfolgenabschätzungs-Instanz für den Bereich der IuK-Technologien
- Völlige Internet-Abstinenz

Rechtliche Maßnahmen:

- Implementierung von Qualitätsstandards und Regelung von Haftungsfragen (für Soft- und Hardware, Homebanking usw.), um zuverlässigere Produkte zu erhalten
- Einführung einer geschützten Berufsbezeichnung des „IT-Sicherheitsexperten“
- Beweislastumkehr, auch für die Nutzung eines Telefonanschlusses, Inkasso für 0190-Nummern durch die Deutsche Telekom nur in unstrittigen Fällen, ansonsten durch die Mehrwertdienstanbieter selbst, Sanktionierung von „Schwarzen-Dialer-Schafen“, restriktive Nummernvergabe durch Mehrwertdienstanbieter
- Zusammenfassung und Harmonisierung der im Bereich der neuen Medien geltenden Datenschutzregelungen (Telekommunikations-, Teledienste-, Mediendienste- und allgemeines Datenschutzrecht) im Rahmen der Novellierung des Bundesdatenschutzgesetzes
- Einführung einer Evaluation von rechtlichen Regelungen, um so zu vermeiden, dass Gesetze Gültigkeit behalten, die bspw. aufgrund aktueller Bedrohungsszenarien entstanden sind
- Optimierung und Harmonisierung der aktuellen Regelungen mit dem Ziel der Schaffung eines rechtlichen Rahmens, der das Vertrauen der Verbraucher in die neuen Medien stärkt; dies betrifft insbesondere folgende rechtliche Regelungen: Signaturgesetz, Datenschutzgesetzgebung, deutsche Telekommunikations-Überwachungs-Verordnung (TKÜV), Europäische Cyber Crime Convention, Kundenschutzverordnung (TKV), Fernabsatzrichtlinie, e-commerce-Richtlinie bzw. EGG (Elektronischer Geschäftsverkehr-Gesetz). Dabei wurden als Einzelmaßnahmen genannt:
  - Benennung der Regulierungsbehörde als Kontrollinstanz für Anbieterpflichten in der TKV
  - Verpflichtung zu Transparenz (bei strittigen Inkasso-Beträgen)
  - Trennung der Dienstleistungen „Telefonieren“ und „Nutzung der Dienste eines Diensteanbieters“
  - Einführung einer „Mitstörerhaftung“ gemäß Wettbewerbsrecht für alle Beteiligten in der Kette vom Anbieter bis zum Netzbetreiber

Diskussion der Maßnahmen:

Etliche der diskutierten Maßnahmen sind bereits implementiert oder zumindest in Planung. Die meisten der technischen Maßnahmen können individuell, entsprechend dem Wissens- und Bewusstseinsstand des Nutzers, umgesetzt werden, und führen zu einem akzeptablen, jedoch - wie viele präventive Maßnahmen des alltäglichen Lebens - nicht zu einem hundertprozentigem Schutz; gleichzeitig können sie die Kommunikation erheblich unkomfortabler machen.

Für die verantwortliche Nutzung des einzigen bisher vorhandenen World Wide Webs - darin sind sich die meisten Referenten einig - ist es unerlässlich, Grundkenntnisse auch über die wesentlichen Sicherheitsrisiken zu besitzen. Doch dieser Anspruch ist in der betrieblichen wie in der privaten Realität bisher kaum umgesetzt, weshalb es zu massiven Vorfällen mit oft immensen Kosten kommt. Die Bundesregierung setzt hier in Kooperation mit der Internet-Wirtschaft vor allem auf Informationskampagnen.

Eine etwas andere Sichtweise präsentiert die Vertreterin der Verbraucher-Verbände: Auch für Nutzer ohne große Vorkenntnisse müsse das Netz sicher sein. Insbesondere für den privaten Nutzer, der sich nicht auf jeder Ebene des alltäglichen Lebens in komplexe Sachverhalte einarbeiten kann, erscheint diese Forderung einerseits nachvollziehbar, denn sonst droht der Rückzug der Verbraucher aus dem Netz und damit auch das Aus für Endkundengeschäfte (sog. Business to Consumer, kurz „B2C“). Andererseits wird es Illusion bleiben, trotz Implementierung bestmöglicher Sicherheitstechnik, bei dieser hochkomplexen Technologie ein „Nullrisiko“ zu erreichen - weshalb Verbraucherverbände ihre Aufgabe zukünftig auch im „Fit-Machen für das Netz“, bspw. durch Bildungsangebote und Beratung, begreifen sollten.

Die Einbindung der Provider in die Sicherheitskette sowohl durch Verstärkung der eigenen Sicherheitsmaßnahmen, als auch durch verstärkten Sicherheitsservice für die Kunden ist unverzichtbar und führt auch auf dieser Ebene zu einem Qualitätsstandard.

Neben reiner Information über Risiken und technische Hilfsmittel setzen Bundesregierung und Internetwirtschaft seit einiger Zeit auch verstärkt auf organisatorische Maßnahmen, wie den Einsatz verschiedener Teams und Task Forces, die Dienstleistungen zur Vorbeugung, zur Früherkennung und zu schneller Reaktion anbieten und Konzepte erarbeiten bzw. umsetzen sollen. Die Auswirkungen dieser Maßnahmen auf die Praxis im Internet bleiben abzuwarten.

Angemahnt wurde von mehreren Referenten eine grundsätzliche Harmonisierung und Verbesserung der rechtlichen Grundlagen. Dabei wurden einerseits datenschutzrechtliche Bedenken in den Vordergrund gestellt, insbesondere seitens des Hamburger Datenschutzbeauftragten und des Vertreters des Chaos Computer Clubs. Die Implementierung höherer Datenschutzstandards steht jedoch, wie die Vertreter der Bundesregierung betonen, oftmals im Gegensatz zu den Interessen der Strafverfolgungsbehörden, wobei ein Interessensausgleich herbeizuführen sei.

Auf der anderen Seite wurden verbrauchergerechtere Rechtsgrundlagen für das Problem des Dialer-Missbrauchs, für Homebanking und e-commerce gefordert. Den Einzug von Qualitätsstandards in den Bereich der neuen Medien hält der Informatikprofessor Klaus Brunnstein für unerlässlich und - wie im historischen Vergleich mit der technologischen Entwicklung von Eisenbahn und Auto dargestellt - für längerfristig unumgänglich.

Während alle bisher dargestellten Maßnahmen - mit Ausnahme der völligen Abstinenz, die von allen Referenten als Konsequenz der Unsicherheit nicht gewünscht wird - sich auf der Ebene der Optimierung der sicheren Nutzung des heute realen Internets bewegen, empfiehlt Professor Klaus Brunnstein - mit Blick über den Tellerrand - den Aufbau eines neuen, sicheren Netzes, welches parallel zum Internet insbesondere für sicherheitsbedürftige Kommunikation genutzt werden solle.

Seine Einschätzung zu dem Internet inhärenten Sicherheitsrisiken ist dabei grundsätzlich verschieden von derjenigen der Vertreter der Bundesregierung: Die von der Bundesregierung geplante Initiative „Bund Online 2005“ soll dazu führen, dass bereits im Jahre 2005 bis zu 376 Dienstleistungen des Bundes über das Netz abrufbar sind. Dies erfordert auch seitens der Bundesregierung, in Kooperation mit den betreffenden gesellschaftlichen Partnern, massive Anstrengungen zur Erhöhung der Sicherheit im Netz; vorausgesetzt, das Internet kann rein konstruktiv genügend Sicherheit für diese Dienstleistungen bieten. Die Bundesregierung hat sich für den Umstieg auf Open-Source-Software entschieden - eine umstrittene Entscheidung, deren grundsätzliche Wirksamkeit von einigen Experten verneint, von anderen wie dem Sprecher des Chaos Computer Clubs jedoch auch bejaht wird.

1. Unternehmen im Visier von konkurrierenden Firmen und Hackern

1.1. Risikofaktoren für Unternehmen im Inter- und Intranet: Gefährdungspotenziale, Erscheinungsformen, Erkennungs- und Zugriffsmöglichkeiten

Prof. Dr. rer. nat. Dipl.- Phys. Klaus Brunnstein
Universität Hamburg, Fachbereich Informatik

Mein Vortrag ist in drei Abschnitte gegliedert: Er beginnt mit den durch das Internet geweckten Erwartungen, beschreibt dann die Realität und schließt mit einem Ausblick.

Erwartungen, die durch den breiten Zugang zum Internet geweckt worden sind:

Die Erwartungen, die diese von Anbietern strukturierte Technologie - denn nicht die Verbraucher, sondern die Anbieter bestimmen die Produkte und deren Bewertung - bei jungen Leuten, bei den Medien und auch bei Politikern geweckt hat, sind mit positiven Begriffen besetzt, wie etwa:

- Aufbau neuer, globaler Wissensspeicher;
- Einstieg in eine Wissens- oder zumindest in eine Informationsgesellschaft, in der Verfahren zur Informationsverarbeitung Produktionscharakter analog zur industriellen Revolution erhalten;
- Weltweites Wirtschaften, bspw. e-banking und e-commerce und neuerdings m-commerce (die mobile Variante mittels Handy oder Personal Digital Assistant (PDA));
- Ökologisch sinnvollere Gestaltung des Arbeitsplatzes: Von zu Hause aus arbeiten und so den Verkehr zum Arbeitsplatz vermeiden;
- Besseres Lernen mittels der potenziell besten Lehrer und Professoren im Internet;
- Nutzung der besten Ärzte durch Beratung bspw. an der Mayo-Klinik statt in unserem regionalen Krankenhaus;

- Optimierung von Abstimmungsprozessen: Wir können uns - statt nur alle vier oder fünf Jahre - im Prinzip an jeder Abstimmung beteiligen, weil ein überlegenes Informations- und Wissenspotential im Internet für unsere eigenen politischen Entscheidungen vorliegt.

All diese Erwartungen wage ich in Zweifel zu ziehen.

Die Realität:

Wir befinden uns mitten in einer Entwicklung, in der die Beziehungen geschäftlicher, organisatorischer und auch persönlicher Art immer mehr auf elektronische Grundlagen gestellt werden, wie zum Beispiel:

- B2B: Business to Business, d.h. der elektronische Kontakt zwischen Unternehmen. Er wird auf vielfältige Art genutzt, bspw. um Vorstufenprodukte mit Produzenten auszutauschen;

- B2C: Business to Consumer, d.h. der elektronische Kontakt zwischen Unternehmen und Kunden. Er ist noch nicht so stark entwickelt, da die Risiken derzeit erheblich sind. Die Bundesregierung versucht „public key infrastructures“ gegen die große Skepsis der Bevölkerung durchzusetzen. Diese Skepsis ist berechtigt, weil zu viele Vorfälle aufgetreten sind und weil wir bei diesem Verfahren noch nicht wissen, wie wir zum Beispiel „keys“, also Schlüssel, zurückholen können; dafür gibt es noch keine technische Methode.

- Electronic voting: Die Frage des „electronic voting“ wird in der Zukunft relevant: Dieses Verfahren wird in einigen europäischen Ländern, auch in der Bundesrepublik, erwogen oder teilweise auch praktiziert. Beim „electronic voting“ spielen zwei konträre Aspekte eine Rolle, nämlich einerseits die Authentizität des Wählers, also die Garantie, dass es sich genau um einen speziellen Wähler handelt und andererseits die absolute Sicherheit, dass die Stimme anonym abgegeben wird.

- Weitere Beziehungen: Es gibt eine ganze Reihe von elektronischen Beziehungen, die noch nicht sehr weit entwickelt sind, wie „health to health“ und „business to government“; letztere entwickelt sich gerade. Es wurden in letzter Zeit rechtliche Regelungen verabschiedet, die vorsehen, dass bspw. Bilanzen und Detailinformationen über Steueraspekte bei Unternehmen gespeichert und seitens der Steuerbehörden elektronisch zugreifbar sein sollen. Der Zugriff erfolgt derzeit vor allem noch lokal, indem der Steuerprüfer mit seinem Laptop in den Betrieb geht, soll in naher Zukunft jedoch hauptsächlich via Internet möglich sein.

Wir gestalten auf diese Weise die bisher durch persönliche Beziehungen - wie das persönliche Erscheinen auf einem Amt oder in einem Unternehmen - geprägte und damit von uns persönlich als sicher angesehene Kommunikation um. Einen weiteren Schritt auf diesem Weg stellt der Einsatz mobiler Technik dar: „Ubiquitous Computing“ geht über die aktuellen lokalen und globalen Netze weit hinaus, indem bestimmte Mikroprozessoren, aber auch das Handy oder der Personal Digital Assistant, an die Netze angeschlossen werden, um dort Informationen zu speichern, zu verarbeiten und abzurufen. Mein Lieblingsbeispiel, das auf den ersten Blick nichts mit Sicherheit im engeren Sinne, aber mit Verfügbarkeit zu tun hat, habe ich kürzlich auf einem Seminar von Daimler-Chrysler diskutiert:

Sie haben Feierabend, gehen zu Ihrem Auto, um nach Hause zu fahren, und während Sie das Auto mit Ihrem elektronischen transactor aufschließen, meldet Ihr persönliches Informationssystem: „Wir haben heute Abend eine Party, bitte verbinde mich mit Deinem household management system, um festzustellen, ob wir noch genug Würstchen und Getränke zu Hause haben.“ Das household management system stellt fest, dass Würstchen und Rotwein fehlen und meldet dem car management system, dass es den schnellsten Weg zum Weinhaus suchen soll. Das car management informiert über den schnellsten Weg und berücksichtigt dabei Staus und Umleitung wegen Bauarbeiten.

Das nennt man „ubiquitous computing“. Teilweise werden Mikroprozessoren eingesetzt, die Sie am Körper tragen - wir sprechen von „ware wear“ - zum Beispiel ein Transponder: Sie nähern sich Ihrem Auto, brauchen nicht den üblichen Schlüssel, um aufzuschließen, sondern werden erkannt; die Tür öffnet sich, die Maschine wird

gestartet, die Klimaanlage vorgekühlt und im Übrigen meldet Ihr Kühlschrank, dass Sie neue Milch brauchen. Alle diese Szenarien sind Entwürfe der Industrie, über deren Wirkungen wir uns folgendermaßen im Klaren sein müssen:

Derzeit nutzen 350 bis 400 Millionen Menschen das Internet: Ein Zustand, den ich heute schon nicht als unbedenklich, sondern eher als riskant einschätze. Wenn Handys, PDA und etliche Mikroprozessoren dazukommen, dann steigt die Nutzerzahl leicht auf über eine Milliarde und mehr. Diese zu erwartende Entwicklung erfordert dringend die Überlegung, ob die verwendeten Techniken inhärent sicher sind.

Und nun muss ich Ihnen einen Schock versetzen: Die Systeme sind nicht beherrschbar, und zwar aus einem ganz einfachen Grund, den man als Informatiker den Politikern offenbar nur sehr schwer klarmachen kann: sie sind zu komplex, als dass irgend jemand, inklusive meiner Person als Experte in Unfall- und Vorfallanalyse, sie nachvollziehen kann. Heutige Computersysteme sind im Groben in verschiedenen Schichten gebaut: oben die Anwendungsschicht, in denen Ihre Textverarbeitungs- und Wirtschaftsprogramme ablaufen, darunter die Betriebssystemschicht und darunter die Hardwareebene. Bei der Dicke an Instruktionsmengen und Datenmengen in den jeweiligen Schichten, ist klar, dass dort nur Datennebel herrscht. Wir können letztlich nicht nachvollziehen, was in einer solchen Maschine mit heute 2 Milliarden Instruktionen pro Sekunde abläuft. Wir können in diesen Kategorien nicht denken. Wenn die Maschine „lade“, „speichere“, „addiere“, „subtrahiere“, „maskiere“ oder „springe“ sagt, dann kann in den Schichten darunter etwas ganz anderes, möglicherweise das Gegenteilige geschehen. In dieser Schichtung sind beliebige Angriffe auf die sehr nützlichen Funktionen möglich und einige von Ihnen werden das auch beim „I-love-you-Virus“ schon selbst erlebt haben. Diese Komplexität, die auch von den Fachleuten nur bei Erwartung eines Vorfalls beherrschbar ist, führt dazu, dass in allen Schichten des Systems Fehlfunktionen, Hintertüren, Viren, Würme und Trojanische Pferde lauern können.

Entgegen der Hoffnung der Bundesregierung ist es auch bei Linux sehr einfach, Viren und Würmer zu schreiben; doch es gibt bisher lediglich fünf Prozent Linux-Nutzer, so dass die Anzahl der Angreifer noch weitaus geringer als bei Microsoft ist.

Noch viel einfacher ist es übrigens, Handy-Viren und Handy-Würmer für die nächste Generation der UMTS-Handys zu schreiben.

Es gibt also eine Vielzahl an leider inhärenten Risiken, die daher resultieren, dass wir eine Technologie verwenden, die nicht auf Sicherheit getrimmt ist. Es ist, als ob man ein Auto kaufen würde, bei dem die Bremse nicht eingebaut ist. Als man feststellt, das man diese braucht, empfehlen die Hersteller, ein Loch ins Blech zu sägen und mittels eines Bleischuhs zu bremsen. So wird versucht, mangelhafte Sicherheit durch eigentlich sachfremde Aktionen der Verbraucher zu kompensieren. Besonders gut lässt sich dieser Aspekt am Internet aufzeigen.

Das Internet ist eine vorzügliche Einrichtung für die freie Kommunikation. Sie ist in den USA unter dem Aspekt implementiert worden, dass man in den sechziger Jahren Angst vor dem nuklear-elektromagnetischen Impuls hatte. Das ist eine Technik, bei der bspw. eine Neutronenbombe in hundert Kilometer Höhe gezündet wird und dabei sämtliche Magnetisierung der aktuellen und der gespeicherten Daten in den Rechnern und auf den Datenspeichern in einem Umfeld von etwa 150 bis 300 Kilometern löscht. Um die Daten zu retten, etwa die der großen Marinebasen-Rechner in Norfolk, Virginia, hat man die Wissenschaft damals mit Mitteln des amerikanischen Verteidigungsministeriums aufgefordert, ein Netz zu entwickeln, mittels dessen man die Daten beispielsweise nach Neuseeland oder Südamerika exportieren kann. Infolgedessen wurde der Aspekt dessen, was wir heute „mirroring“, Spiegelung nennen, in das Netz hinein gebracht. Die Geheimhaltung der Daten wurde jedoch interessanterweise von den Militärs offenbar nicht bedacht.

Infolge dessen ist das Internet für freie Kommunikation ohne jeden Schutzanspruch genial; die Hochschulen haben es exzellent implementiert. Doch wer dieses Netz für sicherheitsbedürftige Kommunikation in Unternehmen, nutzt, etwa für fälschungssichere e-mails, abhörsichere Kommunikation, authentizitätsbedürftige Kommunikation, der ist für die Konsequenzen selber verantwortlich. Das Internet ist eine Umsetzung dessen, was man in den USA „freedom of information“ nennen würde, aber keinesfalls geeignet für sicherheitsbedürftige Kommunikation.

So ist es beispielsweise beliebig einfach, eine Adresse zu fälschen. Sie können niemals sicher sein, dass eine e-mail wirklich vom genannten Absender kommt. Eine große Klasse von Viren hat sich jüngst dieser Tatsache bedient, als geheime Dokumente aus Unternehmen entwendet und unter falschem Absender ins Internet gesandt wurden.

Ein anderer Aspekt ist, dass Ihre Nachrichten im Internet mittels Missbrauch der Monitoring-Funktion an beliebiger Stelle abgefangen werden können - das nennt man „sniffing"- und dann kann man diese Nachrichten auch „hijacken". Auf diese Weise kann man beispielsweise auch eine Überweisung abfangen und fälschen; es stehen dazu eine Reihe von tools im Internet bereit.

Darüber hinaus stecken - wie Nutzer aus eigener Erfahrung wissen - in der Tiefe dieser Netze eine ganze Menge von Viren, Würmern und trojanischen Pferden. Für staatliches und wirtschaftliches Handeln stellen insbesondere die Dienstverweigerungsangriffe, die beliebig leicht in die Netze eingestellt werden können, ein Problem dar. Die Software für diese Angriffe lässt sich im Internet mit entsprechenden Bedienungskursen laden. Im Februar 2000 führte der Angriff auf „amazon" und „yahoo" zu einer großen Öffentlichkeit. Auch heute geschehen diese Angriffe regelmäßig, aber sie werden nicht mehr bekannt, denn die Unternehmen haben kein Interesse daran. Die Regierungen verschließen vor dieser von allen Experten als zur Zeit nicht heilbar angesehenen Schwäche der Internet-Protokolle in aller Regel die Ohren.

Ein weiterer Aspekt zum Thema Viren: Es gibt Schlüsselviren, die die Schlüsselringe Ihrer Datenverschlüsselung entfernen, bspw. der Virus Caligula. Es gibt eine Reihe von Mechanismen, die beobachten, wie Sie Ihre pass phrase oder TAN eingeben, diese abfangen und angreifen. Zur Zeit existieren 60.000 bis 80.000 Viren und Trojaner in unseren Datenbanken. Die Universität Hamburg hat weltweit die einzige Universitätsgruppe, die dieses analysiert. Wir analysieren auch die Qualitäten der Software, die Viren und Trojaner erkennt, und auch sie ist - trotz erkennbarer Anstrengungen der Hersteller - verbesserungsbedürftig.

Inzwischen ist es so, dass die normale e-mail immer stärker mit Viren belastet wird. Im Dezember 2001 hatten wir mit dem „Goner-Virus“, der in der Öffentlichkeit kaum beachtet wurde, eine ähnliche hohe Belastung aller Firmen wie beim „I-love-you-Virus“: In jeder dreißigsten e-mail befand sich ein solcher Virus. Wenn Sie bedenken, dass die Anzahl der Viren weiter zunimmt, ist im Jahr 2004 ein Virus pro zehn e-mails zu erwarten - und dies bei zunehmender Anzahl von eingehenden mails. Dies wird zu einem massiven Problem führen.

Was kann man tun, um sich zu schützen?

Den Rechner in den „Tower of London“ packen, ihn mit Kryptopaketen, Anti-Viren- und Anti-Malware, Firewalls und Intrusion Detection umgeben und Verbindungen über virtual private networks aufbauen? Damit bewegen Sie sich leider auf der falschen Ebene, denn alle diese Sicherheitsmaßnahmen sind unterlaufbar. Um die ohnehin für uns schon zu komplexe Software packen wir immer weitere komplexe Software - das kann nicht die Lösung des Problems sein. Dennoch ist es für die nächste Zeit ein Behelf, da die Systeme heute so unübersichtlich konstruiert sind.

Die Lösung kann nur darin liegen, zu dem unsicheren Netz Internet, welches für die freie Kommunikation von nicht schutzbedürftigen Inhalten ohne jede Konkurrenz und ohne Zweifel extrem wertvoll und bewahrenswert ist, ein weiteres Netz zu kreieren. Dieses Netz darf nicht versuchen, die heutigen unsicheren Netze mittels Kryptoverfahren o.ä. mit einzubinden, sondern muss auf der Protokollebene Sicherheit herstellen. Ein Beispiel: Wenn Sie einen elektronischen Vertrag mit Ihrer Bank oder einem Händler aufbauen wollen, müssen zwei Bedingungen erfüllt sein: Der Händler muss Sie auf jeden Fall annehmen, wenn ein Kontakt zwischen Ihnen besteht und der Kunde darf die Order nicht zurücknehmen[1]. Diese beiden Parameter müssen in die Protokolle aufgenommen werden. Wann darf man damit rechnen?

Nach der Erfahrung der Industriegesellschaft braucht es rund achtzig Jahre, nämlich rund zwei Kondratieff-Zyklen, um Qualitätsstandards zu implementieren, die einem vorsorgenden Verbraucherschutz, bspw. mittels Schadensersatz und Rückrufaktionen, in etwa gerecht werden:

[1] Sog. „Non-deniability“ und „Non-repulliation“

- Von der Erfindung der „doppelt wirkenden Niederdruck-Dampfmaschine“ von James Watt im Jahr 1761 dauerte es noch etwa achtzig Jahre, bis der Dampfkesselüberwachungsverein, aus dem sich später der TÜV entwickelte, gegründet wurde.
- Zwischen der Erfindung des Autos und der als Meilenstein einer veränderten Wahrnehmung geltenden Doktorarbeit von Ralph Nader mit dem Titel „Unsafe at any speed“ vergingen ebenfalls rund achtzig Jahre.

Setzen wir den Beginn der Informationsgesellschaft um 1941, als Konrad Zuse die Z3 erfand, würde ein entsprechendes Qualitätsniveau um das Jahr 2021 zu erwarten sein. Wir können nur hoffen, dass bis dahin die Verbraucher so zornig werden, dass die Hersteller bessere Systeme konzipieren.

1.2. Sicherheits- und Risikofaktor Provider?

Stefan Kratzer
Security Consultant der eco Electronic Commerce Forum e.V., Köln

Provider-Dienstleistungen

Provider ermöglichen Unternehmen, Organisationen und Privatkunden den Zugang zum Internet bzw. den Internet-basierten Datentransport. Angebote fast aller Provider sind:

- Internet-Access (weltweite Kommunikationsverbindung),
- Internet als Transportnetz (z.B. Festverbindungsersatz, IP-basiertes Virtual Private Network VPN),
- Hosting-Dienste: Server-Stellplatz (Strom und Netzzugang) bis zum kompletten Betrieb von Web-Servern durch den Provider sowie
- Mail- und Domainnamen-Services.

Die Nutzer erwarten von Internet-Providern in erster Linie den schnellen, kostengünstigen und zuverlässigen Datentransport von und zu ihren angeschlossenen Computern.

Gleichzeitig sind technische und organisatorische Maßnahmen zu ergreifen, um Gefahren (z.B. Hackerangriffe auf angeschlossene Systeme, Viren oder Ausspähen sensitiver Daten), die sich aus dieser globalen Kommunikation ergeben, möglichst gering zu halten.

Security Herausforderungen

Bei der Forderung nach wirksameren Schutzmaßnahmen sollten jedoch auch folgende Aspekte berücksichtigt werden:

- Der Wunsch nach globaler (und schneller) Kommunikation und hohe Sicherheitsanforderungen sind zunächst einmal gegenläufige Ziele. So können Firewall-Regelsätze (wenn z.B. ein Geschäftspartner kurzfristig über das Internet auf Daten im geschützten LAN zugreifen will) oder Virenfilter (wenn z.B. ein wichtiges geschäftliches Dokument in einer e-mail zufällig dem Muster eines Virus entspricht) auch gewünschte Kommunikationsbeziehungen behindern.

- Beim Datentransport hat der Provider keine Kenntnis über Inhalt und i.d.R. (außer IP-Adressen) über Absender bzw. Empfänger der zu transportierenden Daten. Bestimmungen des Datenschutzes und Verschlüsselungsmechanismen schränken die Möglichkeiten der Inhaltskontrolle weiter ein.

- Im Internet werden gewaltige Datenmengen transportiert, die in kleine Pakete von „0“ und „1“ zerteilt werden. Erst durch Zusammensetzen entsteht wieder für den Menschen interpretierbare Information, wodurch eine Unterscheidung erwünschter von unerwünschter Kommunikation nahezu unmöglich ist. Ist bspw. der plötzliche Anstieg des Verkehrsaufkommens eines e-commerce-Servers auf eine erfolgreiche Werbemaßnahme, eine Fehlfunktion des Endsystems oder auf einen Denial-of-Service-Angriff (DoS Attacke) zurück zu führen?

Teilweise besteht noch Unklarheit darüber, welche Sicherheitsprobleme in die Verantwortung des Providers bzw. des Internet-Nutzers fallen. Bevor kaum finanzierbare Maßnahmen gefordert bzw. falsch adressiert werden, sollten die Möglichkeiten in den folgenden Bereichen ausgeschöpft werden.

Verantwortung der Provider

Ein Provider ist in erster Linie verantwortlich für die Sicherheit seiner eigenen Infrastruktur. Aktive Netzkomponenten wie z.B. Router und zentrale Server müssen unter Berücksichtigung von Security-Anforderungen ausgewählt, konfiguriert und betrieben werden. Hierzu kann es sinnvoll sein, einen Security-Verantwortlichen in die Betriebsprozesse einzubinden. Provider müssen besonderes Augenmerk auf den Schutz sensitiver Daten legen, die auf ihren Systemen nicht nur (weiter-)transportiert sondern gespeichert werden (z.B. Kundendatenbanken, Accounting-Daten). Provider sollten Kunden hinsichtlich sicherheitsrelevanter Aspekte ihrer Dienste aufklären und beraten können. Zusatzangebote wie Security-Workshops oder Audits verhindern den Anschluss leicht angreifbarer Systeme ans Internet. Unterstützungsleistungen bei einem Security-Vorfall mindern die Folgen eines Angriffs.

Kosten für Sicherheitsmaßnahmen steigen um so stärker an, je mehr Sicherheit erzielt werden soll. Andererseits planen Anbieter und Kunden – insbesondere in Zeiten wirtschaftlicher Schwächen – häufig nur geringe Budgets für Sicherheitsmaßnahmen ein. Deshalb ist es erforderlich, übergreifende (öffentlich geförderte?) Maßnahmen einzuleiten.

Übergreifende Maßnahmen

Unter Federführung des eco Electronic Commerce Forum e.V. plant die deutsche Internet-Industrie den Aufbau eines sog. „Internet Security Incident Prevention and Response Teams“ (ISI-PART). Aufgaben sollen neben reaktiven Security-Services (Incident Response, Advisory-Dienste, Quick-Fixes, Unterbrechung von DoS- bzw.Ddos Attacken etc.) insbesondere präventive bzw. pro-aktive Dienste sein: Früherkennungssysteme, regelmäßige Scans, Security-Beratung und -Training, Expertenanalysen und Empfehlungen in Kooperation mit Herstellern von Internet Hard-

und Software, anderen CERTs und ggf. Bedarfsträgern geben dem Internet eine neue Qualität an Sicherheit.

Das Internet ist zu einem wesentlichen Wirtschaftsfaktor geworden. Es birgt neben vielen Vorteilen auch Risiken. Provider ermöglichen zwar den Zugang zum Internet, jedoch sind sie nicht verantwortlich für die Daten, die über das Internet transportiert werden.

Maßnahmen zur Erhöhung der Sicherheit im Internet müssen sich an technischen und wirtschaftlichen Faktoren orientieren. Nur das kooperative Zusammenspiel von Providern, Nutzern und öffentlichen Interessen kann langfristig das Internet als Kommunikationsmedium sichern.

1.3. Forderungen an Politik und Gesetzgebung

Peter Schaar
Stellvertretender Datenschutzbeauftragter der Freien Hansestadt Hamburg

Über die Sicherheit den Datenschutz nicht vergessen

Bereits heute ist Deutschland in der Liga der demokratischen Staaten Weltmeister der Telekommunikations-Überwachung. In der Diskussion über Sicherheitsgefahren und Kriminalität im Internet sind erhebliche zusätzliche Befugnisse eingeführt worden (z.B. die Ausweitung von Überwachungsbefugnissen im Rahmen der Anti-Terrormaßnahmen). Weitere Befugnisse werden gefordert (z.B. der Vorschlag des Bundeswirtschaftsministeriums zur Identifikationspflicht in der Telekommunikation, mit Zugriff der Sicherheitsbehörden auf die Daten). Andere mögliche Maßnahmen z. B. zur Erhöhung der technischen Sicherheit bleiben dagegen ungenutzt. So werden beispielsweise immer noch 99 Prozent aller e-mails unverschlüsselt übertragen.

Die Unschuldsvermutung gilt auch im Cyberspace

Bei allen Maßnahmen muss bedacht werden, dass die große Mehrzahl der Internetbenutzer sich rechtskonform verhält. Forderungen zur Einführung von Mindestspeicherfristen für Bestandsdaten[2] und Verbindungsdaten (gemäß Bundesrats-Beschluss im Rahmen eines Gesetzes zur Bekämpfung des Missbrauchs von Kindern und Jugendlichen) führen dazu, dass jede Nutzung des Internets bleibende auswertbare persönliche Spuren hinterlässt. Derartige Vorgaben sind unverhältnismäßig und stoßen bereits aus diesem Grund auf verfassungsrechtliche Bedenken.

Datenschutzrecht auf hohem Niveau vereinheitlichen

Gerade im Bereich der neuen Medien und des Internet ist der datenschutzrechtliche Rahmen nur für Fachleute verständlich. Sowohl das Telekommunikations-, das Teledienste- und Mediendiensterecht als auch das allgemeine Datenschutzrecht kommen zur Anwendung. Die Gesetze enthalten zum Teil inkompatible Regelungen. Dies führt zu erheblichen Rechtsunsicherheiten und trägt zu einem Vollzugsdefizit bei. Bei der zweiten Stufe der Novellierung des BDSG sollten die unterschiedlichen Regelungen zu einem konsistenten System zusammengeführt werden.

Marktwirtschaftlichen Mechanismen stärken

Ein wirksamer Datenschutz im Internet entsteht erst dann, wenn die Akteure selbst ein Interesse an der Gewährleistung eines hohen Datenschutzniveaus entwickeln. Datenschutz muss zu einem Verkaufsargument werden. Die Verankerung des Datenschutz-Audits in § 9a BDSG bleibt ein theoretisches Konstrukt, solange es kein Umsetzungsgesetz gibt. Der Gesetzgeber ist aufgefordert, die Arbeiten an einem Datenschutz-Audit-Gesetz zu beschleunigen.

[2] Vorlage des BMWi zur Äderung von § 90 TKG

1.4. Maßnahmen der Bundesregierung für mehr Sicherheit im Netz aus Sicht des Wirtschaftsministeriums

Dr. Ulrich Sandl
Referatsleiter IT-Sicherheit, Bundesministerium für Wirtschaft und Technologie, Berlin

Mein Beitrag wird keinen Überblick über die Maßnahmen der Bundesregierung im Einzelnen bieten. Ich möchte Ihnen vielmehr Einblick in die Handlungszwänge, Problembereiche und Spannungsfelder geben, in denen wir uns in diesem Bereich fast täglich bewegen müssen; ich tue dies auch in der Hoffnung, dass dadurch die eine oder andere Bemerkung der Vorredner erklärt wird.

Handlungszwang Nr. 1 ist das e-commerce-Dilemma: Wir erleben ein gewaltiges Ansteigen der wirtschaftlichen Nutzung des Internet; ein Wachstum, wie es bei technischen Entwicklungen bisher noch nie beobachtet werden konnte. Diese Entwicklung ist zu begrüßen, denn sie ist für die Entwicklung unseres Wirtschaftsstandorts und für die Steigerung der Wettbewerbsfähigkeit unserer Unternehmen notwendig. Deshalb gibt es zur Nutzung des Internet derzeit keine Alternative.

Auf der anderen Seite erleben wir gerade aufgrund dieser rasanten Steigerungsrate eine ebenso rasante Steigerung der Angriffe auf das Internet und im Internet. Mir liegt eine Statistik eines CERT vor, die aufzeigt, dass vom Jahr 2000 zum Jahr 2001 eine Verdopplung der Angriffe im Internet stattfand - ich finde, das ist eine beachtliche Rate. Doch gerade durch diese Angriffe steigt auch die Bereitschaft, sich mit dem Internet näher zu befassen. Wenn Professor Brunnstein fordert, aufgrund der Komplexität der Materie besser die Finger vom Internet zu lassen, dann stellt er gerade aus wirtschaftspolitischer Sicht eine gefährliche Forderung, denn wir brauchen das Internet, um unsere Wettbewerbsfähigkeit und unsere Wirtschaftskraft zu erhalten - und letztlich geht es um den Erhalt von Arbeitsplätzen!

Ich habe kürzlich an einem sehr interessanten Vortrag eines Kollegen des IT-Verbandes Bitcom teilgenommen, der die gleiche Entwicklung am Beispiel des Straßenverkehrs nachgezeichnet hat. Der Referent stellte fest, dass auch der Straßen-

verkehr zugenommen, die Anzahl der Unfälle jedoch abgenommen hat - und man könnte überlegen, inwieweit diese Entwicklung auf das Internet übertragbar ist.

Handlungszwang Nr. 2 liegt in den wachsenden Abhängigkeiten. Ich habe Übersichten gesehen, aus denen hervorgeht, dass inzwischen 60 Prozent der mittelständischen Unternehmen vom Funktionieren des Netzes abhängig sind. Man denke daran, wie hilflos wir sind, wenn unser e-mail-account plötzlich abstürzt. Die Abhängigkeiten steigen also, und damit auch die Schäden, die auftreten, wenn wirklich etwas passiert. 1988 trat der erste Virus, der Morris-Wurm, der sich unkontrolliert vermehrte, auf. Dieser Wurm verursachte damals einen Schaden in zweistelliger Millionenhöhe. Der Schaden, den der „I-Love-you“-Virus verursacht hat, gehört noch in eine ganz andere Kategorie. Hier bestehen also auch für die Bundesregierung ganz erhebliche Handlungszwänge, weil einerseits unsere Wirtschaftskraft, unsere wirtschaftliche Leistungsfähigkeit auf dem Spiel steht, und weil dies auf der anderen Seite unmittelbar mit der Sicherheitslage zusammenhängt.

Das dritte Problemfeld eröffnet sich - und hier wird es wirklich kritisch - bei den Maßnahmen, die wir ergreifen müssen. Hier stoßen folgende Interessen aufeinander: die Nutzerinteressen, die Herstellerinteressen und die Interessen der Strafverfolgungsbehörden. Ich bin ein Veteran der sogenannten Krypto-Diskussion, aus der wir viel gelernt haben, insbesondere über das Verhältnis von Strafverfolger- und Nutzerinteressen. Es ist ein täglicher Balanceakt, den wir ausüben müssen, denn es ist wirklich wichtig, zwischen diesen Interessen abzuwägen. Manchmal beneide ich manche der Kollegen für den Luxus einer etwas puristischeren Sichtweise, denn die Bundesregierung ist verpflichtet, die verschiedenen Interessen zu berücksichtigen.

Lassen Sie mich zum Schluss noch auf drei Handlungsfelder zu sprechen kommen, die aus wirtschaftspolitischer Sicht sehr wichtig sind, wenn wir wirklich Sicherheit im Internet verwirklichen wollen:

Das erste Handlungsfeld ist die Bewusstseinsbildung, die Sensibilisierung: Die Entwicklung geht furchtbar schnell vonstatten und manch einer ist überfordert mit dem, was um ihn herum passiert. Wir bemerken immer wieder, dass gerade im mittelständischen Bereich große Defizite bei der Sicherheitsproblematik bestehen. Jeder weiß,

wie wichtig es ist, ins Internet zu gehen, aber über die Risiken spricht keiner. Also sind wir als Bundesregierung gehalten, gerade in diesem Bereich eine „Awareness"-Kampagne zu starten, was wir auch derzeit tun, damit wir genau dieses Bewusstsein bei den Mittelständlern schaffen. In diesem Zusammenhang bauen wir zur Zeit auch CERT-Strukturen auf.

Das zweite Handlungsfeld ist die Steuerung der Transparenz von sicherheitstechnischen Prozessen. Nach meiner Erfahrung ist nicht jedes Sicherheitsprodukt vertrauenswürdig. In diesem Bereich kommt auch die sogenannte „open-source-Debatte" wieder zur Geltung. Die Bundesregierung hat eine etwas andere Einstellung als Herr Professor Brunnstein, denn es geht nicht nur darum, ob ein Virus für bestimmte Betriebssysteme entwickelt werden kann. Uns geht es darum, dass Transparenz herrscht und dass man wirklich beurteilen kann, wo letztendlich Sicherheit kreiert werden kann.

Der dritte Bereich, der möglicherweise nicht in dieser, doch in der nächsten Legislaturperiode an Bedeutung gewinnen wird, ist die Gesetzgebung. Es beginnt eine Debatte, in der gefragt wird, ob nicht auch die Haftungsregeln der aktuellen Entwicklung angepasst werden müssen. Diese Debatte läuft bereits in den USA, wo gefragt wird, ob, sofern durch den Fehler eines Software-Produktes ein Schaden verursacht wird, dann nicht der Hersteller haften muss. Auch die Umkehr der Beweislast wird diskutiert.

Unabhängig davon, wie die nächsten Bundestagswahlen ausgehen - auch die CDU hat diesen Punkt in ihr Wahlprogramm aufgenommen – wird die Debatte über die Haftung wahrscheinlich in der nächsten Legislaturperiode beginnen. Momentan setzen wir natürlich lieber auf marktwirtschaftliche Mechanismen:

- Bei der Transparenz-Richtlinie sind Manager gehalten, sofern sie selber nicht in die Haftung genommen werden wollen, sich mehr um die Sicherheit zu kümmern.
- Im Versicherungsbereich variieren Versicherungsprämien danach, wie gut IT-Sicherheit implementiert ist; auch das ist ein marktwirtschaftlicher Anreiz.
- Im Bankenbereich wird die Kreditvergabe auch davon abhängig gemacht wird, wie gut die vom Unternehmer vorgelegten Sicherheitskonzepte sind.

1.5. Maßnahmen der Bundesregierung für mehr Sicherheit im Internet aus Sicht des Innenminsteriums

Christoph Verenkotte
Referatsleiter IT 3, Sicherheit in der Informationstechnik, Bundesministerium des Inneren (BMI), Berlin

Ich darf meine folgenden Ausführungen in drei Teile gliedern:

1) Die Rolle und Funktion des BMI im Rahmen der Debatte zu Sicherheit im Internet
2) Ein kurzer Exkurs zu den Maßnahmen der Bundesregierung insgesamt - denn in Bezug auf Maßnahmen für Sicherheit im Internet steht das BMI ja nicht allein
3) Der Versuch eines vorsichtigen Ausblicks

Rolle und Funktion des BMI im Rahmen der Debatte zu Sicherheit im Internet:

Das BMI ist auf Bundesebene dasjenige Ministerium, das für die innere Sicherheit in Deutschland zuständig ist. Auch vor dem Hintergrund der fortwährenden und in allen Politikbereichen intensiv geführten Bund-Länder-Diskussion ist es dennoch in der Bevölkerung keine Frage, dass man gerade an das Bundesministerium des Innern die Erwartung richtet, Sicherheit zu vermitteln. So gibt es auch beim Thema Internetsicherheit eine erhebliche Erwartungshaltung, die sich speziell am BMI fest macht. Wir müssen uns dieser Erwartungshaltung stellen, obwohl wir nur in bestimmten Bereichen Verantwortung übernehmen können.

Für das BMI sind folgende Aspekte beim Thema „Sicherheit im Internet“ von herausragender Bedeutung:

- Kriminalität im Internet und deren Bekämpfung
- Kritische Infrastrukturen (nach dem 11.September muss man dazu wohl nicht mehr allzu viel erläutern)

Natürlich kann das BMI nicht der genannten Erwartung entsprechen, Garant für eine umfassende Sicherheit im Internet zu sein.

Gleichwohl möchte ich darauf hinweisen, dass sich die Bundesregierung insgesamt und auch der Innenminister federführend in Zugzwang gesetzt haben: Man kann nicht e-Government promoten, ohne etwas für die Sicherheit im Netz zu tun. Wenn der Bundesinnenminister und die Bundesregierung insgesamt planen, bis zu 376 Dienstleistungen bis zum Jahre 2005 in der Initiative „bund online 2005“ verfügbar und für den einzelnen Bürger über das Netz abrufbar zu machen, dann sind wir gewissermaßen in einer Garantenpflicht, dass dies durch sichere Wege funktioniert.

Darüber hinaus ergeben sich einige weitere Verantwortlichkeiten, wie zum Beispiel diejenige für Hochsicherheitsnetze oder für besondere Sicherheitsvoraussetzungen zur sicheren Regierungskommunikation, auf die ich aber jetzt nicht im Detail eingehen möchte.

Kurzer Exkurs zu den Maßnahmen der Bundesregierung insgesamt

- Weiterentwicklung des BSI (Bundesamt für Sicherheit in der Informationstechnik) zum Sicherheitsdienstleister: Wir bemühen uns seit einiger Zeit und mit großer Anstrengung, das BSI zu einem Sicherheitsdienstleister in der Breite zu entwickeln. Dafür haben wir Einiges getan: Das BSI ist nicht bloß ein Dienstleister für die Regierung selbst, sondern wir wollen, dass der dort vorhandene Sachverstand in der Breite genutzt werden kann. Es gibt etliche Beispiele für diese mittlerweile breite Nutzung; etwa das IT-Grundschutzhandbuch des BSI, das inzwischen in weiten Teilen der Privatwirtschaft zur Prüfung von Sicherheitskriterien genutzt wird. Das Grundschutzhandbuch beinhaltet nicht nur technische Maßnahmen, sondern auch Angaben zu organisatorischen Erfordernissen, zum Sicherheitsbewusstsein und vielem mehr, und ich möchte an dieser Stelle ganz deutlich sagen, dass etwa das IT-Sicherheitsbewusstsein eine nicht zu unterschätzende Größe für die IT-Sicherheitskultur ist.
- Die „Task Force Sicheres Internet“ unter Federführung des BMI: Sie wurde im wesentlichen als Folge der Denial-of-Service-Attacken im Frühjahr 2000 ins Leben gerufen. Natürlich ist es richtig, dass die Politik zu entsprechenden Anlässen deutlich reagieren muss - nicht nur, weil es sachlich geboten scheint, sondern auch, weil es allgemein und zurecht erwartet wird. Den Maßnahmenkatalog der Task Force können Sie auf der BSI-Homepage nachlesen. Gelegentlich wird kritisiert, dass in diesem Bereich noch konkreter gehandelt werden müsste, aber ge-

legentlich sind entsprechende Erwartungen an den Kreis von Regierungsvertretern auch zu hoch gesteckt: Erwartet man im Ernst, dass die Experten sich ausschließlich über gesetzgeberische Maßnahmen unterhalten? Ich finde es gut und richtig, wenn durch geeignete Maßnahmen das Sicherheitsbewusstsein der Nutzer verbessert wird. Ein wichtiger Schritt ist die Bürger-CD des BSI, die einfach über die Homepage des BSI angefordert werden kann. Wir wissen von etlichen Experten, dass die CD zwar nur Hinweise für den einfachen Nutzer enthält, aber an diesen Kreis richtet sie sich eben gerade. Deshalb unterstützen wir diese CD. Sie dient dazu, Sicherheitsbewusstsein zu schaffen und gleichzeitig ein paar einfache Sicherheits-Tools anzubieten. Diese für jeden nutzbar zu machen, ist ein Schritt in die richtige Richtung.

- Computer Emergency Response Team (CERT): Wir haben beim BSI das CERT-Bund eingerichtet und arbeiten zur Zeit sehr intensiv an einem Verbund mit anderen CERTs. Der CERT Bund ist rund um die Uhr erreichbar; und wir arbeiten sehr intensiv daran einen Verbund zu schaffen, der bei entsprechenden Situationen ansprechbar ist. Ich darf in diesem Zusammenhang auch unterstützen, was mein Kollege vom Wirtschaftsministerium gesagt hat: Gerade in Bereichen, in denen es besonders schwierig ist, CERT-Strukturen ans Laufen zu bekommen, unterstützen wir staatlicherseits, bspw. beim M-CERT, also dem CERT für den Mittelstand. M-CERT haben wir ausdrücklich gemeinschaftlich unterstützt, gemeinsam mit dem Industrieverband „BITKOM“, und daran wird deutlich, dass wir bereit sind, erheblich in die Förderung der IT-Sicherheit zu investieren.
- Open-Source-Software: Natürlich hat es Diskussionen vielfältiger Art zu diesem Thema gegeben. Wir wissen, dass es anlässlich der gemeinsamen Presseerklärung des Innenministers mit IBM-Chef Staudt zum Rahmenvertrag zwischen Bund und IBM zur Förderung von Open-Source-Software etliche Nachfragen gegeben hat. Es besteht ja überhaupt kein Zweifel, dass wir uns auch in einer Linux-Umgebung nicht in einer sicheren Welt bewegen - die Tatsache, dass man auch dort Angriffen ausgesetzt ist, ist evident. Darum geht es uns aber nicht. Uns geht es vor allem um mehr Transparenz. Microsoft-Produkte sind nach wie vor in weiten Bereichen intransparent - und gerade aus diesem Grunde für uns zwangsläufig nicht sicher genug. Deshalb haben wir auf Bundesebene die Entscheidung getroffen, in transparenten Systemen arbeiten zu wollen, und deshalb fördern wir eine Migration hin zu Open-Source-Software. Zudem haben wir den Rahmenver-

trag so gestaltet, dass er nicht alleine für den Bund gilt, sondern dass die gesamte öffentliche Verwaltung unter Bezugnahme auf diesen Rahmenvertrag zu günstigen finanziellen Bedingungen eine Eintrittsmöglichkeit erhält. Dies war, ich wiederhole es, eine bewusste strategische Entscheidung hin zu mehr Transparenz und zur Offenlegung von Schnittstellen. Ich will an dieser Stelle nicht die ganze Litanei wiederholen, die wir in den langen Diskussionen mit Microsoft hatten. Wir haben uns diesen Schritt sehr gründlich überlegt - wohl wissend, dass wir damit nicht alle Sicherheitsprobleme aus der Welt geschafft haben.

Ausblick und Prognose

Ich finde es immer ein wenig vermessen, wenn so getan wird, als sei die Realität im Internet eine Realität besonderer Art. Wir bewegen uns im Internet wie im täglichen Leben. Daraus folgt u.a.: Genauso wenig, wie der Bundesinnenminister mich grundsätzlich davor bewahren kann, am hellichten Tage oder spätabends in Berlin oder Hamburg ausgeraubt zu werden, so wenig kann er mich grundsätzlich davor bewahren, dass ich in meiner privaten Internetnutzung gestört, gehackt oder manipuliert werde. Wir leben in einer Welt, in der es Kriminalität und Sicherheitsrisiken gibt. Über diese Risiken müssen wir uns im klaren sein.

Natürlich kümmert sich neben den dafür zuständigen Bundesländern auch das BMI intensiv um Kriminalitätsbekämpfung, und natürlich müssen wir die entsprechenden Instrumente weiter entwickeln; aber es gibt keine einhundertprozentige Sicherheit. Wichtig sind vor allem Information und Sensibilisierung – vor allem in dieser Hinsicht können wir sicherlich noch mehr tun – im Hinblick auf die Sicherheitsrisiken im Internet. Es muss uns dadurch gelingen, Vertrauen in die Nutzung des Internet zu schaffen, bei gleichzeitiger Kenntnis der Sicherheitsrisiken.

Ich finde in diesem Zusammenhang das Signal, das die Bundesregierung gibt, indem sie selbst wichtige Dienstleistungen im Netz bis 2005 anbieten möchte, besonders wichtig. Hier handelt es sich um ein Signal der Selbstverpflichtung, noch mehr für das Vertrauen ins Internet zu tun. Hier ist die Bundesregierung in der Pflicht, sehend allerdings, dass wir das nicht alleine tun können: Es ist nicht allein eine staatliche Aufgabe, wir sind im intensiven Dialog mit der Internet-Wirtschaft, mit den Nutzern, mit Verbraucherverbänden und auch mit dem Datenschutz. Dass wir viel zu tun haben, wissen wir, aber wir zählen auch auf Unterstützung von allen Seiten!

2. Private Nutzer im Visier von Unternehmen und dubiosen Geschäftemachern

2.1. Gefahrenpotenziale und Missbrauchsziele: Von der elektronischen Signatur, systematischen Datenauswertung bis hin zu Viren und Trojanern

Jens Ohlig
Sprecher des Chaos Computer Clubs, Köln

Der Chaos Computer Club wurde vor mehr als 20 Jahren als Treff von Computerbegeisterten gegründet. Er gibt seit 1984 in Hamburg die Zeitschrift „Die Datenschleuder“ heraus und ist seit 1986 eingetragener Verein. Im Jahr 1985 gab es einen kleinen Bruch in der Vereinsgeschichte: Damals wurde das zweite Wirtschaftskriminalitätsgesetz verabschiedet, in dem Vollkontaktvarianten des Hacksports mit so hässlichen Wörtern wie „Ausspähen von Daten“ belegt wurden. Für uns stand die Frage im Raum, ob wir als kriminelle Vereinigung nach § 129a oder als eingetragener Verein weitermachen. Wir haben uns für letztere Option entschieden.

Der Chaos Computer Club arbeitet heute als bundesweiter Verband und ist in die Lobby-Liste des Deutschen Bundestages für die Bereiche Telekommunikation, Post etc. eingetragen. In unserem Handeln fühlen wir uns von der Hacker-Ethik geleitet, wobei ich im heutigen Rahmen nur auf wenige Punkte dieser Ethik eingehen möchte, die Sie auf unserer Web-Seite www.ccc.de nachlesen können. Wir fühlen uns einerseits dem Anspruch verpflichtet, dass alle Informationen frei sein müssen, auf der anderen Seite formulieren wir jedoch auch datenschutzrechtlich den Anspruch, öffentliche Daten zu nutzen und private Daten zu schützen. Wir denken, dass der spielerisch-schöpferisch-kreative Umgang mit der Technologie zu diesem neuen, in vielen Bereichen noch unerforschten Medium vielleicht der richtige Ansatzpunkt ist.

Sicherheit ist das Thema dieser Veranstaltung, und wenn ich einen Eintrag des Brockhaus paraphrasieren darf, den ich zu diesem Stichwort gefunden habe: „Sicherheit ist die gefühlte Abwesenheit von Bedrohung“, dann handelt es sich in erster Linie nicht um etwas objektiv Messbares, sondern um etwas Fühlbares, ähnlich wie

bei der gefühlten Temperatur oder auch bei der gefühlten Uhrzeit, wie man sie morgens beim Aufstehen wahrnimmt. So sieht es auch mit der Sicherheit aus: wenn man sich gut und sicher fühlt, dann ist man meist auch sicher.

Auf der einen Seite wird in Deutschland viel für die Sicherheit im Netz getan, wie wir schon von den Vertretern der Ministerien gehört haben: Im Bereich des Signaturgesetzes soll Deutschland Vorreiter in Europa sein, die Datenschutzgesetzgebung ist im Prinzip vorbildlich und bspw. mittels des Volkszählungsurteils immer sehr auf die Bürger gerichtet gewesen. Die Technik wird immer bedienungsfreundlicher, so dass sich immer mehr Leute mit Sicherheitsprodukten vertraut machen können. Und letztendlich gibt es eigentlich auch keinen Grund, sich um die Sicherheit zu sorgen, denn die meisten Menschen sind einfach gut und stellen keine Bedrohung dar. Es gibt eine Statistik, dass weniger als ein Prozent aller e-bay-Transaktionen, also von Geschäften übers Internet, bei denen völlig Fremde völlig Fremden Geld zuschicken und dann dafür Waren bekommen, zu Beschwerden führen. Das Standardverhalten ist, gut zu sein und den Menschen Gutes zu wollen. Über Sicherheit müssen wir uns aus diesem Blickwinkel keine Gedanken machen.

Andererseits: Wir haben es heutzutage nicht mehr mit Programmen zu tun, wir haben es auch nicht mehr mit Maschinen zu tun, bei denen wir jedes Bit einzeln kennen, sondern - Herr Brunnstein hat das auch mehrfach betont - wir arbeiten mit komplexen Systemen, die nicht mehr überschaubar sind und wir arbeiten mit dem Problem der Konvergenz, so dass Systeme zusammenwachsen. Die Überschaubarkeit ist also letztendlich überhaupt nicht mehr gegeben.

Das Internet, das es ja erst seit ein paar Jahren in dieser Form gibt - ich erinnere mich, wie ich als Schüler Anfang der neunziger Jahre meinen Zugang ans Internet über eine Universität erstreiten musste - und das immer stärker sämtliche Lebensbereiche durchdringt und immer wichtiger für Geschäftsabläufe wird, wird jetzt auch immer attraktiver für Angreifer, die unterschiedlich motiviert sein können. Es kann sich um materiell interessierte „08/15-Kriminelle“ handeln, aber auch um Politiker, die jetzt sehen, dass sich über die Jahre hinweg etwas selbststeuernd ohne ihr Zutun entwickelt hat, und die jetzt in diesen Prozess steuernd eingreifen möchten.

Nicht alles, was in der Theorie so schön klingt, ist in der Praxis wirklich relevant. In der Theorie soll es so sein, dass es zwischen Theorie und Praxis keinen Unterschied gibt, aber in der Praxis sieht das anders aus: Vieles, was wir unter dem Stichwort „Signaturgesetz“ oder auch über die Sicherheitsprodukte der Industrie gehört haben, relativiert sich in der Wirklichkeit. Public Key Infrastructure (PKI) und Firewall sind letztendlich nur Worte für Konzepte. Man beschreibt das Problem, löst es aber nicht. Man hat jetzt viele schöne Fremdworte, um das Problem besser in Worte zu fassen; das Ganze erinnert mich sehr an Naturreligionen, etwa Voodoo, wo Worte als Beschwörungsformel eingesetzt werden.

Das Ziel von Sicherheitsmaßnahmen, so hat es jemand vom Chaos Computer Club mal formuliert, kann nur sein, zwischen dem Aufwand zur Sicherung und dem Aufwand zum Durchbruch dieser Sicherung ein Ungleichgewicht zu Ungunsten des Angreifers herzustellen. Das klingt vielleicht ein bisschen komplizierter als notwendig, trifft aber meiner Meinung nach den Kern der Sache. Schauen wir uns die Problematik mal an einigen Beispielen aus der Praxis an:

Mobile Systeme haben uns im letzten Jahr in Form von drahtlosen Funknetzwerken[3] beschäftigt. Damals war noch der Start-Up-Boom zu sehen, bei dem junge, freche, fröhliche Leute sagten, dass sie auf Kabel auch in ihrer Heimvernetzung verzichten und mit Funknetzwerkkarten in ihrem Gebäude mobil machen. Was nicht bedacht wird: wenn man ein solches Gerät einfach kauft und aufstellt, ohne es vorher zu konfigurieren, dann ist das alles sehr, sehr „gastfreundlich“: Man strahlt nämlich auch auf die Straße. Diese Technologie hat sich inzwischen zur Massentechnologie entwickelt und die Reaktion darauf ist, dass sich ein neuer Volkssport entwickelt hat, nämlich das Finden von offenen Funknetzwerken: man fährt einfach mit einem PKW und einer Funknetzkarte, die ca. 100 Euro kostet - also im Bereich des erweiterten Taschengeldes liegt - durch die Stadt und findet viele freundliche Firmen, die einem gerne Internet spendieren möchten oder kein Problem damit haben, einen an Privatkorrespondenz oder internen Geschäftsberichten teilnehmen zu lassen. Im Chaos Computer Club in Berlin haben wir unsere Bemühungen hierzu kartografiert, und uns fiel bspw. auf, dass sämtliche Krankenhäuser in Berlin mit Funknetzwerken ausgestattet sind, über die dann Patientendaten und Medikationen gesendet werden.

[3] Anm.: Häufig unter dem Begriff WLAN - Wireless Local Area Network diskutiert

Das Schöne an diesem Volkssport „offene Funknetzwerke finden“ ist, dass hier der deutsche Gesetzgeber in weiser Voraussicht gehandelt hat, denn das Ganze ist vollkommen legal. Das Ausspähen von Daten ist gemäß dem entsprechenden Strafrechtsparagrafen nur dann illegal, wenn eine besondere Sperre umgangen wird. Wenn Firmen aber so „gastfreundlich“ sind und ihre Daten auf die Straße strahlen, dann ist keine Sperre vorhanden, kein Passwort, dass ausgespäht werden muss, keine Verschlüsselung, die geknackt werden muss. Es handelt sich also eigentlich um eine Art „Public Service“.

Wir haben bezüglich der Krankenhäuser mit dem Berliner Datenschutzbeauftragten Kontakt aufgenommen und haben ihn darauf hingewiesen, dass Privatpersonen betroffen sind. Es ist uns gelungen, dass die Krankenhäuser umgestellt haben und jetzt die Möglichkeit zur Verschlüsselung nutzten. Doch immer noch findet man in jeder deutschen Großstadt offene Funknetze von Firmen - Businesspläne der NRW-Kabelbetreiberfirma ish sind auf diesem Wege aufgetaucht, da das Funknetz direkt auf ein Studentenwohnheim strahlte - es ist ein Kampf gegen Windmühlenflügel.

Das eigentliche Problem ist das Problem der black box: Man stellt sich ein Gerät auf, dass die Probleme der Verdrahtung lösen soll und man weiß eigentlich gar nicht genau, was damit gemacht wird. Wir werden demnächst sicher auch erleben, dass so etwas wie Bluetooth, also kleine Mikronetzwerke, in denen das Handy mit dem Notebook oder dem PDA redet, im Sinne der erwähnten Gastfreundschaft in Deutschland genutzt werden.

Das nächste Beispiel: der Source Code für das Virus „I love you“. Was ich für ein riesiges Problem im Bereich der Privatanwender halte, ist, dass das Betriebssystem Windows mit seinem überragenden Marktanteil dafür optimiert ist, möglichst alle Viren dieser Welt abspielen zu können. Ich persönlich verstehe nicht, wieso ein e-mail-Programm wie Outlook unbedingt ferngesteuert werden muss. Als Vergleich: man kauft sich ein Fertighaus und bei diesem Fertighaus ist auch ein Briefkasten dabei, der natürlich mit dem Badewasser und der Gasleitung des Hauses verbunden und wenn ich eine speziell geschriebene Postkarte hinein werfe, dann wird das Badewasser aufgedreht und der Gashahn wird geöffnet und nach einigen Minuten wird ein

Streichholz gezündet... - und wenn man sich dann bei Microsoft beschwert, dann heißt es: It´s not a bug, it´s a feature...

Ein Punkt, der Privatanwendern auch zu Denken geben sollte, ist das Wachsen von Begehrlichkeiten bspw. in der Industrie: Es gibt die Tendenz dazu, außerhalb des Deutschen Datenschutzgesetzes regelrechte Datensammlungen anzulegen. Spezialisiert darauf hat sich bspw. die Firma EDS (Electronic Data Systems) in den USA, gegründet vom ehemaligen Präsidentschaftskandidaten Ross Perrot. Die Firma EDS bietet als Service auch Datensammlungen als Komplettlösung für ganze Bundesstaaten oder kleinere Staaten oder Länder an, mit denen man genau sehen kann, wann jemand seine Alimente nicht gezahlt hat und daraufhin den Führerschein sperren kann. Man kann mit diesen Datensammlungen hervorragende Profile anlegen. Jeder, der eine Bahn Card hat, kann sich glücklich schätzen, bei EDS mit einem Foto in der Datenbank zu landen. Es gibt viele Großfirmen, die ihre Datensammlung über EDS betreiben und ganz froh sind, dass man so etwas in den USA fernab der allzu strengen deutschen Datenschutzgesetze machen kann. 1996 hat schon American Express ganz deutlich zugegeben, dass das neue Kerngeschäft gar nicht mehr das Geschäft mit Kreditkarten und das Hin- und Herbezahlen ist, sondern das Data Mining, das Erstellen von Benutzerprofilen, die dann auch gewinnbringend verkauft werden können.

Wie eine Bombe hat diese Meldung nicht eingeschlagen. In den USA ist der Umgang damit auch etwas lockerer, wie man an einer Werbung von American Express sehen kann: Ein junger Mann kauft sich regelmäßig Holzfällerhemden. Eines Tages möchte er heiraten und kauft sich einen Anzug. Da klingeln die Alarmglocken im Geschäft, er wird nach hinten gebeten und die Verkäufer erklären ihm aufgeregt, dass dies nicht zu seinem bisherigen Benutzerverhalten passt. Der Spot endet mit dem Slogan „American Express - we care for you.“ Ich weiß nicht, ob wir in Deutschland auch schon an diesem Punkt angelangt sind, oder ob dies eine Entwicklung ist, für die wir noch ein, zwei Jahre Zeit brauchen.

Auf der anderen Seite gibt es natürlich auch politische Begehrlichkeiten, und es wird vor dem 11. September (2001) anders entschieden als danach. Ein Beispiel: In den USA wurde die Einrichtung eines National Infrastructure Protection Center geplant,

für das ein paar Milliarden Dollar veranschlagt wurden. Nach der heute schon angesprochenen Distributed-Denial-of-Service-Attacke, die im Frühjahr 2000 gegen Amazon und andere große Großhändler im Internet stattfand, hatte auch der letzte Senator verstanden, was National Infrastructure Protection heißen sollte. Das Budget für diese Planung wurde umgehend genehmigt.

Am Beispiel des I-love-you-Virus kann man sehen, dass über die Konvention über Straftaten im Cyberspace, die sog. Cyber-Crime-Konvention des Europarates viel diskutiert wurde; und es war einem von der Schule frustrierten Filipino[4] zu verdanken, dass man sich einig war, bei diesem Thema länderübergreifend zusammenzuarbeiten und die Polizeiarbeit zu koordinieren. Nach dem 11. September brach diese Diskussion jedoch ab.

In Deutschland wurde die Telekommunikations-Überwachungs-Verordnung relativ intensiv diskutiert, wobei auch der Chaos Computer Club auf einer Anhörung einigen Input liefern konnte. Nach dem 11. September war die Diskussion abrupt zuende. Die Verordnung ging noch nicht einmal durch den Bundestag, sondern wurde letztendlich im Kabinett abgenickt. Ebenso ging es auch mit der Cyber Crime Convention, die dann auch sehr, sehr schnell vom Europarat und anderen Ländern, dabei an erster Stelle Japan und die USA, angenommen wurde. Vor zwei Wochen wurde dann versucht, den Datenschutz für Verbindungsdaten abzuschaffen. Im Gesetz zum Schutz von Kindern vor sexuellem Missbrauch gibt es neben der rechtlichen Regelung für IMSI-Catcher auch noch die Abschaffung der Maximalspeicherzeit, so dass Verbindungsdaten unendlich lang gespeichert werden können - und dies natürlich mit direktem Zugriff für Polizei und Geheimdienste.

Ich frage mich bei diesen ganzen Maßnahmen: Wenn Sicherheit ohnehin nur die gefühlte Abwesenheit von Bedrohung ist, schaffen dann solche Maßnahmen ein Gefühl der Sicherheit? Wenn man den Bürgern in diesem Land die Bedrohung durch immer restriktivere Gesetze ständig vor Augen führt, wächst dann das subjektive Sicherheitsgefühl oder wächst das Gefühl der Bedrohung?

[4] Anm.: als Tatverdächtigem

Ich komme nun zu meinem Utopia, meinen Visionen für die Gesellschaft: Es hat sich wirklich gezeigt, und dies nur als kleine Randnotiz zur open-source-Problematik: das Prinzip „Security by obscurity“ ist vollkommen überholt, denn es ist durch die Realität oft widerlegt worden. Sicherheitsmängel werden dadurch behoben, dass ich mit möglichst vielen Leuten rede und möglichst mit offenen Karten spiele.

Ich sehe noch ein großes Problem in der Aufklärung, auch im Umgang mit dem, was als Sicherheitslücke verstanden wird. Anzudenken wäre eine Art Spielwiese für Hacker. Vielleicht sollte man auch die kostenlose Sicherheitsberatung unseres Clubs, die dann geleistet wird, wenn Organisationen, auf deren Web-Seite gehackt wurde, sich beim Chaos Computer Club darüber beschweren, als Zugewinn an Information oder als externes Potenzial nutzen.

In Richtung Politik muss hinsichtlich der Gesetzesbearbeitung die Forderung formuliert werden, dass Verantwortlichkeiten definiert werden - das ist gerade beim Homebanking nicht im Sinne des Verbrauchers geregelt. Ich würde mir wünschen, dass man nicht davon ausgeht, ein theoretisch sicheres Verfahren zu haben, sondern dass man die Verantwortlichkeit umdreht und die Bank in vollem Umfang für Fehler dieses Verfahrens haftet.

Man lebt besser ohne Verschwörungstheorie. Man lebt besser, wenn man akzeptiert, dass unsere Welt unsicher ist - das Beispiel des Straßenverkehrs wurde heute morgen schon genannt - und vielleicht sollten wir eine Kultur entwickeln, in der wir mit der Unsicherheit leben und Spaß an der Unsicherheit gewinnen. Ich habe mir diesen Satz geklaut, auf einer ähnlichen Veranstaltung, als noch der dot.com-boom blühte und ein sehr amerikanisch wirkender Redner aufs Podium stieg und schrie: „New Economy ist Spaß an der Unsicherheit“. Damit hat er einen sehr wichtigen kulturellen Punkt der Hacker-Gemeinde auf seine Art und Weise formuliert und in diesem Sinne wünsche ich Ihnen viel Spaß am Leben mit der Unsicherheit.

2.2. Teure Dialer – Unseriöse Anbieter und ihre Tricks

Sascha Borowski
Journalist und Betreiber der Internetseiten www.dialerschutz.de, Augsburg

Ich weiß nicht, wie hoch Ihre letzte Telefonrechnung war. Mir ist ein Herr aus Frankfurt bekannt, bei dem betrug die Aprilrechnung 90.000 Euro. Inzwischen hat der Herr die zweite Mahnung seiner Telefongesellschaft auf dem Tisch und einen Anwalt engagiert. Das Ganze hat nämlich einen großen Haken: Der Mann weiß bis heute nicht, wer genau diese 90.000 Euro eigentlich von ihm haben will.

Von der Höhe her ist das sicher ein Einzelfall, die Situation selbst ist es nicht. So wie diesem Mann ist es in den vergangenen Monaten Hunderten, vermutlich sogar Tausenden Menschen in Deutschland ergangen – sie wurden Opfer so genannter 0190-Dialer. Genauer gesagt, sie wurden Opfer des Missbrauchs von Webdialern. Dialer sind nämlich eigentlich ein völlig seriöses und auch sinnvolles Abrechnungssystem im Internet. Kurz gesagt sind Dialer kleine Programme, die auf einem Rechner einen neuen Internetzugang einrichten. Wenn das Ganze über eine höher tarifierte Mehrwertnummer wie der 0190 erfolgt, spricht man von 0190-Dialern. Gedacht sind solche Dialer eigentlich dafür, Dienstleistungen im Internet, beispielsweise Support, Softwaredownloads, aber auch erotische Angebote, einfach über die Telefonrechnung bezahlen zu können. Denn das Inkasso der meisten 0190-Gebühren übernimmt die Telekom. Und in vielen Fällen klappt das auch einwandfrei und problemlos, weil die meisten Dialeranbieter, auch wenn es einen anderen Anschein hat, seriös arbeiten .

Dass die 0190-Dialer gerade in den vergangenen Monaten massiv in Verruf geraten sind, liegt an einigen Schwarzen Schafen der Branche, die den Dialer als Mittel erkannt haben, Websurfer ganz bequem und ohne großen Aufwand abzocken zu können. Fakt ist nämlich, dass das System der 0190-Dialer, so wie es sich heute darstellt, sehr anfällig für den Missbrauch ist. Dies hauptsächlich aus vier Gründen:

- Zum Einen, ich habe es vorhin angesprochen, übernimmt die Telefongesellschaft in der Regel das Inkasso der Dialer-Gebühren. Der Betroffene, oder eben das Opfer, bekommt den tatsächlichen Anbieter des Mehrwertdienstes auf der Rechnung überhaupt nicht zu sehen. Diese relative Anonymität lockt Schwarze Schafe natürlich geradezu an.

- Eine zweite Schwachstelle ist das System der Mehrwertnummern an sich. Zuständig für die Nummernvergabe in Deutschland ist die Regulierungsbehörde für Telekommunikation und Post. Diese vergibt die 0190-er Nummern in Tausenderblöcken an Netzbetreiber wie die Telekom oder Hansenet hier in Hamburg. Die Netzbetreiber wiederum vermieten die Nummern an Unternehmen, zum Beispiel Betreiber von Dialern. Und die vermieten Dialer und Nummern an ihre Kunden, etwa Betreiber von Erotikseiten. Der Endverbraucher, nämlich der Surfer, der mehr oder weniger freiwillig über einen Dialer ins Internet geht, hat eigentlich kaum eine Chance herauszufinden, bei wem er sich denn nun über seine überhöhte Telefonrechnung beschweren soll.

- Ein dritter Punkt ist die Vergabepraxis bei den Webdialern. Es ist auch heute noch so, dass man binnen fünf Minuten, meistens gleich online, einen Dialer und eine zugehörige 0190-Nummer mieten kann. Wie und wofür dieses Wählprogramm dann eingesetzt wird, interessiert den Dialerbetreiber in der Regel eher weniger – kein Wunder, er verdient ja auch mit.

- Das vierte und eigentlich auch verhängnisvollste Problem ist die Freigabe der Tarife bei den 0190-0-Nummern. Seit Anfang des Jahres können Betreiber von 0190-0-Nummern selbst festlegen, wie viel Geld sie dafür verlagen wollen. Das Ergebnis waren die so genannten Pauschal-Dialer, die pro Einwahl bis zu mehreren hundert Euro abrechneten. Was es bedeutet, wenn man sich mehrere Mal nacheinander mit einem 300-Euro-Dialer ins Internet einwählt, können Sie sich vorstellen.

Diese vier genannten Punkte haben zu der Situation geführt, wie wir sie heute vorfinden: auf der einen Seite Schreckensmeldungen über Dialer-Opfer und damit verunsicherte Surfer, auf der anderen Seite Abzocker, die versuchen, ihre Webdialer mit

allen Mitteln unters Volk zu bringen. Ich höre oft den Vorwurf, man müsse schon sehr unvorsichtig sein, um auf einen Dialer hereinzufallen. Ich glaube das nicht. In den sechs Monaten, in denen es die Seite Dialerschutz.de jetzt gibt, habe ich knapp 2000 Mails erhalten von Menschen, die mich auf neue (oder auch alte Tricks) von Dialeranbietern aufmerksam machten. Herauskristallisiert haben sich dabei zwei Kategorien von Tricks: zum einen technische Tricks und zum Anderen Fälle, die man als „unlautere Werbung“ bezeichnen könnte.

Diese unlautere Werbung wird in vielen Fällen verwendet, um einen 0190-Dialer überhaupt erst einmal an den Mann zu bringen. Eine Paradebeispiel dafür ist der Dialer eines Düsseldorfer Unternehmens, der sich nicht Dialer nennt, sondern „Kostenloses Update der Verbindungssoftware“. Das klingt gut und hilfreich, kann aber sehr teuer kommen, wie leider viele Menschen im Frühjahr dieses Jahres feststellen mussten. Aber das Wort „kostenlos“, das wissen Sie und das wissen auch die Dialeranbieter, zieht eigentlich immer. Zum Beispiel in e-mails, die zu Tausenden unaufgefordert versandt werden und die das Blaue vom Himmel herunter versprechen. Das geht vom kostenlosen Doftwaredownload bis hin zum berüchtigten „Crack-Dialer“, über den angeblich der freie Zugang zu Erotikangeboten möglich ist.

Andere Dialer-Anbieter halten sich nicht lange mit Werbung auf, sondern lügen ihren Seitenbesuchern direkt ins Gesicht. Da wird dann behauptet, die Seite werde ohne eine bestimmtes „Plug-in“ nicht richtig dargestellt oder es wird gleich eine völlig gefälschte Fehlermeldung angezeigt – und der Lösungsvorschlag gleich mit: ein 0190-Dialer. Der Gipfel der Irreführung, und hier kommen wir in den strafrechtlich relevanten Bereich, ist die Tarnung von Webdialern durch renommierte Namen. Hier hat es vor allem zwei aufsehenerregende Fälle gegeben: einen Dialer, der angeblich ein Virenschutzprogramm von Microsoft war, und ein 0190-Dialer, der als Zugangsprogramm von T-Online getarnt war. Bis heute ist übrigens unklar, wer diese Programme in Umlauf gebracht hat.

In die zweite Kategorie der Tricks fallen die technischen Spielereien. Besonders ärgerlich sind hier zum einen die so genannten Autodialer, also Dialer, die sich beim Betreten einer Webseite automatisch installieren und in bestimmten Fällen sogar selbstständig einwählen. Aktuell sind mir in Deutschland nur zwei Firmen bekannt,

die solche selbsteinwählenden Dialer anbieten. Es versteht sich von selbst, dass sich solche Firmen juristisch auf sehr dünnem Eis bewegen. Der automatische Download ist dagegen auf sehr vielen Seiten verbreitet. Zu den technischen Tricks zählt es sicherlich auch, Webdialer so zu manipulieren, dass sie sich einwählen, die Verbindung trennen und dann erneut einwählen. Das hatten wir Anfang des Jahres häufig, als ein paar Dialeranbieter die Vorzüge der Pauschalabrechnung für sich entdeckten. Ich muss nicht weiter ausführen, was es bedeutet, wenn man sich einen 300-Euro-Dialer einfängt, der sich pro Minute viermal einwählt.

Viele hohe Rechnungen, und damit bin ich beim dritten Punkt der technischen Tricks angekommen, haben die so genannten Capi-Dialer verursacht. Das sind Webdialer, die sich im Hintergrund direkt über die ISDN-Karte einwählen um vom Surfer quasi überhaupt nicht bemerkt werden. Auch diese Dialer wurden Anfang des Jahres verstärkt – und unter falschem Namen – an Tausende Menschen per Email verschickt.

Sie sehen, wenn es ums schnelle Geld geht, ist der Einfallsreichtum groß. Ein bisschen schwieriger wird es, wenn es um Lösungen für die aktuelle Dialer-Problematik geht. Man kann natürlich die 0190-Nummern für seinen Anschluss sperren lassen. Das geht relativ problemlos, hat aber den Nachteil, dass man danach auch keine seriösen Mehrwertdienste mehr nützen kann.

Eine zweite Möglichkeit besteht darin, nur über DSL ins Internet zu gehen. Webdialer können sich über DSL nicht einwählen. Das Problem dabei ist, dass man beispielsweise für das Faxen über den PC trotzdem eine ISDN-Leitung oder ein Modem braucht.

Viele Menschen setzen inzwischen auf diverse Schutzprogramme, die im Internet erhältlich sind. Diese aber haben den Nachteil, dass sie keine hundertprozentige Sicherheit bieten. Verschiedene Webdialer sind so programmiert, dass sie vor der Einwahl erst einmal sämtliche Schutzprogramme deaktivieren.

Was bleibt, sind rechtliche und verbraucherpolitische Lösungen, darüber werden wir ja später auf dieser Tagung noch diskutieren. Verbraucherschutzministerin Renate Künast hat zur Klärung der Dialer-Problematik bereits einige Vorschläge gemacht,

die meiner Meinung nach auch in die richtige Richtung gehen. So soll die Telekom künftig nur noch das Inkasso der 0190-Gebühren übernehmen, wenn der Kunde keine Einwendungen dagegen hat. Anderenfalls soll der Mehrwertdienstanbieter die Forderung eintreiben müssen. Das hätte den Vorteil, dass Schwarze Schafe sich früher oder später outen müssten.

Ein weiterer Punkt ist eine Art Beweislastumkehr. Bisher ist es so, dass der Inhaber eines Telefonanschlusses, also der Surfer, zunächst einmal für alle Gebühren an seinem Anschluss haftbar gemacht wird. Fühlt er sich betrogen, muss er das nachweisen. Künast will es genau umgekehrt haben: Der Dienstanbieter soll nachweisen, dass er die Gebühren zu Recht einfordert. Auch das dürfte zum Verbraucherschutz beitragen. Ebenso die geforderte Anbieterkennung, anhand derer jeder Webdialer einem namentlich bekannten Anbieter zugeordnet werden kann. Gerade die vergangenen Monate haben gezeigt, dass die gewünschte Selbstkontrolle der Betreiber von Webdialern so nicht funktioniert. Es gibt zwar einen Verhaltenskodex, an den sich die Dialer-Anbieter halten sollen. Verpflichtend ist er aber nicht. Und echte Sanktionen haben Schwarze Schafe auch nicht zu erwarten. So lange das so bleibt, wird es weiter Fälle geben wie den Herrn aus Frankfurt mit seiner 90.000-Euro-Rechnung.

2.3. Produkte für mehr Sicherheit im Internet

Björn Dehms
Bundesamt für Sicherheit in der Informationstechnik (BSI), Referat Sicherheitsanalysen, Bonn

Der Vortrag befasst sich mit Programmen, die den privaten PC vor Angriffen schützen und die unerwünschte Preisgabe sensibler Daten verhindern sollen. Ich werde Ihnen dabei keine Produkte von bestimmten Herstellern vorstellen, da ich deren Güte nicht beurteilen kann. Um die Güte bestimmter Software-Produkte beurteilen zu können, müssen diese in menschenlesbarer Form vorliegen; dem BSI liegt der Zugriff aber meistens nur in maschinenlesbarer Form vor. Darüber hinaus ist das BSI als Bundesamt zu einer gewissen Neutralität verpflichtet und darf nur Produkte weiter empfehlen, die dort zertifiziert wurden.

Ich werde jedoch Produktkategorien vorstellen, also Typen von Produkten, die Sie bei sich zu Hause am PC einsetzen können und ich möchte Ihnen dann vorschlagen, ins Internet zu schauen, mit Hilfe einer Suchmaschine nach diesen Produkten zu suchen und gegebenenfalls eines davon, möglicherweise auch ein kostenloses, auszuwählen. Einige Werkzeuge und weitere Hinweise zum sicherheitsbewussten Verhalten am Heim-PC finden sich auch auf der vom BSI erstellten CD „Ins Internet – mit Sicherheit“. Ich empfehle Ihnen, diese kostenlose CD zu bestellen; sie beinhaltet auch eine Link-Liste zu weiterführenden Themen.

Zwei grundsätzliche Bedrohungen sind vom Heimanwender in Betracht zu ziehen, zum einen die Zerstörung von Daten bzw. Software, zum anderen das Ausspähen sensibler Informationen wie z. B. Zugangsdaten zum Online-Banking. Dementsprechend habe ich das Thema „IT- bzw. PC-Sicherheit im privaten Umfeld“ im Folgenden in zwei Bereiche unterteilt:

1) Der Schutz Ihres Rechners; d.h. Schutz der Software und Ihrer Daten vor Zerstörung;
2) Der Schutz Ihrer Daten vor Einsichtnahme; d.h. der Schutz davor, dass Ihre Daten ungewollt in das Internet gelangen.

Der Schutz Ihres Rechners

Viren und Virenscanner

Ein Virus ist ein selbständiges Programm, das versucht, sich zu reproduzieren. Von einem Rechner versucht es per Diskette oder via Internet auf andere zu gelangen, und in aller Regel versuchen Viren auch, Schaden anzurichten, Dateien zu zerstören oder, im Extremfall, die Festplatte zu formatieren.

Sie können sich mit einem Virenscanner davor schützen. Der Virenscanner stellt eine Positivliste sämtlicher bekannter Viren dar. Wenn eine Datei bei Ihnen auf der Festplatte gespeichert oder per e-mail heruntergeladen wird, dann kann ein Virenscanner diese Datei mit der Liste vergleichen und erkennen, ob die Datei möglicherweise virenverseucht ist. Das Problem der Virenscanner liegt darin, dass ein Virenscanner von heute keine Viren von morgen erkennen kann. Jeder neue Virus muss in die Lis-

te eingetragen werden, sie müssen Ihr Produkt „updaten“, sonst sind Sie vor einem brandneuen Virus nicht geschützt.

Virenscanner gibt es in zwei Ausprägungen: Zum einen den Virenwächter, der beim Neuaufspielen von Dateien automatisch aktiv wird. Die andere Version ist der Boot-Sektor-Prüfer, den Sie einmal bei Bedarf starten - in der Regel dann, wenn Sie den Virenscanner neu installiert haben - um einen Grundschutz Ihres Rechners sicherzustellen.

Personal Firewall per Diskette oder via Internet

Das Besondere an einer Firewall ist, dass Sie den Zugriff auf Ihren Rechner beschränken können; d.h. Sie können speziell andere Rechner oder Anwendungen im Internet davon ausschließen, mit Ihrem Rechner Kontakt aufzunehmen. Zum zweiten können Sie Anwendungen wie Ihren Internet Explorer oder Ihren Netscape Communicator daraufhin überprüfen, ob Manipulationen von Schadprogrammen vorgenommen wurden. Es wird eine sogenannte Checksumme gebildet, und diese wird periodisch von der Firewall auf Veränderungen überprüft. Bei Veränderungen wird Alarm ausgelöst und sie werden darauf hingewiesen, dass möglicherweise Manipulationen stattgefunden haben.

Das Problem dieser Produktgruppe liegt darin, dass zur Nutzung einer Personal Firewall erhebliches Fachwissen erforderlich ist. Mich erreichen oft Anfragen von Bürgern, die mit den Fehlermeldungen der Firewall überfordert sind. Zu jedem Produkt gibt es jedoch auch entsprechende Anleitungen.

Intrusion Detection System (IDS)

Ein IDS versucht, Angriffe, die über das Netz auf Ihren Rechner gefahren werden, automatisiert zu erkennen. Es treten im Prinzip bei Angriffen auf Ihren Rechner typische bit-Folgen, besondere Muster, auf, die im IDS gespeichert sind, und sobald diese erkannt werden, schlägt das IDS Alarm. Das Funktionsprinzip ähnelt den Virenscannern, es ist wiederum eine Positivliste vorhanden und es findet ein Vergleich statt.

Die Systeme sind teilweise noch stark fehlerbehaftet: Es werden viele Fehlalarme ausgelöst; wenn also ein Alarm vorliegt, dann heißt das noch nicht, dass wirklich etwas passiert ist. Aber man sollte dem Alarm natürlich nachgehen. Ein Beispiel:

Sie haben sicherlich über die Internet-Würmer gelesen. Diese Würmer sind mittlerweile auf vielen Rechnern im Internet installiert und versuchen, eigenständig, wahllos zu anderen Rechnern im Internet Kontakt aufzunehmen. Das ist für Sie, wenn Sie über ein Modem ins Internet gehen, vergleichsweise ungefährlich, aber trotzdem schlägt das IDS dann bei Ihnen recht häufig Alarm. Das BSI hat einen Testrechner ins Internet gestellt und dieser meldete rund tausend Alarme an einem einzigen Wochenende.

Dialer-Schutz

Der Dialer-Schutz passt nicht ganz in die Systematik, denn eigentlich dient er nicht dem Schutz Ihres Rechners, sondern dem Schutz Ihrer Rechnung. Dennoch möchte ich ihn kurz erwähnen, denn ihm galt das Hauptinteresse der CeBit-Besucher am Stand des BSI.

Ein Dialer versucht, ohne dass Sie es merken, eine 0190-Verbindung aufzubauen. Prinzipiell stellen die 0190-Nummern eine sinnvolle, einfache Möglichkeit zur Bezahlung dar. Es kann jedoch passieren, dass bei Ihnen ein Dialer aufgebracht wird, ohne dass Sie es merken. Sobald Sie sich das nächste Mal ins Internet einwählen, wird nicht mehr die ursprüngliche Nummer Ihres Internet-Providers gewählt, sondern eine 0190-Nummer angewählt. Das hat zur Folge, dass erhebliche Kosten für Sie entstehen können, und zwar aktuell bis zu 400 Euro pro Minute.

Was können Sie dagegen tun? Es werden im Internet etliche Programme zum Schutz vor Dialern angeboten, die Sie sich herunterladen können. Diese Programme machen Folgendes: zum Einen werden Sie alarmiert, wenn ihr Modem - statt der ursprünglichen Nummer Ihres Internet-Providers - eine 0190-Nummer anwählt. Sie sind dann informiert und können die Verbindung schnell beenden, möglichst noch, bevor die Verbindung aufgebaut wurde. Zum Anderen untersucht das Programm Ihre Festplatte auf 0190-Dialer. Analog zu den Virenscannern gibt es eine Liste aller derzeit bekannten Dialer und diese werden mit den Dateien auf der Festplatte verglichen.

Sobald ein Dialer gefunden wurde, werden Sie alarmiert und haben die Möglichkeit, den Dialer zu entfernen.

Es gibt noch weitere Möglichkeiten, sich vor Dialern zu schützen, beispielsweise durch sichere Browser-Grundeinstellungen. Einen guten Überblick bietet die Seite dialerschutz.de, die ein ganzes Bündel von Maßnahmen vorstellt.

Lassen Sie mich noch auf ein Problem hinweisen: Auf der Suche nach Dialerschutzprogrammen im Internet kann es Ihnen passieren, dass Sie sich ein sogenanntes Trojanisches Pferd herunterladen; schlimmstenfalls laden Sie sich ein Programm herunter, dass sich Dialerschutz nennt, aber in Wirklichkeit selbst ein 0190-Dialer ist. Von der Seite dialerschutz.de aus gibt es aber sicherlich Links zu vertrauenswürdigen Produkten.

Zum Schutz des Rechners ließe sich noch einiges ergänzen: Sie können bspw. JavaScript filtern, Sie können sogenannte Sand-Boxes einsetzen; doch ich habe mich in meinem Vortrag auf die Produktgruppen beschränkt, die Ihnen auf einen Schlag den größten Schutz bringen.

Der Schutz Ihrer Daten auf Ihrem Rechner

Anti-Spyware-Werkzeuge

Spyware ist ein Begriff für Programme, die auf irgendeinem Weg auf Ihren Rechner gelangt sind und nun Informationen über Sie sammeln, zum Beispiel von der Festplatte oder durch Speicherung Ihres Nutzer-Verhaltens. Beim nächsten Verbindungsaufbau ins Internet versendet das Programm die Daten an den Rechner des Angreifers. Solche Spyware steckt heutzutage auch in vielen kommerziellen Software-Produkten; der Hersteller möchte wissen, was die Festplatte des Nutzers beinhaltet, ob illegale Software installiert ist und Ähnliches.

Möglicherweise wird über das Internet vieles ausspioniert, doch man weiß es nicht genau, wenn man es nicht ständig überwacht.

Was bewirkt ein Anti-Spyware-Werkzeug? Anhand einer Positivliste wird die Festplatte auf Spyware-Programme untersucht. Analog zum Virenscanner erhalten Sie Nachricht, sobald eine verdächtige Datei gefunden wird, so dass Sie diese entfernen können. Noch wichtiger ist: Anti-Spyware unterbindet die automatische Versendung von Informationen. Die Programme arbeiten verschieden, jedes hat seine Spezifika, doch alle bieten den Schutz vor - möglicherweise unbemerkter - Preisgabe von Informationen über Sie.

Auch hier sind regelmäßige Software-Updates sinnvoll, damit die Erkennung neuer Spyware-Programme möglich ist.

Web-Filter

Web-Filter sollen verhindern, dass unerwünschte Daten auf Ihren Rechner gelangen. Meistens stellen die Web-Filter Kindersicherungen für den Abruf bestimmter Internet-Seiten dar: Sie enthalten in der Regel eine Liste bedenklicher Seiten aus dem Internet und blocken die Anzeige dieser Seiten. Auch hier empfiehlt sich ein automatisches Software-Update, da sich die Adressen der Seiten sehr schnell ändern und immer wieder neue Seiten hinzukommen, die in die Liste eingepflegt werden müssen.

Die Programme lassen sich außer für den Schutz Ihrer Kinder auch als Schutz vor „Hacker-Seiten“ nutzen, von denen Sie sich möglicherweise unbemerkt 0190-Dialer herunterladen könnten.

Verschlüsselung

Das Thema „Verschlüsselung“ sollte man nicht unterschätzen: In den Jahren 1993/1994 hat bspw. eine deutsche Firma, die den ICE nach Asien verkaufen wollte, unverschlüsselt Daten übertragen. Diese wurden vom französischen Geheimdienst abgefangen; der TGV wurde geringfügig billiger angeboten. Datenverschlüsselung macht also durchaus Sinn, wenn die Daten wirklich schützenswert sind.

Verschlüsselung stellt die Vertraulichkeit Ihrer Daten her. Dies spielt hauptsächlich bei e-mails eine Rolle: wenn Sie bedenkliche oder sicherheitsrelevante e-mails schreiben, sollten Sie darüber nachdenken, diese zu verschlüsseln.

Mit einer elektronischen Signatur können Sie demgegenüber die Authentizität des Versenders sicherstellen. Die Fälschung des Absenders gelingt relativ leicht. Mit einer Signierung können Sie das verhindern. Ihr Rechner bekommt dann eine Meldung, dass eine gefälschte e-mail eingegangen ist. Wenn die Daten es wert sind, macht die Anwendung einer Signierungssoftware durchaus Sinn

Zum Abschluss möchte ich noch auf einen übergeordneten Aspekt hinweisen: Sämtliche von mir vorgestellten Produkte können eines nicht wett machen, und zwar Ihre Aufmerksamkeit! Ihre Augen und ihr Gehirn sind die besten Tools, die Sie verwenden können. Wenn Sie ein gesundes Gespür für bedenkliche Aktionen entwickeln, dann bringt Ihnen das mehr Sicherheit als das reine Aufrüsten des PC mit allen erhältlichen Sicherheitsprogrammen.

2.4. Forderungen der Verbraucherschutzverbände und Antworten von Politik und Gesetzgebung: Statements

2.4.1. Verbraucherschutzpolitische Forderungen

Edda Castello
Leiterin der Rechtsabteilung der Verbraucher-Zentrale Hamburg

Die zur Zeit wohl größte Unsicherheit für Verbraucher im Netz resultiert aus der "Dialer-Problematik". Der Kunde wird mit einer Telefonrechnung konfrontiert, deren Höhe er sich nicht erklären kann. Erst anhand eines Einzelverbindungsnachweises kann er erahnen, dass er vermutlich auf einen Dialer hereingefallen ist.

Die Verbraucher-Zentrale Hamburg hat den „Aufschrei nach mehr Sicherheit für Internet-Nutzer“, wie er im Vortrag des CCC-Sprechers gefordert wurde, deshalb schon gestartet: Wir haben seit Anfang Juni 2002 einen Aufruf zum Zahlungsboykott gegen 0190-Betrüger ins Netz gestellt. Damit wollen wir alle Verbraucher, die von einem 0190-Dialer betrogen wurden, aufrufen, die Zahlung an die Telekom oder den Netzbetreiber zu verweigern. Angesichts der gesetzlichen Situation mag dieser Aufruf ein wenig vorlaut erscheinen, denn es gibt zahlreiche Gerichtsentscheidungen zu Un-

gunsten der Verbraucher, die gegen die Zahlung unerwünschter Dialer-Dienste geklagt haben. Doch dies kann weder verbraucherpolitisch noch rechtspolitisch das letzte Wort sein.

Die gesamte Dialer-Problematik - und sie ist derzeit für die Verbraucher das Hauptproblem im Netz - erinnert stark an die Probleme mit dem Vertrieb von Zeitschriften vor einigen Jahren: Drücker wurden in die Dörfer und Städte geschickt und haben dort von Tür zu Tür Abonnements für Zeitschriften, und in der Anfangszeit auch für Buchclubs, verkauft - in der Regel an wehrlose Verbraucher. Unser Ansatz zur Lösung des Problems erforderte die Kenntnisse der Verantwortlichkeiten in der Vertriebskette: Zwar war der Drücker derjenige, der das Abonnement letztendlich verkauft hat, doch verantwortlich waren diejenigen, die diese Vertriebsform ins Leben gerufen haben und betreiben: die angesehenen Verlage Springer, Gruner und Jahr, Burda, Bauer und Bertelsmann.

Die Verbraucherzentrale Hamburg hat damals die Verbraucher aufgerufen, an der Haustür kein Abonnement zu unterschreiben - und dieser Aufruf ähnelt unserem heutigen Appell an die Internet-Nutzer, bei der Nutzung des Netzes gut aufzupassen. Doch man kann die Verbraucher nicht so fit machen und so schulen, dass sie sich im Netz immer richtig bewegen. Man muss dafür sorgen, dass das Netz so sicher ist, dass ein dummer, schlichter, einfacher Verbraucher das Netz vertrauensvoll nutzen kann, ohne dass etwas dabei passiert. Ich zähle mich übrigens auch zu diesem Nutzerkreis - ich habe keine Ahnung von Firewall und Virenschutzprogrammen; und auch im möchte mich sicher im Netz bewegen können.

Erfolg mit unserem Protest gegen die unlautere Buchclub- und Zeitschriftenwerbung hatten wir erst in dem Moment, als wir die Verantwortung bei den Verlagen festgemacht haben. Eine vergleichbare Situation liegt auch jetzt vor: Verantwortlich sind im Grunde die Netzbetreiber und die Telekom, denn alle Beteiligten in Zwischenstufen in der Kette vom Netzbetreiber über etliche Untermieter verdienen sehr gut an diesem Betrug. Wir werden erst dann ein Ende des Betrugs erreichen, wenn dieser sich nicht mehr lohnt. Dazu müssen wir ganz oben an der Kette die Verantwortlichkeit setzen und dafür sorgen, dass dort nichts mehr verdient wird.

Die aktuellen Maßnahmen, die in Bezug auf die Änderung der Kundenschutzverordnung in Angriff genommen werden, sind zwar ein Schritt in die richtige Richtung, doch bei weitem nicht ausreichend. Die Verbraucher, die sich unserem Boykott anschließen, brauchen gute Nerven, um ihn durchzuhalten, denn der Netzbetreiber kann mit einer Anschlusssperre drohen. Sie müssen mit Inkasso-Briefen rechnen, die die üblichen Drohungen der Inkasso-Büros wie Zwangsvollstreckung, Gerichtsvollzieher, Lohnpfändung beinhalten. Weiterhin ist damit zu rechnen, dass die Netzbetreiber versuchen, ihre Forderungen vor Gericht einzutreiben - und dann stellt sich die Frage, wie das Gericht entscheiden wird.

In der Rechtsprechung ist die Zahlungsverweigerung bei Dialer-Betrug noch nicht abschließend geklärt. Dort, wo eine Klärung scheinbar vorliegt (0190-Telefon-Sex-Gespräche), ist sie in einer solchen Weise grob ungerecht, dass sie nicht Bestand haben kann; überdies ist die Dialer-Problematik noch nicht beleuchtet. Einige Urteile:

Urteil des Bundesgerichtshofes vom 22. November 2001 Az.: II ZR 5/01

Der BGH nimmt in diesem Grundsatzurteil zum Verhältnis der Vertragsbeziehungen zwischen dem Nutzer einer 0190-Nummer, des Netzbetreibers und des Anbieters der 0190-Mehrwertdienste Stellung (Telefonsex).
Fazit: Der Kunde muss zahlen.

Urteil des Bundesgerichtshofes vom 16. Mai 2002 Az.: II ZR 253/02

Der BGH bestätigt seine Rechtsprechung, Telefonverbindungen seien wertneutrale Hilfsgeschäfte (Telefonsex).
Fazit: Der Kunde muss zahlen (in diesem Fall DM 16.654,67).

Kernpunkt ist die Frage: Ist die Telefon (oder Internet-)verbindung ein "wertneutrales Hilfsgeschäft" (dann muss der Kunde zahlen) oder wirkt sich der Inhalt des Gesprächs auf die Telefonverbindung aus oder handelt es sich um zwei Vertragsbeziehungen nämlich ad 1) Telefongesellschaft - Kunde (für das Herstellen der Verbindung) und ad 2) Diensteanbieter - Kunde (für die Inhalte).

Letzteres wäre für den Kunden am besten. Er zahlt die reinen Telefonentgelte an die Telefongesellschaft, der Diensteanbieter muss - wir üblich im Zivilrecht - einen eige-

nen Anspruch auf Zahlung seiner Leistung gegenüber dem Kunden haben und geltend machen. Dieser Anspruch muss sich auf einen wirksamen Vertrag stützen.

Die Rechtsprechung der Oberlandesgerichte ist uneinheitlich. Auf der Linie des BGH liegen folgende Urteile:

OLG Saarbrücken, Urteil vom 19.12.2000 Az.: 7 U 160/00-42

Telefonverbindungen sind wertneutral und im Verhältnis zu evt. sittenwidrigen Telefonsexverträgen bloße Hilfsgeschäfte.

OLG Hamm, Urteil vom 27.11.2000 Az.: 17 U 73/2000

Eine etwaige Sittenwidrigkeit von Telefonsexverträgen wirkt sich im Verhältnis des Netzbetreibers zum Kunden nicht aus.

Urteil des OLG Jena vom 11.07.2000 Az.: 9 U 393/00

Telefonverbindungen sind wertneutral und im Verhältnis zu evtl. sittenwidrigen Telefonsexverträgen bloße Hilfsgeschäfte.

Demgegenüber fallen die nächsten Urteile kundenfreundlicher aus:

Urteil des OLG Stuttgart vom 09.05.2001 Az.: 9 U 18/01

Der Kunde schließt mit dem Telefonunternehmen einen Vertrag über eine einheitliche Leistung, die nicht nur ein wertneutrales Hilfsgeschäft darstellt. Der sittenwidrige Inhalt eines Gespräches vernichtet auch diesen Vertrag.

Urteil des OLG Düsseldorf vom 24.04.2001 Az.: 20 U 127/01

Leitungsbetreiber haben keinen Anspruch aus Telefonaten mit sittenwidrigem Inhalt, das Herstellen der Verbindung ist nicht nur bloßes Hilfsgeschäft.

OLG Celle, Urteil vom 29.11.2000 Az.: 21 U 36/00

Telefonnetzbetreiber und Anbieter von Telefonsex über eine 0190-Nummer schließen getrennte Verträge mit dem Telefonkunden.

OLG Düsseldorf, Urteil vom 08.06.1999 Az.: 20 U 100/98

Der sittenwidrige Inhalt eines Telefonsexvertrages ist dem Netzbetreiber zuzurechnen

Bei den hier zitierten Entscheidungen handelt es sich um Urteile zu "normalem" Telefonsex - nicht um die Dialer-Problematik! Es sind bislang auch nicht jene Fälle gerichtlich entschieden worden, bei denen das Anwählen einer 0190-Verbindung durch ein vermeintliches Nebenverdienstangebot, vermeintlichen Gewinn, vermeintlichen privaten Kontakt oder ähnliche Wege provoziert wurde.

Die Dialer-Problematik ist von den Gerichten auch insbesondere in Bezug auf die 0190-0-Nummern noch gar nicht erfasst worden. Hier kann der Kostenrahmen schnell etliche tausend Euro umfassen. Ich bin insgeheim fast ein wenig froh darüber, dass es diese 0190-0-Nummern gibt, denn sie spitzen den Skandal zu und lassen auf eine andere Rechtsprechung hoffen.

Der zur Zeit diskutierte Ansatz, dass

- Telefonfirmen ihre Untermieter zu gesetzmäßigem Handeln verpflichten müssen,
- die Anschriften der Diensteanbieter auf der Telefonrechnung angegeben werden müssen,
- umstrittene Rechnungen nicht mehr eingezogen werden dürfen und
- nach Kenntnis geeignete Maßnahmen zur Unterbindung zu ergreifen sind,

ist wohl nicht falsch, aber nicht ausreichend. Denn diese diskutierten Änderungen spiegeln die aktuelle Rechtslage wider. Die Telekom zieht ohnehin keine umstrittenen Forderungen mehr ein, sondern verschiebt das Problem auf den nächsten in der Kette (wie Talkline u.a.). Bei einem vielstufigen Vertriebssystem gehen Maßnahmen "nach Kenntnis" ins Leere.

Wir als Verbraucherschutz-Organisation fordern deshalb - neben der Forderung nach Änderung der rechtlichen Regelungen - zum Zahlungsboykott auf. Wir müssen nun die betroffenen Kunden in einer verantwortlichen Art darauf hinweisen, was sie erwarten kann: dass sie sich möglicherweise aktiv per einstweiliger Anordnung gegen eine drohende oder durchgeführte Anschlusssperre wehren müssen, dass sie viel-

leicht verklagt werden und möglicherweise auch vor Gericht verlieren werden. Doch Druck auf die Verantwortlichen lässt sich nur durch die Weigerung vieler Verbraucher zur Zahlung der nichtbestehenden Forderungen ausüben. Diese werden dann kalkulieren, wieviel es kostet, in tausenden oder zehntausenden Einzelfällen ihre Forderungen einzuklagen; sie werden überlegen, ob sich dies lohnt; ein Ergebnis könnte eine interne Marktbereinigung sein, nach der es wieder möglich sein wird, das Netz unbefangen und frei zu nutzen. Dass dem bislang nicht so ist, hören wir immer häufiger in unseren Beratungen: Familien überlegen, sich komplett vom Netz abzukoppeln, solange es keine wirksame Garantie gibt, nicht in solche Kostenfallen hineinzustolpern, die bis zur Verschuldung führen können - und das kann nicht in unserem Sinne sein!

2.4.2. Rechtspolitische Problemfelder

Prof. Dr. Thomas Hoeren
Institut für Informations,- Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster

Ich möchte - provozierend - mein Statement mittels dreier Fragen strukturieren:

Welches Internet ist gemeint?
Die Internet-Kommunikation „B2B“, also „Business to Business“ wird praktiziert. Der Austausch „B2C“, also „Business to Consumer“ via Internet hat jedoch derzeit kaum noch eine Bedeutung, und er wird zukünftig noch unbedeutender werden. Das hat zwei Gründe:

- Zum einen die Dialer-Problematik, die auch Frau Castello erwähnt hat. Wenn die Verbraucher nicht wissen, was mit den Dialern auf sie zukommt, werden sie sich aus den Netzen ausklinken.

- Zum anderen wirkt sich die allgemeine Sicherheitsdiskussion in diesem Bereich aus: Es gibt inzwischen erste Urteile der Landgerichte Bonn und Rostock, die besagen, dass e-mails und andere elektronische Nachrichten keinen Beweiswert

haben. Dies macht Bestellungen auf dem elektronischen Weg sowohl für Unternehmen als auch für Verbraucher höchst unsicher: Jedermann kann mit Ihrer e-mail Adresse etwas bestellen, es gibt keine Planungssicherheit. Auch die digitale Signatur ist - entgegen der Äußerungen der Vertreter der Ministerien - tot, weil in der Wirtschaft keine Bereitschaft bestanden hat, in dieses Projekt zu investieren.

Welche Verbraucherschutzverbände sind gemeint?

Ich habe immer den Eindruck, die Verbraucherverbände leben noch im neunzehnten Jahrhundert, und das zeigt sich auch im Statement von Frau Castello: Ein Aufruf zum Zahlungsboykott ist ein ineffizientes, überholtes Instrument.

Als ich begonnen habe, mich mit der Dialer-Problematik zu beschäftigen, habe ich an die Verbraucherschutzverbände geschrieben und zur Antwort bekommen, man könne hier nichts tun, da man nicht wisse, welche Firmen beteiligt seien. Genauso machtlos sind die Verbraucherschutzverbände im Grunde auch heute noch. Sie fallen völlig aus bei der Frage „Privatkopie im Urheberrecht“; dabei ist es das Verbraucherschutzrecht per se, Privatkopien urheberrechtlich geschützt zu machen. Verbraucherverbände sind aber zu diesem Thema nicht aktiv.

Alles, was in Verbraucherschutzgesetzen verabschiedet wurde, ist im Grunde Makulatur, da Missachtung nicht sanktioniert wird. Die Informationspflichten für Homepages werden massiv von der gesamten Wirtschaft missachtet, weil die Abmahnungen dazu fehlen. Den Verbraucherverbänden fehlt es an der technischen Kompetenz und Ausstattung, um diese Verstöße zu verfolgen. Das ist nicht die Schuld der Verbraucherschutzverbände, sondern einer Politik, die den Verbraucherschutzverbänden nicht das Equipment gibt und vielleicht auch gar nicht geben will.

Welche Antworten aus der Politik sind gemeint?

Es gibt keine Antworten aus der Politik. Wir haben eine wirre und völlig konfuse Ansammlung verschiedenster Gesetze zu diesem Thema; wir haben rechtshistorisch zum ersten Mal in Deutschland die Situation, dass ein Gesetz gleichzeitig mit seinem Änderungsgesetz im Bundesgesetzblatt veröffentlicht wird - dies ist ein Symbol für den Wettlauf, der in diesem Rechtsbereich stattfindet.

Als wichtigstes Beispiel für diese These noch einmal die Dialer-Problematik: Ansprechpartner muss - entgegen der Ansicht von Frau Castello - die Regulierungsbehörde für Telekommunikation und Post sein, um das Problem langfristig zu lösen. Denn es geht nicht nur um die Dialer-Problematik, es geht um das Selbstbild einer großen, mächtigen Behörde, die das Selbstverständnis hat, nur für technische Nummerierungen, aber nicht für die darüber transportierten Inhalte zuständig zu sein. Dieses Selbstverständnis ist schlichtweg falsch. Wir müssen die Regulierungsbehörde daran erinnern, dass sie es mit lizenzpflichtigen Telekommunikationsanbietern zu tun hat, denen sie Auflagen bspw. für die Untervermietung der Nummern machen kann.

In diesem Punkt kann man die Änderung der TKV begrüßen, da die 0190er-Problematik künftig aufgenommen wird und damit deutlich wird, dass die Regulierungsbehörde als Überwachungsorganisation für die TKV aktiv werden muss. Die TKV-Änderung selbst - und da stimme ich Frau Castello zu - ist Augenwischerei. Denn für die eingebrachte Sperrungsverpflichtung bei mehrmaligem Missbrauch einer Nummer sind die Sanktionen nicht geregelt.

Die TKV-Änderung sieht auch vor, dass auf der Rechnung angegeben wird, dass es eine Einwendungsmöglichkeit gibt und dass auf das Recht, die Forderung zu verweigern, hingewiesen wird. Doch auch für diese Pflichten sind die Sanktionen nicht geregelt. Es gäbe Sanktionen - und hier schließt sich der Kreis, wenn die Verbraucherschutzverbände endlich begreifen würden, dass sie hier eine Abmahnbefugnis haben und sie auch dementsprechend künftig ausnutzten.

Auch weitere politische Antworten in anderen Bereichen sind ebenso unbefriedigend, wie bspw. die falsche Umsetzung der Fernabsatzrichtlinie, die über 35 Informationen auf einer Home Page vorsehen. Die Darstellung der Handelsregisternummer, der Umsatzsteuernummer - welchem Verbraucher ist eigentlich damit gedient? Das hat mit einer sinnvollen Planung von Verbraucherschutz aus meiner Sicht nichts zu tun.

2.4.3. Antworten von Politik und Gesetzgebung

Jella Teuchner, MdB
Verbraucherpolitische Sprecherin der SPD-Bundestagsfraktion, Berlin
(in Abwesenheit, schriftliche Stellungnahme)

Politik und Gesetzgebung müssen die gesetzlichen Rahmenbedingungen schaffen, die einerseits der Förderung des Internet dienen und andererseits das Vertrauen der Verbraucher in die neuen Medien stärken.

Die Verbraucher müssen auf einen sicheren und fairen Umgang vertrauen können. Allen Beteiligten muss klar werden, dass starke Verbraucherrechte das Vertrauen stärken und so auch den Unternehmen zugute kommen.

Politik und Gesetzgebung haben in den Jahren unserer Regierungsverantwortung viele Antworten auf ungelöste Fragen gegeben. Es wurden entscheidende Maßnahmen für mehr Rechtssicherheit und für mehr Verbraucherschutz ergriffen.

Es hat sich auch gezeigt, dass vor allem der europäische Gesetzgeber gefordert ist, einheitliche Regelungen zu schaffen. Denn das grenzüberschreitende Medium Internet verlangt grenzüberschreitende Rechtsklarheit. Deutschland hat, im Gegensatz zu 12 anderen Ländern, Gesetze zur fristgerechten Umsetzung der e-commerce-Richtlinie verabschiedet:

- Das EGG (Elektronischer Geschäftsverkehr-Gesetz) mit Änderungen des Teledienstegesetzes und des Teledienstedatenschutzgesetzes.

Dazu gehören auch:

- Das Signaturgesetz (16.02.01) sowie das Gesetz zur Anpassung der Formvorschriften im Privatrecht; damit können elektronische Signaturen Wirkungen im Rechtsverkehr erzeugen;
- Die Abschaffung von Rabattgesetz und Zugabenverordnung,
- Die Änderung der Verwaltungsverfahrensgesetze des Bundes zur Zulassung elektronischer Dokumente.

In Umsetzung der e-commerce-Richtlinie und der Fernabsatzrichtlinie haben wir für hinreichenden Verbraucherschutz gesorgt. Dem Diensteanbieter sind bestimmte Informationspflichten gegenüber dem Verbraucher auferlegt (§ 305 ff. BGB). Auch das viel kritisierte Herkunftslandprinzip findet keine Anwendung auf den Bereich der vertraglichen Schuldverhältnisse in Bezug auf Verbraucherverträge.

Die Bundesregierung hat einen modernen Rechtsrahmen geschaffen zur Förderung des Internet. Diese Bedingungen müssen die Unternehmen nutzen, um beispielsweise die digitale Signatur in der Geschäftswelt voran zu bringen. Auch im Bereich der Internet-Zahlung müssen wir gemeinsam an Projekten arbeiten, die das Problem der Vorkasse lösen können.

Deutschland muss weiter auf EU-Ebene für seinen hohen datenschutzrechtlichen und wettbewerbsrechtlichen Standard werben. Bei einer anstehenden Harmonisierung des Wettbewerbsrechts und des Verbraucherschutzrechts müssen wir uns für ein hohes Schutzniveau einsetzen. Die SPD steht hier beispielsweise weiter für ein Verbot gesundheitsbezogener Werbung, wie es in Deutschland gilt.

Wir müssen für eine weite Informations- und Aufklärungsvermittlung Sorge tragen. Aufgeklärte und informierte Internetnutzer wissen, welche Gefahren im Internet lauern und geben unseriösen und kriminellen Unternehmern wenig Chancen. Der Selbstschutz spielt also eine große Rolle.

Für ein Gelingen des „Unternehmen Internet“ sind alle gesellschaftlichen Kräfte aufgerufen, mitzuarbeiten.

3. Diskussion und Ausblick

Ist das Internet sicher? Wie schon der Titel der Tagung vermuten lässt, kann die Frage in dieser Pauschalität allenfalls mit einem klaren „(un-)sicher“ beantwortet werden. Sowohl angesichts rund einer halben Milliarde überwiegend „gutartiger“ Seiten im WWW als auch der in aller Regel unbedenklichen Kommunikation in Foren, Chatrooms usw. ist das Internet mit Sicherheit weit davon entfernt, vorrangig Tummelplatz für Kriminelle zu sein. Andererseits zeigen die offiziellen Statistiken, bspw. die Polizeiliche Kriminalstatistik (PKS), sowohl für den eher konventionellen Bereich des Computerbetrugs als auch für neuartige Problemstellungen im Bereich der Computersabotage oder der Datenveränderung deutlich steigende Tendenz.

Dass die Kriminalstatistik zudem nur die Spitze des Eisbergs markiert, weil die weitaus meisten Vorfälle entweder gar nicht erkannt, aus Imagegründen nicht angezeigt oder wegen fehlender Ermittlungsmöglichkeiten nicht verfolgt werden, verschärft die Problematik um Einiges. Selbst die gelegentlich geäußerte Einschätzung, das Internet sei zumindest sicher für diejenigen, die nicht „drin“ sind - die also aus welchen Gründen auch immer über gar keinen Internet-Anschluß verfügen - lässt sich nicht aufrecht erhalten. Wer eine Kreditkarte besitzt, eine Bahncard oder Ähnliches, ja selbst jeder Kontoinhaber oder Inhaber eines Telefonanschlusses taucht in den globalen Datennetzen auf, ob er will oder nicht.

Handlungsbedarf ist also dringend gegeben, sowohl bei den während der Tagung ausführlich diskutierten Problemen mit 0190-Dialern als auch in jeglicher anderer, politischer, rechtlicher wie wirtschaftlicher Hinsicht. Nun ist nicht nur für das Internet selbst eine kaum fassbare Komplexität charakteristisch, sondern erst recht für die mit dem Netz der Netze verbundenen Auswirkungen auf unser tägliches Leben. Man könnte also versucht sein, eine Diskussion über die Technik-Geister zu führen, die wir gerufen haben und von denen wir immer noch nicht so genau wissen, ob wir sie nun brauchen oder doch besser wieder loswerden wollen. Leider gibt Goethe an dieser Stelle keine brauchbare Antwort, denn angesichts eines klaren Feindbildes (Besen) und bevorstehender Überschwemmung fällt dem Zauberlehrling zum einen die

Entscheidung dafür oder dagegen leicht und zum anderen gibt es den Meister, der alles wieder richtet.
Beides passt wenig zum Internet, wenngleich auch hier der Wunsch nach Vereinachung so manches Feindbild nährt (bspw. das des allmächtigen Überwachungstaats) und so manchen Guru hervorgebracht hat. Um dem Bedarf nach Reduktion von Komplexität einerseits und der Vermeidung von Stereotypen andererseits gerecht zu werden, wird das Thema der Tagung im Folgenden entlang einiger zentraler Fragen diskutiert und kommentiert werden, aufbauend auf den Vorträgen und unter Einbeziehung der Diskussionsbeiträge während der Tagung.

Frage 1: Welche technischen Schutzmöglichkeiten stehen zur Verfügung und was können sie bewirken?

Das Spektrum der Einschätzungen reicht hier von Lobgesang bis Fundamentalkritik, wobei im Laufe der Tagung eine vorsichtige, eher kritische Einschätzung überwogen hat. Fest steht, dass in der Tat eine solche Vielzahl einzelner technischer Schutzmechanismen häufig sogar kostenlos zu erhalten sind, dass eher die Auswahl als die Verfügbarkeit ein Problem darstellt. Andererseits liefern die Experten gewichtige Argumente dafür, dass der Datenaustausch im Internet gerade aufgrund dessen konstruktiver Eigenschaften quasi zwangsläufig unsicher ist, und dass das Internet auch mit den verbreiteten Instrumenten wie Firewall oder Virenscanner nicht wirklich sicher gemacht werden kann.

Der Vertreter des Chaos Computer Club (CCC), Jens Ohlig, spart in diesem Zusammenhang nicht an beeindruckenden Erfahrungen und Kritik. Das Hauptproblem besteht für ihn darin, dass Menschen Produkte anwenden, die sie nicht überblicken (können); so entstünden paradoxe Situationen wie die, dass Patientendaten und Medikationen auf den Straßen von Berlin relativ leicht und vollkommen legal mitgelesen werden konnten. Er geht davon aus, dass hier wie auch bei anderen Sicherheitslücken mit technischen Lösungen allenfalls Brände gelöscht, aber das eigentliche Problem nicht beseitigt werden kann. Für ein gesellschaftliches Problem fordert er eine gesellschaftliche Lösung. Wichtig sei eine Kultur der Technikfolgenabschätzung, denn es gehe nicht nur um das „Know-How“, sondern auch um das „Know-Why“.

Grundsätzlich skeptisch zeigt sich auch der Hamburger Informatikprofessor Klaus Brunnstein und betont, dass kein Artefakt des menschlichen Geistes je ohne Risiko sein wird und dass es wohl immer seine Zeit brauche, bis die Menschen gelernt haben, halbwegs vernünftig mit einer neuen Technologie umzugehen: Sowohl von der revolutionären Erfindung der Dampfmaschine bis zur Einführung durchgehender Qualitätsstandards[5] als auch von der Erfindung des Autos bis zur (akzeptierten) Erkenntnis seiner massiven Unsicherheiten[6] dauerte es jeweils rund 80 Jahre.

Da diese Zyklen weniger von der Art der Technik als vielmehr von der Fähigkeit der Menschen zur Reaktion auf tiefgreifende Veränderungen bestimmt werden, spricht Einiges dafür, dass auch bei der Informationstechnologie ein akzeptables Qualitätsniveau kaum vor dem Jahr 2020 erreicht werden kann[7]. Bis dahin wird es noch eine Reihe von Rückschlägen zu bewältigen geben, und zumindest stellenweise wird auch immer wieder das Recht des Stärkeren gelten – sowohl jeder Einzelne als auch die Gesellschaft im Ganzen sind also gut beraten, sich aktiv stark zu machen, um nicht zu den Verlierern zu gehören.

Inwieweit hier Forderungen nach einem zweiten, sicheren (Regierungs-)Netz, wie sie vor allem auch in den USA immer wieder diskutiert werden (sog. Govnet-Debatte), wirklich zu mehr Sicherheit führen, darf bezweifelt werden. Professor Klaus Brunnstein und andere Tagungsteilnehmer sehen darin fast einen Königsweg. Jens Ohlig, der Vertreter des CCC, hingegen führt aus, dass das Prinzip „security by obscurity“ vollkommen überholt und durch die Realität oft widerlegt sei. Sicherheitsmängel würden dadurch behoben, dass man mit möglichst vielen Leuten rede und möglichst mit offenen Karten spiele. Die Wahrheit liegt vermutlich in der Mitte. Natürlich wäre es naiv, jedem alles offen zu legen, aber „möglichst“ mit offenen Karten zu spielen, bedarf eben der individuellen Entscheidung im Einzelfall. Ein eigenes, feststehendes Netz hingegen, von dem jeder weiß, dass es sensible Information in besonderer Konzentration erhält, zieht zweifellos besonderes Interesse auf sich – nicht umsonst gehört es zu den ältesten Geheimdienstprinzipien, neben dem Verbergen wirklich wichtiger Information auch weniger wichtige Information anzubieten, um Vertrauen zu erwecken oder abzulenken.

[5] Gründung des Dampfkesselüberwachungsvereins als Vorläufer des heutigen TÜV
[6] vgl. die Arbeit „unsafe at any speed“ von Ralph Nader
[7] den Anfang datiert durch die Erfindung der Z3 durch Konrad Zuse im Jahre 1941

Selbst wenn es technisch durchsetzbar wäre, den Datenstrom vom Moment der Eingabe[8] bis zur Ausgabe der Botschaft beim (hoffentlich richtigen) Empfänger mit angemessenem Aufwand sicher zu gestalten, so bliebe doch das Problem, dass am einen wie am anderen Ende und auch dazwischen Menschen sitzen, für die das sogenannte menschliche Versagen durchaus arttypisch ist. Da man bekanntlich am schwächsten Glied der Kette angreift, um zu dem zu kommen, was man so heiß begehrt, böte sich hier immer noch ein umfassendes Feld für vielfältigste Aktivitäten.

Doch nicht nur der Staat steht vor schwierigen Fragen, wenn es um technische Lösungen geht: So sehr im Grunde die Fundamentalkritik an der technisch-strukturellen Sicherheit des heutigen Internet berechtigt scheint, so wenig hilft sie auch dem Verbraucher oder Unternehmer weiter, der vor konkretem Entscheidungsbedarf steht. Er kann sich ein anderes, sicheres Internet nicht stricken und muss nehmen, was da ist – oder die Finger vom Internet lassen.

Letzteres hält der Vertreter des BMWi, Dr. Ulrich Sandl für wirtschaftspolitisch sehr gefährlich - und in einer Zeit, in der der Verband Bitcom erstmals sinkende Umsatz- und Gewinnzahlen für den Hoffnungssektor IT mitteilt, mag man ihm nur ungern widersprechen. Gleichwohl wird sich der Bürger wenig um abstrakte wirtschaftspolitische Erwägungen kümmern, wenn er befürchten muss, dass es ihm an die (Geld-)Börse geht, bspw. durch 0190-„Abzocker“ und andere schwarze Schafe. Hier sind Politik, Genehmigungsbehörden und Wirtschaft schon in der technischen und organisatorischen Gestaltung gut beraten, präventiv vorzugehen und Verbraucherschutz besonders ernst zu nehmen.

So kann es bspw. nicht angehen, die heute schon für viele Verbraucher weitgehend undurchschaubare Gestaltung von 0190-Nummern zu Abrechnungszwecken mit der zukünftig beabsichtigten Einführung von 0900–Nummern noch undurchschaubarer zu machen, indem nicht nur Summen, sondern auch Zeittakte weiter flexibilisiert werden. Statt dessen wäre es – über die auf der Tagung diskutierten Maßnahmen hinaus[9]- eine klare präventive Maßnahme, die Summen strikt nach oben zu begren-

[8] weiter durch das komplexe Innenleben eines Rechners über komplexe globale Pfade und verschiedenste Server und Datenbanken bis zum wiederum komplexen Rechner des Empfängers, von dort zum Bildschirm oder zum Drucker ...

[9] vgl. Zusammenfassung

zen (0900-Nummern lediglich für sog. Micropayment bis zu Beträgen von wenigen Euro) und die Vergabepraxis so zu gestalten, dass Nummern nicht beliebig weiter zu vermieten sind und eine gewerbliche Zulassung erforderlich wird.

Insgesamt herrscht weitgehend Übereinstimmung in der Einschätzung, dass technische Maßnahmen zwar nicht zu vernachlässigende Hilfsmittel darstellen, aber keinesfalls geeignet sind, die Problematik strukturell und nachhaltig zu entschärfen. Die geforderte Kultur der Technikfolgenabschätzung macht mehr Sinn denn je – wenngleich das Instrument zumindest im öffentlichen Bereich spätestens seit den 90er Jahren allenfalls im Range eines Feigenblatts steht.

Schnittstellen zwischen den Beteiligten müssen geschaffen, Foren müssen eingerichtet werden: So treffen sich bspw. jedes Jahr die Experten des CCC im Rahmen eines Kongresses, um über wahrscheinliche Sicherheitsrisiken des kommenden Jahres zu debattieren. Noch sehr viel intensiver werden solche Foren in den USA kultiviert, genannt sei nur der jährlich stattfindende große DEFCON-Kongress[10], wo Hacker debattieren, aber über die Wirtschaft bis hin zu Regierungsvertretern auch alle anderen Schattierungen vertreten sind. Möglicherweise schlummert auf dieser Ebene ein Potenzial, dem sich auch die etablierten Strukturen mittels Förderung derartiger „Spielwiesen“ nähern sollten.

Perfekte Sicherheit ist in der Tat nicht zu erreichen, aber sofern durch Maßnahmen der technischen Prävention ein akzeptabler Schutzstandard für Bürger und Unternehmen zu erreichen ist, der die Wahrscheinlichkeit und Dimension von Schadensereignissen entscheidend begrenzt – und danach sieht es durchaus aus, so können Internet und Mobilkommunikation aus diesem Blickwinkel heraus als genügend sicher bezeichnet werden. Voraussetzung dafür ist allerdings neben dem reinen Vorhandensein der technischen Schutzmaßnahmen auch deren zielgerechte Anwendung. Dazu müssen nichttechnische Rahmenbedingungen und Mindeststandards erfüllt sein – von Rechtssicherheit bis zum Wissen um den Nutzen und die Sinnhaftigkeit einzelner Produkte.

[10] siehe www.defcon.org

Frage 2: Wie haben sich die bereits bestehenden Sicherheitsregelungen und -konzepte politischer und rechtlicher Art bewährt?

Einerseits verändern Neue Technologien unser Alltagsleben mit einer nie dagewesenen Schnelligkeit und Intensität. Andererseits ist unser Rechtsapparat schwerfällig – teils berechtigt, denn schließlich können nicht im Wochenrhythmus neue Gesetze erlassen und alte verändert werden[11], ohne zentrale Werte wie Gerechtigkeit oder Zuverlässigkeit als gemeinsame Verhaltensnormen der Gesellschaft in Frage zu stellen. Insofern können sich bereits bestehende Regelungen allenfalls auf der Ebene von Grundwerten bewähren; in allen anderen Bereichen besteht zwangsläufig permanenter Anpassungsdruck. Selbst bei den Grundwerten ergeben sich aber schon vielfältige Spannungen, bspw. beim Brief-, Post- und Fernmeldegeheimnis (Artikel 10 Grundgesetz), etwa wenn es um die Abwägung von Einschränkungen der Kommunikationsfreiheit geht, um ein Mindestmaß an Sicherheit gewährleisten zu können. Insgesamt wird eine dynamische Weiterentwicklung solange erforderlich bleiben, wie sich Neue Technologien weiter rapide entwickeln und verbreiten.

Beispielhaft kann hier die Open-Source-Debatte genannt werden: Professor Klaus Brunnstein zufolge stellt Open-Source-Software (OSS) im Grunde eine „unzulässige“ Sozialisierung von Werten dar, die von Einzelnen geschaffen wurden; dies entspreche nicht unserer Wirtschaftsform. Die Verfahren der hochkomplexen Informationstechnik könnten so nicht auf der sonst in der Industriegesellschaft üblichen Grundlage „Mehrwerterzeugung im Wettbewerb“ ablaufen. Wettbewerb sei aber wichtig, denn nur auf dieser Basis könne beherrschbare Software entwickelt werden und sich durchsetzen.

Patentschutz auf technische Entwicklungen, so entgegnet der Vertreter des BMWi, Dr. Ulrich Sandl, habe bei der Entscheidung der Bundesregierung für OSS eine Schlüsselrolle gespielt, und es wurden dazu einige Gutachten eingeholt. Entwicklungen des Industriezeitalters könnten jedoch nicht einfach ins Informationszeitalter fortgeschrieben werden. Transparenz sei letztlich wichtiger, und die Bundesregierung gehe davon aus, dass der jetzige Diskussionsstand zukunftsweisend und nicht rückwärtsgewandt - wie bei einem Vergleich mit Mechanismen der Industriegesellschaft - ist. Der Schutz berechtigter wirtschaftlicher Interessen, wie bspw. die intensive Inves-

tition in die Entwicklung von Algorithmen für Kryptoprodukte, ist auch aus Sicht des Innenministeriums ohne Zweifel legitim. Es gebe keinen diametralen Gegensatz zwischen der Nutzung von OSS und Patentschutz; auch weiterhin sei es selbstverständlich, dass mit Software Geld verdient werden könne.

Insgesamt muss es also zukünftig weniger darum gehen, dauernd neue Normen zu entwickeln oder alte im statischen oder linearen Sinne anzupassen. Vielmehr gilt es, Entwicklungsziele festzulegen und Verfahrensregeln zu definieren, wie diese Entwicklungsziele erreicht werden können. Dazu gehören zweifellos auch klare Aussagen und ggf. Sanktionen, wie mit denjenigen umzugehen ist, die diese Entwicklungsziele nicht mittragen oder die Verfahrensregeln missachten. In diesem Sinne mahnt eine Teilnehmerin Optimierungen unter dem Stichwort Konvergenz an: Da verschiedene Techniken und Wirtschaftsbereiche zusammenwüchsen, müssten auch verschiedene Rechtsbereiche zusammengeführt werden. Im Bereich der Haftungsregelungen für Provider und der weitgehenden Haftungsfreistellung für Softwaremängel müsse man europäisch und international arbeiten. Auch der Vertreter des BMWi hält die tabufreie Auseinandersetzung mit diesen Themen für wichtig.

Ein weiterer zentraler Aspekt, wenn es darum geht, wie sich bereits bestehende Regelungen bewährt haben, ist die Datenschutzgesetzgebung. Hier hat sich im vergangenen Jahrzehnt eine Frontlinie erhalten, die woanders schon lange keine Rolle mehr spielt: Aus Sicht mancher Datenschützer geht es offenbar immer noch vorrangig darum, personenbezogene Daten vor einem übermächtigen Schnüffelstaat zu bewahren. Die wahren Auseinandersetzungen dagegen spielen sich schon lange auf anderer Ebene ab, etwa beim Data Mining im Bereich des wirtschaftsorientierten Ausspähens von Verbrauchern12.

Wo ist die Balance zwischen den Risiken, vor denen der Staat mich schützen muss, und den Risiken, vor denen ich mich selber schützen muss? Die Balance zwischen Freiheit und Schutz muss in der Wissensgesellschaft neu geschaffen werden, fordert Professor Klaus Brunnstein. Diese Forderung unterstützen sicherlich auch Referen-

[11] Wenngleich, wie Prof. Hoeren treffend bemerkt, genau dies einzutreten droht: Er erwähnt die rechtshistorisch in Deutschland einmalige Situation, dass ein Gesetz mit einem diesbezüglichen Änderungsgesetz im Bundesgesetzblatt gleichzeitig veröffentlicht wurde.

[12] (siehe auch Frage 3).

ten und Teilnehmer der Tagung, dennoch definiert jeder die Balance ein wenig anders.

Aus Sicherheitsgründen müssen nach seiner Einschätzung Daten gespeichert werden, die auch personenbezogen interpretiert werden können, da es sein könne, dass etwas, was in einem Augenblick passiert, sich erst später in der Analyse als gravierender Angriff herausstellt. Dies sei ein inhärentes Risiko der heutigen Technik. Er plädiert dafür, die Technik dabei so zu gestalten, dass der Datenschutz besser berücksichtigt werden kann. Doch das Risiko, dass die eigenen Bewegungen im Netz verfolgt werden können, müsse jedem Nutzer klar sein.

Nach Ansicht des BMWi-Vertreters Dr. Ulrich Sandl sollte versucht werden, einen Interessenausgleich herbeizuführen. Zwar seien Wirtschaftsinteressen auf ein hohes Datenschutzniveau ausgerichtet, nicht zuletzt weil gespeicherte Daten Speicherplatz benötigen und damit einen kommerziellen Nachteil bedeuten. Aber auch die Interessen der Strafverfolgungsbehörden hätten eine Schnittmenge zu Wirtschaftsinteressen, denn die Wirtschaft ist auf Sicherheit im Internet angewiesen.

Dem widerspricht der Hamburger Datenschützer Peter Schaar: Aufgrund der Komplexität der Materie könne der normale Nutzer die Risiken nicht abschätzen. Eine gesellschaftliche Schieflage erschwere zudem gegenwärtig die angemessene Berücksichtigung des Datenschutzes. Die Grundstimmung in der Gesellschaft räume derzeit der Sicherheit einen höheren Wert ein als den Freiheitsrechten. Der Politik wirft er vor, diese Grundstimmung zu bedienen, statt die Diskussion zu versachlichen, und insbesondere nach dem 11. September nicht ausgereifte Sicherheitsgesetze zu verabschieden. Eine Chance zur besseren Balance sieht er in der, auch von der Politik zu tragenden, Versachlichung der Diskussion sowie in einer Evaluation von Gesetzen, damit nicht Fakten geschaffen werden, die über aktuelle Bedrohungsszenarien und -empfindungen hinausgehen und dann unwiderrufen Bestand haben. Weiter mahnt er eine Harmonisierung der Datenschutzgesetzgebung an.

Eine Polemik gegen Datenschützer[13] seit dem 11. September, wie sie von mehreren Tagungsteilnehmern angesprochen wird, kann wiederum Christoph Verenkotte, der Vertreter des BMI, nicht erkennen; er hält sie auch für völlig fehl am Platz. Im weiteren weist er (zu Recht) darauf hin, dass der Innenminister nicht jeden Einzelnen persönlich davor schützen könne, Opfer einer Straftat zu werden - dass also Eigenverantwortung im Internet zwangsläufig groß geschrieben werden muss und die Erwartungshaltung an den Staat oder auch die IT-Unternehmen sich am Möglichen orientieren müsse. Er spricht sich aber auch für die besondere Verantwortung der Regierung aus, die sich selbst unter Zugzwang hin zu mehr Sicherheit setze, wenn sie tatsächlich bis 2005 erfolgreich ihre Dienstleistungen im Netz anbieten will (Bund Online 2005).

Frage 3: Wo besteht weiterer Handlungsbedarf für staatliche Eingriffe und Regularien?

Vordringlicher Handlungsbedarf wird von etlichen Referenten und Teilnehmern bei der Dialer-Problematik gesehen. Der Kommunikationsrechtsexperte der Universität Münster, Professor Thomas Hoeren, vergleicht den rechtlichen Stand hierzu mit dem bekannten Wettlauf von Hase und Igel. Dabei hat er für eine nationale Lösung einen Ansatz parat: Zum Einen müsse die Regulierungsbehörde ihre Verantwortung begreifen, zum Anderen die „Mitstörerhaftung“ eingeführt werden, d.h. alle, die in der Kette verdienen, sind Mitstörer im juristischen Sinne. Letzteres wurde bereits in einem allerdings bis heute nicht rechtskräftigen Urteil des Amtsgerichts Nidda angedacht.

Die Hamburger Verbraucherschützerin Edda Castello begrüßt die auch von der Verbraucherzentrale angedachte Mitstörerhaftung, verweist jedoch auf zwei Entscheidungen des OLG, bei denen dieser Ansatz verneint wurde. Insofern gebe die Rechtsgrundlage für die Verbraucherschützer derzeit keinen Anlass, mit Optimismus in - teure - Verfahren einzusteigen. Es macht nach ihrer Einschätzung ebenso wenig Sinn, einzelne Unterlassungserklärungen gegen windige Geschäftemacher zu erwir-

[13] Zweifellos ist aber wohl Polemik bei den Datenschützern selbst im Spiel, wenn bspw. der Landesdatenschutzbeauftragte von Schleswig-Holstein mit Blick auf die Sicherheitsbehörden und den Bundesrat im Internet zu einer Aktion „Rote Karte für Internetschnüffler“ aufruft.

ken. Zur strukturellen Lösung des Problems müsse bei dem Ersten angesetzt werden, der an diesem Geschäft verdient.

Während Professor Thomas Hoeren seine Einschätzung, dass die Regulierungsbehörde der einzig richtige Ansprechpartner sei, damit untermauert, dass diese gehandelt habe, nachdem sie auf seinen Aufruf in der Neuen Juristischen Wochenzeitung hin selbst Empfänger von massenhaft unerwünschter Faxwerbung wurde, gibt Verbraucherschützerin Edda Castello zu bedenken, dass dies nur ein kleiner Teilerfolg sei, da im Bereich der 0190-Nummern eine Verlagerung zu provozierten Kontakten per Handy auftrete. Sie schlägt demgegenüber einen zivilrechtlichen Ansatz vor, der die zwei Dienstleistungen, nämlich die Bereitstellung der Möglichkeit zu telefonieren und das inhaltliche Angebot des Diensteanbieters, trennt. Das Angebot des Diensteanbieters wiederum soll bestimmten Anforderungen genügen: Es soll vertraglich geregelt sein, eine Vereinbarung über den Preis enthalten und weder wucherisch noch sittenwidrig sein. Auch favorisiert sie die praktische Umsetzung des § 18 TKV: Dort ist vorgesehen, dass man die Gesamtsumme, für die man monatlich telefonieren möchte, im Voraus festsetzen lassen kann. Leider existiert dieser Weg bislang nur auf dem Papier; die praktische Umsetzung steht noch aus. Um all dies zu erreichen, hält die Verbraucherschützerin Edda Castello den Aufruf zum Zahlungsboykott für das Mittel der Wahl.

Der Betreiber der Seite www.dialerschutz.de, Sascha Borowski, zeigt auf, dass sich derzeit jeder mit geringem Zeitaufwand einen Web-Dialer mit entsprechender Nummer bei einem Mehrwertdiensteanbieter mieten kann. Die konkrete Nummernvergabe muss seiner Meinung nach restriktiver gehandhabt werden. Eine Teilnehmerin weist darauf hin, dass es sich um verschiedene Vergabeverfahren in verschiedenen Bereichen (Telekommunikationsdienste/ Medienangebote/ Tele- und Mediendienste) und mit verschiedener Zielrichtung handelt.

Sascha Borowski würde grundsätzlich eine freiwillige Selbstkontrolle präferieren, weist jedoch darauf hin, dass diese in der Vergangenheit nicht funktioniert hat. Die Änderung der Telekommunikations-Kundenschutz-Verordnung sei Anfang Juni 2002 erfolgt. Danach darf bzw. muss die Telekom das Inkasso bei strittigen Beträgen nicht mehr übernehmen. Doch als Betroffener lande man dann nur eine Stufe tiefer in der

Kette und kommt an den eigentlichen Anbieter nach wie vor nicht heran. Der Dialerschutzexperte fordert mehr Transparenz, indem der Netzbetreiber verpflichtet werden müsse, dem Nutzer mitzuteilen, wer das Geld fordert. Eine potenzielle Verantwortung der Telekom für die Inhalte der Anbieter verneint er mit Verweis auf ein Urteil des Landgerichts Berlin aus dem Jahr 2001, welches besagt, dass die Leitungsherstellung völlig wertneutral ist.

Der Journalist Burkhard Plemper, Moderator der Tagung, weist darauf hin, dass vor einigen Jahren dieses Thema auch bzgl. der Telekom diskutiert wurde. Im Anschluß an diese Diskussion war es möglich und ist heute selbstverständlich, als Kunde bspw. einen Einzelverbindungsnachweis zu erhalten.

Ein Teilnehmer erläutert, dass die Rechtsprechung dazu neigt, aus der Technik, mit der die Verbindungsdaten im Telefonverkehr ermittelt werden, einen Beweis des ersten Anscheins zu erheben, d.h. es spricht die allgemeine Lebenswahrscheinlichkeit dafür, dass diese Daten richtig sind, da die Technik ausgereift ist. Daraus folgt, dass derzeit nicht die Telekom, sondern der Telefonkunde nachweisen muss, dass ein Fehler vorliegt. Die gleiche Problematik liegt auch bei Dialern vor. Der Teilnehmer fordert, dass derjenige, der die Beträge geltend macht, nachweisen soll, dass gemäß der Preisangabenverordnung ordnungsgemäß über die Installation eines Dialers und die entsprechenden Kosten informiert wurde. Seitens der Verbraucherschutzverbände führt der Bundesverband derzeit entsprechende Gespräche mit der Regulierungsbehörde. Der Teilnehmer fordert hier eine gesetzliche Regelung im BGB.

Die Regeln zum Telefonieren mit den zukünftig zu verwendenden 0900-Nummern sind noch nicht an die Verbraucher verteilt. Noch haben also die Regulierungsbehörde und das Wirtschaftsministerium Zeit, hier für die Zukunft mögliche Sicherheitslöcher zu stopfen und offensichtliche Missbrauchspotenziale zu verhindern. Auch die TKV kann zu Beginn der neuen Legislaturperiode überarbeitet werden, ohne im vielstimmigen Chor der verschiedenen Interessengruppen bis zur Wirkungslosigkeit des kleinsten gemeinsamen Nenners abgeschwächt zu werden.

Gelegenheit zum Verbessern, wie das Beispiel der Web-Dialer aufzeigt, gibt es also reichlich. Darüber hinaus ist die Harmonisierung der aktuellen rechtlichen Regelungen mit dem Ziel der Schaffung eines Rahmens, der geeignet ist, das Vertrauen in

die neuen Medien zu stärken, überfällig. Dabei sollte der verbraucherfreundlichen Regelung von Haftungsfragen hohe Priorität eingeräumt werden.

Frage 4: Was ist von Vertrauensinstanzen und freiwilligen Selbstverpflichtungen zu halten?

Professor Thomas Hoeren hält sowohl die Nutzung des Internet für Kommunikation mit Kunden (sog. B2C, Business to Consumer) für ein Auslaufmodell als auch die Public Key Infrastruktur (PKI) als Vertrauensinstanz. Als Indizien für diese Entwicklung nennt er u.a. die Dialer-Problematik sowie die durch Landgerichtsurteile bekräftigte Auffassung, dass elektronische Nachrichten unter den derzeitigen Rahmenbedingungen keine Beweiskraft haben. Aber auch die mangelnde Bereitschaft der Industrie, gemeinsame und nutzerfreundliche Standards für die PKI marktreif anzubieten, trage zum Ende bei.

Versäumnisse bei dem Versuch, die Sicherheit im Internet als Grundlage für Vertrauen zu erhöhen, macht er sowohl bei der Politik als auch bei den Verbraucherverbänden aus. Erstere reagierten nicht zielgerichtet im Wettlauf mit dem technischen Fortschritt, wie die Änderung der TKV und die Umsetzung der Fernabsatzrichtlinie zeigten. Letztere vernachlässigten - auch aufgrund des evidenten Mangels an Ressourcen - ihre eigentlichen Aufgaben zum Schutze des Verbrauchers, wie bspw. die Ausschöpfung ihrer Abmahnbefugnisse. Als Konsequenz fordert er über die Dialer-Problematik weit hinaus gehend Verbraucherschutzkonzepte für die gesamte Internet-Problematik. Die Verbraucherverbände müssen hierzu seiner Meinung nach besser mit Geld und Kompetenz ausgestattet werden und ihren bisherigen Auftrag über klassische Themen ausweiten. Die Vertreterin der Verbraucherzentrale mahnt ergänzend eine Rechtsprechung an, die die Dialer-Problematik angemessen würdigt.

In der Diskussion weist ein Teilnehmer auf die aktuellen Anstrengungen Belgiens zur Einführung der elektronischen Signatur hin, die nach seiner Einschätzung Alltägliches, wie den Eintrag im Melderegister, für den Bürger wesentlich vereinfachen könne. Der Teilnehmer regt dies auch für Deutschland an, was von Christoph Verenkotte als Vertreter des BMI prinzipiell begrüßt wird: Auch die Bundesregierung setze sich seit langem für Weiterentwicklungen im Bereich der elektronischen Signatur ein. Doch aufgrund der noch nicht ausgereiften Technik sei es derzeit nicht sinnvoll, Vor-

reiter zu sein und weitreichende Entscheidungen zu treffen, sondern zunächst gelte es, Erfahrungen zu sammeln. Er verweist auf das gerade einige Tage alte Signaturbündnis, von dem er sich erhofft, den bisherigen technologischen Vorsprung in Deutschland zu halten. Grundsätzlich haben für ihn PKI und digitale Signatur die höchste Priorität. Professor Klaus Brunnstein stellt ergänzend klar, dass Deutschland weltweit das erste Signaturgesetz vorgelegt hat, die Industrie aber ihre Chancen nicht genutzt habe, da alle heutigen Systeme hochgradig inkompatibel und nicht interoperabel sind. Auch er hält die Technik noch nicht für ausgereift, doch es handele sich um eine wichtige Technologie der Zukunft. Die Entwicklung von interoperablen Strukturen gehöre jedoch in die Verantwortlichkeit der Industrie, nicht der Bundesregierung.

Beim Thema Vertrauensinstanzen spielt schließlich auch die Zertifizierung von Produkten durch das BSI eine gewichtige Rolle. Das BSI zeigt auf seiner Homepage von ihm zertifizierte Produkte an, wobei die Zertifizierung sich nach Aussage von Björn Dehms, BSI, nur auf eine bestimmte Produktversion zu einem Prüfzeitpunkt bezieht. Die Zertifikate sind somit zeitlich nicht befristet, und es können regelmäßig auch nur Teile eines Produktes zertifiziert werden. Empfehlenswert erscheint also auch weiterhin die regelmäßige Lektüre von Tests in der einschlägigen Fachliteratur.

Für das BSI stellt sich aber auch eine weitere Frage. Wie kann es beiden Interessen dienen, denen der staatlichen Kunden mit möglicherweise besonderem Geheimhaltungsbedarf und denen der unternehmerischen bzw. auch noch der privaten Kunden, die zwar einerseits an jeweils offener Kooperation bei der Entwicklung und Bewertung ihrer Produkte interessiert sein müssen, für die andererseits eine staatliche Einrichtung, die sowohl Strafverfolger und Nachrichtendienste als auch die eigene Konkurrenz bedient, möglicherweise selbst ein „Sicherheitsproblem“ darstellt? Kann das BSI bspw. ein Produkt zertifizieren, d.h. bei jeder erkannten Sicherheitslücke gemeinsam mit den Herstellern umgehend für deren Beseitigung sorgen, und kann es gleichzeitig den Sicherheitsbehörden helfen, die in ihrer Arbeit ja unter Umständen auf das Gegenteil angewiesen sind, bspw. das Knacken von verschlüsselter Information durch Ausnutzen von Schwachstellen?

Frage 5: Wie können Weiterbildung und Beratung der Internet-Nutzer verbessert werden?

Erste und wohl wesentlichste Voraussetzung für eine aktive Stärkung ist ein möglichst gutes Wissen um die wichtigsten Potenziale und Risiken des Internet. Für einen sicheren Umgang mit den neuen Techniken reicht es eben nicht aus, einen PC einschalten, den Internet-Browser aufrufen und eine e-mail verschicken zu können. Wenn die Vertreterin des Verbraucherschutzes dafür plädiert, das Netz müsse so sicher sein, dass auch der völlig unkundige Nutzer es ohne besondere Risiken nutzen könne, so greift sie damit die Werbeaussagen der Internetindustrie, die Ähnliches suggerieren möchte („Bin ich schon drin?“) auf. Doch könnte sie nicht mit etwa dem gleichen Recht fordern, dass sich in der realen Welt doch bitte jeder deutsche Urlauber auch ohne Landeskenntnis in der Bronx, in Afghanistan oder im nächtlichen Johannesburg bewegen können sollte? Die Forderung wäre zwar berechtigt, aber unrealistisch.

Andererseits sind die Risiken im Internet eben nicht gänzlich mit den Risiken des restlichen Alltags, etwa im Urlaub oder im Straßenverkehr, zu vergleichen. Man stelle sich vor, im Internet gäbe es jährlich mehrere tausend Tote durch Verhaltensfehler! Aber auch, wenn die Risiken nicht vergleichbar sind, gilt eben, dass sich im Grunde berechtigte Forderungen auch an ihrer Realisierbarkeit messen lassen müssen. Zwar ist ein einfach zu bedienendes Kommunikationsmedium „Internet“ mit viel Spaß und Gewinn, dafür ohne allzu viel Verantwortung im Grunde genau das, was die Verbraucher wollen, und was mit Blick auf die „Digital Divide“, also die Spaltung der Gesellschaft in Informationsarme und Informationsreiche, auch gewährleistet sein muss. Weder ältere Menschen, die nicht mit dem PC aufgewachsen sind, noch jüngere, zu deren spezifischen Begabungen oder Interessen das Ausharren vor Bildschirmen und das Durchdringen von Unterweisungen in Fachchinesisch eben nicht zählt, dürfen ausgeschlossen bleiben. Der Nutzer ist auch nicht selber schuld, wenn er auf einer Dialer-Seite landet. Es gab in der Vergangenheit so irreführende Dialer-Seiten wie win-zip.de oder cebit.de, bei denen man, bei entsprechend geringer Sicherheitseinstellung bei einem selbsteinwählenden Dialer landete.

Es bleibt aber dabei: Wer heute seine Daten ins globale Internet schickt (und das tut auch jeder, der sich nur passiv Seiten anschaut), sollte mit den Mindeststandards zur

Eigensicherung vertraut sein, sollte transparente Informationen über den Provider seines Vertrauens haben und sollte regelmäßig beurteilen können, welche Verfahren zur Datenübermittlung noch als sicher gelten und welche (meist veralteten) Betriebssystem- oder Browserversionen besonders anfällig für Viren, Trojanische Pferde u.a. Schadprogramme sind. Wer dies nicht zu tun bereit ist, möge die Verantwortung selbst tragen.

Auch der Dialerschutzexperte Sascha Borowski ist, wie einige Teilnehmer, der Meinung, dass Nutzer gewisse Vorkenntnisse besitzen sollten, wenn sie sich ins Netz begeben. Der Vertreter des CCC, Jens Ohlig, plädiert für einen Aufschrei der Verbraucher, die u.a. bei Microsoft ein Sicherheitskonzept fordern sollen. Microsoft solle deutlich machen, dass die Produkte mitnichten für den normalen Verbraucher geeignet seien!

Für den individuellen Nutzer empfehlen sich einfache Verhaltensregeln, wie sie auch für Laien verständlich aus einer breiten Palette von Angeboten im Internet oder aus kostenlos verteilten CD und anderen Materialien zu entnehmen sind. Christoph Verenkotte und Dr. Ulrich Sandl, die Vertreter von BMI und BMWi, weisen zu Recht auf die Angebote der Task Force Sicheres Internet, des BSI und der BMWi-Initiative „Sicherheit-im-Internet“ hin.

Über diese Möglichkeiten hinaus bieten sich aber noch eine Reihe weiterer Potenziale, denn Aus- und Fortbildung dürften generell nachhaltigeren Return on Investment bringen als der schnelle Euro durch Ausnutzen von Wissenslücken beim Verbraucher. So darf bspw. die Sensibilisierung für IT-Sicherheit nicht fehlen, wenn Schulen ans Netz gebracht werden. Welcher Verbraucherverband bietet, analog zum Handy-Führerschein, den Internet-Führerschein an, wie er bspw. von der Gesellschaft für Informatik und auf europäischer Ebene propagiert wird? Wo bleibt die Anlaufstelle für Bürger mit konkreten Problemen beim Umgang mit dem Internet – ein Bürger-CERT, das spätestens dann unvermeidlich werden dürfte, wenn es tatsächlich wie geplant zu einem Verlagern von öffentlichen Dienstleistungen ins Internet auf breiter Front kommen soll (Stichwort Bund Online 2005)? Die Anbieter von PC, Betriebssystemen oder Browsern müssten sich selbst verpflichten oder verpflichtet werden, ihre Produkte mit sicheren Voreinstellungen auszuliefern, die der Nutzer je nach Know-How

und eigener Risikoeinschätzung dann von sich aus erweitern kann. Heute ist es genau andersherum. Viele Rechner werden mit geringen Sicherheitseinstellungen ausgeliefert, die der Nutzer dann, sofern er über das nötige Wissen verfügt, intensivieren kann.

Warum wird, in Analogie zur Govnet-Debatte, nicht über ein sicheres Bürger-Netz diskutiert, das statt Surfen (und Untergehen) im globalen Informationsbrei wesentliche Funktionalitäten auf (narren-)sicherem, d.h. auch einfach zu bedienendem Niveau bereitstellt, wie: 1. Online-Banking, 2. Telefon- und Fahrplanauskunft, 3. e-mail, 4. Pizza-Service oder ähnliches, 5. Lexikon und Wörterbücher, 6. Kino- und Veranstaltungskalender, 7. Tageszeitung?

Für Unternehmen hingegen ist über die in der Zusammenfassung genannten Maßnahmen das Vorhandensein eines (je nach Größe abgestuften) Risikomanagements und als vordringlichste Maßnahme die Ausarbeitung und das Training eines Notfallplans von zentraler Bedeutung. Professor Klaus Brunnstein beleuchtet in diesem Zusammenhang einen weiteren wichtigen Aspekt der Sicherheitsdiskussion, nämlich den Qualifikationsstandard von IT-Experten: In Deutschland wurden bisher 50.000 Informatikerinnen und Informatiker ausgebildet, doch die Anzahl der Leute, die sich derzeit als IT-Spezialisten bezeichnen, wird auf ca. 800.000 bis 1 Million geschätzt. Auch die spezielle Bezeichnung als IT-Sicherheitsexperte ist nicht geschützt und wird bspw. gerne nach einer einjährigen Fortbildung ohne explizite Sicherheitsausrichtung verwendet. Diese nicht standardisierte Qualifikation sieht er als eine wesentliche Ursache für das Faktum, dass in nagelneue Betriebssysteme zwischen 50.000 und 100.000 Fehler hineinprogrammiert werden.

Ausblick

Der Aufbau riesiger personenbezogener Datensammlungen außerhalb unseres rechtlichen Geltungsbereichs, wie in den USA durch die Firma EDS, lässt den Vertreter des CCC, Jens Ohlig, auf Gefahren im Sinne von „big brother“ hinweisen. Großen Handlungsbedarf macht er vor allem bei der Legislative aus, wobei er besonderen Bedarf in Richtung Verbraucher- und Datenschutz konstatiert, die Entwicklungen seit dem 11. September jedoch gerade in die entgegengesetzte Richtung zielen sieht.

Bei aller Kritik ist aber sein Credo, dass wir alle immer in einer unsicheren Welt leben - und es genießen sollten. Leider wird dieser wesentliche Diskussionspfad im weiteren Verlauf der Tagung nur sehr eingeschränkt verfolgt.

Das Dilemma ist eigentlich darin zu sehen, dass die Werkzeuge, mit denen Kommunikation für Dritte unlesbar zu machen und mit denen die eigenen Spuren im Internet zu verwischen sind, zwangsläufig auch Terroristen, Betrügern, Kinderschändern und der organisierten Kriminalität zur Verfügung stehen. Wenn es also, wie vom Datenschutz propagiert, möglich ist, hochwertig zu verschlüsseln, ohne dass die Strafverfolgungsbehörden entschlüsseln können, und wenn staatlicherseits Anonymisierungsserver gefördert werden, mit denen man sogar perfekt die Tatsache verbergen kann, dass man überhaupt im Internet war, dann bleibt bei bestimmten Tatbeständen für Polizei und Staatsanwälte nicht mehr viel zu tun. Auch dieser Tatsache muss man sich in der Güterabwägung bewusst sein. Natürlich wäre es bedenklich, wenn bspw. die zeitweise Speicherung von Verbindungsdaten dazu führte, dass sich bestimmte Data-Mining-Unternehmer noch hemmungsloser im Bereich individuelle Verbraucherprofile tummeln könnten; natürlich wäre es ebenso bedenklich, wenn unser Rechtsstaat grundlegende Persönlichkeitsrechte durch systematische Ausspähung verletzte. Hemmungsloses Data-Mining erscheint dann unwahrscheinlicher, wenn es sanktioniert würde (besserer Datenschutz). Ob sich hingegen ein demokratischer Rechtsstaat in einen Überwachungsstaat verwandelt, ist eine Frage, die sich – zumindest absehbar - nicht im Internet entscheidet. Im Übrigen genügt es, sich die beschränkten Ressourcen und die Ausstattung von Einrichtungen anzusehen, die staatlicherseits mit der Verbrechensbekämpfung im Internet befasst sind, um zu wissen, dass eine Gefahr für systematische Ausspähung nicht gegeben sein kann.

Der von Datenschützern gern zitierte Aphorismus „Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, wird am Ende Beides verlieren“ (nach Benjamin Franklin) erscheint in diesem Zusammenhang als verfehlt. Statt Polarisierung muss es doch vielmehr um die Frage nach gegenseitigem Nutzen gehen. Welche Sicherheitsmaßnahmen bergen also besondere Potenziale für die freie Entfaltung des Einzelnen? Ist es wirklich das Sich-Verstecken, die Tarnkappe im Sinne von Anonymisierungstools, die das Internet attraktiv macht? Und wer nutzt zu welchen Zwecken Anonymisierung? Hinweise auf eine breite Akzeptanz derartiger Tools liegen bislang

nicht vor; im übrigen hinterlässt der Verbraucher zu ganz anderen Gelegenheiten, etwa wenn ein Gewinn oder Rabattpunkte winken, bereitwillig persönliche Daten im Netz. Wäre es also nicht sinnvoller, zwar Vertraulichkeit und, sofern gewünscht, Anonymität im Netz zuzulassen, im Fall von Ermittlungen wegen strafwürdiger Vergehen aber doch Polizei und Justiz technisch wie rechtlich die Möglichkeit einzuräumen, zu entschlüsseln, Verbindungsdaten und Personalien festzustellen?

Die freie Entfaltung im Internet bedarf doch gerade der Möglichkeit, sich ohne detaillierte IT-Sicherheitskenntnisse, ohne Tarnkappe und ohne die Befürchtung im Netz bewegen zu können, dass hinter jeder Ecke oder besser jedem Mausklick ein Ausspionieren von persönlichen Daten, ein betrügerischer Dialer oder anderes mehr lauert. Nicht zuletzt ist IT-Sicherheit ein entscheidender Faktor unter dem Gesichtspunkt, auf volkswirtschaftlicher Ebene Verluste zu vermeiden. Gesamtökonomisch gesehen kann dies weder durch prosperierende Anbieter von Sicherheitsprodukten geschehen noch durch „Netiquette“. Auf freiwillige Netzmoral zu setzen, könnte allenfalls dann funktionieren, wenn Internet-Teilnehmer signifikant bessere Menschen wären bzw. sich besser verhielten als die Menschen in der realen Welt, die offenbar detaillierte Straßenverkehrsordnungen ebenso benötigen wie ein umfangreiches Strafrecht. Die Existenz des erleuchteten „Homo Internet“ aber darf vorläufig bezweifelt werden.

Im Lauf der Tagung wurde prägnant zum Ausdruck gebracht, dass die Akzeptanz des Internet als breite, zukünftig vielleicht wesentlichste Grundlage unseres wirtschaftlichen Tuns entscheidend davon abhängt, wie viel Unsicherheit die Verbraucher bereit sind in Kauf zu nehmen. (Un-)Sicherheit in diesem Zusammenhang als notwendiges, aber lästiges Übel zu begreifen, führt in die Sackgasse.

Moderation:

Burkhard Plemper

Freier Journalist beim NDR, Hamburg

Udo Riedesel

Freier Wirtschafts- und Fernsehjournalist, Neunkirchen

Referenten und Teilnehmer/-innen an der Podiumsdiskussion:

Sascha Borowski

Journalist und Betreiber der Internetseiten www.dialerschutz.de, Augsburg

Prof. Dr. rer. nat. Dipl.-Phys. Klaus Brunnstein

Universität Hamburg, Fachbereich Informatik

Edda Castello

Leiterin der Rechtsabteilung der Verbraucherzentrale Hamburg

Björn Dehms

Bundesamt für Sicherheit in der Informationstechnik (BSI), Referat Internet-Sicherheitsanalysen, Bonn

Prof. Dr. Thomas Hoeren

Institut für Informations,- Telekommunikations- und Medienrecht, Westfälische Wilhelms-Universität Münster

Stefan Kratzer

Projektmanager Security, eco Electronic Commerce Forum e.V., Köln

Jens Ohlig

Sprecher des Chaos Computer Clubs, Köln

Dr. Ulrich Sandl
Referatsleiter IT-Sicherheit, Bundesministerium für Wirtschaft und Technologie, Berlin

Peter Schaar
Stellvertretender Datenschutzbeauftragter der Hansestadt Hamburg

Jella Teuchner, MdB (in Abwesenheit, schriftliche Stellungnahme)
Verbraucherschutzpolitische Sprecherin der SPD-Bundestagsfraktion, Berlin

Christoph Verenkotte
Referatsleiter Sicherheit in der Informationstechnik, Bundesministerium des Inneren, Berlin

Tagungskonzeption und –organisation:

Hannelore Hausmann
Oliver Dalichau
Margit Durch
Wirtschafts- und sozialpolitisches Forschungs- und Beratungszentrum der Friedrich-Ebert-Stiftung, Abt. Wirtschaftspolitik, Bonn

Verfasser der Broschüre:

Dr. Jürgen Malley und **Maria Rieping**, Mainz