FIFF Kommunikation
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. 17. Jahrgang 2000 • Einzelpreis: 5 EUR

3/2000
September 2000

G 7625

Verletzlichkeit der Informationsgesellschaft

Reiten auf der Risikowelle

ISSN 0938-3476

Inhalt

Editorial

Reiten auf der Risikowelle – Ute Bernhardt 3

Aktuell

Grundrechte in der Informationsgesellschaft – Thilo Weichert 4
Der Stellenwert des modernen Grundrechtdiskurses – DVD Vorstand 7
Behördenverkehr in Bremen ab jetzt mit Chipkarte – Eva Hornecker 9
ICANN – Von Namen und Nummern – Ute Bernhardt 12
ICSC 2001 – International Conference on Social Computing – Bremen 14
Pressemitteilung zu Online Privacy 47
Für Kurzentschlossene: Programm der 16. FIfF-Jahrestagung in Hamburg 49

Schwerpunkt

IT-Sicherheit – eine griechische Tragödie – Ute Bernhardt und Ingo Ruhmann 16
Kritische Infrastrukturen – Christiane Schulzki-Haddouti 19
AG Kritis: Papierberge ohne Ende – Ingo Ruhmann 21
FoeBuD »Big Brother Award« – padeluun und Rena Tangens 22
Bundesregierung nimmt Stellung zu Cybercrime-Abkommen – Christiane Schulzki-Haddouti 24
Jugendschutz im Internet – Dörte Neundorf 26
Elektronische Kommunikation – Manuel Kiper 30
Normative Anforderungsanalyse – Volker Hammer 36
Verletzlichkeit und Vertrauen – Marit Köhntopp 45

FIfF e.V.

FIfF e.V., Vorstand 47

Rubriken

Adressen 51
FIfF-Bibliothek 52
Impressum 55

Reiten auf der Risikowelle

Mit der Verletzlichkeit der Informationsgesellschaft leben?

Die Medizin kennt einige Krankheiten, die nur unspezifische und wenig störende Symptome entwickeln, bis sie zum schnellen Ende führen. Solche Krankheiten sind schwer zu diagnostizieren und es kommt meist erst dann zu einer Behandlung, wenn es zu spät ist.

Mit der Verletzlichkeit der Informationsgesellschaft verhält es sich ziemlich ähnlich: Sie wird als ein verbreitetes Alltagsübel wahrgenommen. Sicher kennt jede und jeder die Symptome eines Computerabsturzes, eines Befalls durch Computerviren oder auf andere Weise unlesbar gewordener Daten. Das ist ärgerlich, aber etwa so wie ein morgendlicher Kopfschmerz. Die Schäden halten sich in Grenzen und selbst der Übergang zum Jahr 2000 ging ohne den angekündigten großen GAU ab. Alltag sind mittlerweile die Rückrufe von Prozessoren und die üblichen Softwareprodukte, deren Garantie nur besagt, dass sie fehlerhaft sind.

Warnungen vor den Möglichkeiten umfassender Schäden werden etwa so ernst genommen wie die Warnhinweise vor dem Rauchen auf Zigarettenpakkungen: Akademisch gesehen bestreitet niemand das Schadenspotential, aber so richtig katastrophal wird es schon nicht werden, denn schließlich ist es bisher doch immer noch gut gegangen.

Typisch dafür war das Y2K-Problem. Nachdem die kritisch beäugte Datumswende überstanden war, interessierte sich niemand mehr dafür, wieviel Geld und Anstrengungen in den letzten Jahre notwendig waren, um diesen reibungslosen Übergang zu ermöglichen oder gar, was auch weiterhin an Umbauten bei den IT-Anlagen nötig ist. In Erwartung des großen Crashs waren kleine »Ausfälle« und Probleme geradezu »peanuts«.

Anders ist dies mit der Aufmerksamkeit gegenüber mutwilligen Eingriffen in IT-Infrastrukturen. Seit den ersten Statistiken zu den Ursachen von Ausfällen von IT-Systemen ist klar, dass Hacker und andere externe Verursacher nur eine marginale Rolle spielen. Trotzdem standen sie schon bei der Verabschiedung der »Hackerparagraphen« in Deutschland 1986 im Mittelpunkt. Ausgehend von der Entwicklung der IT-Sicherheit in den letzen Jahren gehen *Ute Bernhardt* und *Ingo Ruhmann* der Frage nach, ob aus der staatlichen Pflicht zur Daseinsvorsorge für den Schutz der Informationsgesellschaft nicht auch ganz andere Schlußfolgerungen zu ziehen und Maßnahmen zu ergreifen wären.

Im Gegensatz dazu verschärfte sich die Verengung der Verletzlichkeit der Informationsgesellschaft allein auf Hacker jedweder Form in den 90er Jahren durch die Entwicklung von Information Warfare. Sicherheit und Schutz der IT-Infrastruktur wurden seither zur staatlichen Aufgabe. Die Maßnahmen der Bundesregierung zur Sicherheit von kritischen Infrastrukturen und die Arbeit der »AG Kritis« unter Leitung des Bundesinnenministeriums beschreiben *Christiane Schulzki-Haddouti* und *Ingo Ruhmann* in ihren Beiträgen.

Risiko in der Informationsgesellschaft bedeutet aber nicht nur, Informations- und Kommunikationstechnik möglichst von Softwarefehlern zu bereinigen oder vor Mißbrauch zu schützen. In der Diskussion um die Verletzlichkeit der Informationsgesellschaft und den Möglichkeiten, das Risiko von Ausfällen zu minimieren, wurde immer auch davor gewarnt, als Ergebnis drastischer Schutzmaßnahmen das Schreckgespenst eines Überwachungsstaates entstehen zu lassen. Die Verletzlichkeit der Informationsgesellschaft bedeutet damit auch, diese Technologie entsprechend der Bedürfnisse einer demokratischen Informationsgesellschaft zu gestalten.

Als Verschärfung der »Hackerparagraphen« wird auf EU-Ebene die Einführung neuer Tatbestände diskutiert, was erhebliche Konsequenzen für die Aufdeckung von Sicherheitsdefiziten hätte. Effekt wäre, nicht die Sicherheitslücken zu stopfen, sondern das Reden darüber unter Strafe zu stellen. *Christiane Schulzki-Haddouti* stellt in einem Beitrag dazu das EU-Cybercrime-Abkommen vor. Wie versucht wird, das Internet als Hauptschlagader einer Informationsgesellschaft zum Schutz vor schädlichen und rechtswidrigen Inhalten zu reglementieren, wird am Beispiel von Filtersystemen zum Zwecke des Jugendschutzes von *Dörte Neundorf* untersucht.

Einen Mikrokosmos des reglementierten Zugangs zum Internet stellt der Arbeitplatz dar. Nach den USA setzen auch in Deutschland immer mehr Arbeitgeber Software zum Monitoring ihrer ArbeitnehmerInnen ein. Existierende Schutzrechte werden kaum beachtet oder sind sogar weitgehend unbekannt. *Manuel Kiper* beschreibt die derzeitige betriebliche Praxis der Überwachung und die gesetzlichen Gegenmittel.

Sicherheit durch Überwachung ist nicht nur auf den Betrieb beschränkt. Die Zahl der Überwachungskameras nimmt ebenso stetig zu wie die der genehmigten Telefonüberwachungen. Um auf diese Entwicklung aufmerksam zu machen, entstand vor zwei Jahren in Großbritannien der »Big-Brother-Preis«, der nun auch in Deutschland verliehen werden soll. Padeluun und Rena Tangens stellen ihre Initiative vor.

Überwachungsmaßnahmen und gesetzliche Regelungen sollen die Sicherheitsdefizite kompensieren, die von der Technik verursacht wurden. Das Modell einer rechtlichen und gesellschaftlichen Anforderung entsprechenden Gestaltung von IT stellt *Volker Hammer* mit seinem Ansatz einer normativen Anforderungsanalyse vor.

Technische und rechtliche Ansätze zur Sicherung zur Informationsgesellschaft vergessen jedoch einen grundsätzliche Aspekt: den Vertrauensverlust, den die Anfälligkeit der IT verursacht.

Fortsetzung im Schwerpunkt S. 18

Aktuell

Thilo Weichert, Kiel

Grundrechte in der Informationsgesellschaft – vergiss es?

Am 18. und 19. Februar 2000 fand an der Technischen Universität (TU) Berlin eine Tagung mit dem Titel »Grundrechte in der Informationsgesellschaft« statt. Der Titel klingt harmlos: Dass wir an der Schwelle von der Industrie- zur Informationsgesellschaft stehen, ist ein Allgemeinplatz. Dass hierbei die Grundrechte beachtet werden, sollte angesichts der zumindest in Westdeutschland entwickelten Rechtstradition ein Selbstläufer sein. Doch näheres Hinschauen offenbart die Brisanz des Themas: Nach dem Zusammenbruch des Ostblocks und angesichts des Siegeszuges der Informationstechnik stellen sich viele gesellschaftspolitische Fragen neu: Das reale Verschwinden des Antagonismus zwischen Kapitalismus und Sozialismus hat zwar die klar erscheinenden Fronten zwischen rechts und links aufgebrochen. Angesichts wirtschaftlicher Konzentrationen bei Marktgiganten wie Microsoft und der Globalisierung der Märkte v.a. durch die Informations- und Kommunikationstechnik gibt es neue soziale, wirtschaftliche, kulturelle und politische Fronten. Der Konflikt zwischen ökonomischen Modernisierungsgewinnern und -verlierern hat schon Eingang in die Schlagzeilen der Medien gefunden. Dass dabei die Grundrechte auf dem Prüfstand der technischen Entwicklung oder gar auf der Abschussliste stehen, haben bisher nur wenige gemerkt.

Neue Bedrohungen...

»You have zero privacy anyway. Get over it« (Du hast ohnehin Null Privatsphäre. Vergiss es!). Mit diesem Zitat wirbt der Chef von Sun, Scott McNealy, für seine Produkte. Demgemäß sammelt sein Unternehmen ebenso wie die Konkurrenz von Microsoft, oder etwa Telekom und Mannesmann, Daten von Kundinnen und Kunden ohne Ende. Um die Überwachung technisch zu gewährleisten, wird von Intel bei der Chip-Produktion jeweils eine unveränderbare Seriennummer eingebaut. Das Jahr-2000-Problem hat kurzfristig unsere Abhängigkeit von einer funktionierenden Informationstechnik klar gemacht. Die Lehre, dass künftig sämtliche neuen Verfahren einem Sicherheitscheck unterworfen werden sollten, um derartige Probleme künftig zu vermeiden, ist bei der Politik aber bis heute nicht angekommen. Information Warefare, das gezielte Eindringen in die EDV-Systeme einer anderen gesellschaftlichen Ordnung zwecks Zerstörung und Manipulation der Programme, kann einen Staat in die Knie zwingen, ohne dass Panzer rollen oder Raketen abgeschossen werden müssten. Die Digitalisierung der Telekommunikation ermöglicht deren totale Kontrolle, und dies nicht nur für fremde staatliche Geheimdienste oder für die Polizei, sondern auch für technisch versierte Einzelpersonen. Die Automation praktisch sämtlicher Verrichtungen im Alltag lässt Datenschatten entstehen, die ein massives Kontroll- und Manipulationspotential für Arbeitgeber, sog. Sicherheitsbehörden oder Großkonzerne, von Bertelsmann bis zur Deutschen Bank, darstellen. Welche grandiosen Kontrollmöglichkeiten sich eröffnen, wird mit jeder Zeitungsmeldung über Echelon, Internetkontrolle, Videoüberwachung oder Satellitenbeobachtung klarer. Was für den Einstieg in die Informationsgesellschaft mit der elektronischen Datenverarbeitung gilt, trifft erst recht für dessen biotechnische Weiterentwicklung zu. Die genetische Vermessung und Manipulation des Menschen und das Zusammenwachsen von Bio- und Informationstechnik lassen noch keine Ende der Entwicklung erkennen.

... und Chancen

Diese Risiken sind nur die halbe Miete. Die Technik liefert die Instrumente mit, mit denen neu entstandene Gefahren wieder gebannt werden können: Mit Verschlüsselung lassen sich Integrität, Authentizität und Vertraulichkeit der elektronischen Kommunikation gewährleisten. Anonymisierungs- und Pseudonymisierungsverfahren eröffnen Techniknutzungen und Erkenntnismöglichkeiten, ohne dass die daran Beteiligten beeinträchtigt würden. Der Einsatz biometrischer Verfahren erlaubt ganz neue Sicherheiten, ohne dass dies in Überwachung enden müsste. Damit nicht genug. Informationstechnik enthält nicht nur ein Potential zur Abwehr von Gefahren, sondern auch zur verbesserten Inanspruchnahme von demokratischen Freiheiten und Rechten. Die Möglichkeiten, über das Internet seine Meinung zu äußern, zu kommunizieren und sich zu informieren, sind quantitativ wie qualitativ der große Sprung gegenüber allen bisherigen konventionellen Medien. Die Erleichterungen vieler Alltagsverrichtungen erlaubt es uns, uns auf´s Wesentliche zu konzentrieren und uns ganz anders zu verwirklichen – wenn wir nur wollen und wissen, was wir wollen. Demokratische Diskussion, öffentliche Äußerung und Entscheidungsprozesse müssen nicht mehr auf

Wahlkämpfe und Wahlen beschränkt bleiben.

Es bedarf angesichts der dargestellten Phänomene eigentlich keiner langen Erklärungen, dass die Informationsgesellschaft aus den verfassungsrechtlich garantierten Grundrechten etwas anderes macht, als sie bisher waren: Menschenwürde, freie Entfaltung der Persönlichkeit, Schutz der Privatsphäre, der Wohnung, der Kommunikation, Berufsfreiheit, Informations- und Meinungsäußerungsfreiheit, demokratische Beteiligungsrechte; all dies ist offensichtlich betroffen. Tatsächlich gibt es kein Grundrecht, das von der derzeit stattfindenden technischen Revolution nicht berührt wäre.

Die Denkblockaden der Politik

Betrachtet man nun die öffentliche Debatte in Parlament und Regierung, so verblüfft die politische Abstinenz. Die Politik scheint sich von der Gestaltungsaufgabe bei der Grundrechtsverwirklichung verabschiedet zu haben. Es hat sich bis dorthin herumgesprochen, dass es auf der »Datenautobahn« keine Mittelstreifen gibt; dass es für diese aber Verkehrsregeln bedarf, ist politisches Neuland. Als Wirtschaftsmotor hat sich die Informationstechnik wohl profiliert. Technikeuphorie und technische Ignoranz liegen aber nahe beieinander. Politiker weihen mit stolzgeschwellter Brust neue Chipfabriken oder Informationsnetze ein, als handele es sich bei der Datenautobahn nur um eine technische Variante der Autobahn für Kraftfahrzeuge. Dies gilt praktisch für jede Partei und jede Couleur. Die Diskussion über Meinungsfreiheit, Informationsfreiheit, Datenschutz und Informationssicherheit sind Nischenthemen für Hinterbänkler geblieben. Es scheint noch nicht profilierungsträchtig zu sein, ein neues Grundrechtskonzept angesichts globaler technischer Herausforderungen zu diskutieren und zu entwickeln.

Alle Parteien haben mit der Informationstechnik ihre jeweils eigene Not: Christdemokraten sind zwar nicht technikfeindlich, aber strukturell konservativ und fühlen sich angesichts der revolutionären technischen Umbrüche überfordert. Für Sozialisten und Sozialdemokraten ist das Wegbrechen der typischen Anhänger- und Wählerschaft durch die Automation nicht nur der Waren-, sondern auch der Wissensproduktion existentielle Bedrohung. Zudem erleben sie – staatsfixiert wie sie teilweise immer noch sind – schmerzlich, dass Informationstechnik nicht mehr mit hoheitlicher Regulierung allein gezähmt werden kann. Für die Liberalen wird plötzlich das Duo von wirtschaftlicher und politischer Freiheitlichkeit zum Konfliktherd; wirtschaftliche Freiheit tendiert dazu, Konsumentenmanipulation und die Beschneidung politischer Rechte zu fördern. Und die Grünen stehen als ökologische Fortschrittsskeptiker vor dem Problem, dass sich der Fortschritt in der Informationstechnik – anders als bei sonstigen risikobehafteten Großtechnologien (Atom, Chemie) – unaufhaltsam und bisher ohne politische Vorgaben entwickelt. Das Feindbild »Technik« muss dringend abgelegt werden, zumal das grüne Wählerpotential sich vorrangig aus den Gewinnern der Informationstechnik rekrutiert. Diese ist offensichtlich ökologisch, sozial und bürgerrechtlich neutral – nutzbar zum Guten wie zum Bösen.

Dass angesichts dieser historischen Bruchlinien bei den politischen Parteien die Gestaltung der Informationsgesellschaft (noch) nicht im Vordergrund steht, ist verständlich, zugleich aber für sie selbst politisch kurzsichtig und für die gesamte Gesellschaft hochgradig gefährlich. Gestaltung bedeutet hier die Chance zur Wahrung ethischer und kultureller Werte, die Gewährleistung von individueller und gesellschaftlicher Sicherheit (CDU-Thema), das Streben nach sozialer Gerechtigkeit (SPD-Thema), der Schutz der natürlichen Lebensgrundlagen und die Verteidigung der Grundrechte (grünes Thema) oder von Pluralität, Wettbewerb und wirtschaftlicher Entfaltung (F.D.P.-Thema). Insofern hätten alle politischen Parteien ihren eigenen traditionellen Zugang zu einem neuen Thema. Politische Gestaltungsbereitschaft in der Informationsgesellschaft ist nicht nur ein Nachweis von Modernität, sondern bedeutet auch Sicherung und Gewinnung neuer Wählerschichten. Während die ganz große Mehrheit der Kaste der real existierenden Politiker noch eine informationstechnikfreie Sozialisation durchlief, gehören zur Wählerschaft inzwischen schon zwei jüngere Generationen, eine die die Informationsgesellschaft aufgebaut hat, die andere, die hineingeboren wurde. Für die ist die Informationsgesellschaft Alltag, nicht nur durch elektronische Spiele und 40 Fernsehkanäle, sondern durch Technikeinsatz in sämtlichen Lebensbereichen – von der Arbeit über die Freizeit bis hinein in die private Kommunikation.

Die Notwendigkeit der Neudefinition der Grundrechte

In diesen beiden Generationen gibt es nur wenige Gates oder McNealys, denen die ungebremste informationstechnische Marktentwicklung der Schüssel für jegliche Glückseligkeit ist. Und viele erkennen die neuen sich entwickelnden Bedrohungen für materiellen Wohlstand, Privatsphäre und demokratische Rechte. Sie sehen aber auch die Potentiale für Erleichterungen des Lebens und für´s Geldverdienen, die Chancen sich zu informieren und seine Meinung zu äußern, sich in neuen Welten zu entfalten. Diese Menschen mit ihren Ängsten und Hoffnungen bzgl. einer technikbestimmten Zukunft haben in der Politik (noch) keine Lobby, obwohl sie ein großes demokratisches Potential darstellen. Für diese Menschen und für die Gesellschaft, in der sie leben, müssen neue Politikansätze gefunden werden.

Es geht um eine Neubestimmung schräg gewordener Interessenvertretung. Es muss und darf dabei nicht nur um ökonomische, soziale und kulturelle Interessen gehen, sondern auch um die Verteidigung der freiheitlichen und demokratischen Grundrechte. Die Arbeitsthese dazu ist, dass die technologische Entwicklung die Grundrechte nicht obsolet macht. Es ist vielmehr davon auszugehen, dass auch in der Informationsgesellschaft jeder Mensch ein Bedürfnis nach individueller Entfaltung, freiheitlicher Entwicklung, nach ungestörter sozialer und politischer

Kommunikation hat. Nicht nur die Technik, sondern auch der Mensch mit seinen Bedürfnissen und Fähigkeiten entwickelt sich weiter. Dazu ist eine Neudefinition der Grundrechte unter den veränderten Rahmenbedingungen angesagt. Das wohl bestdiskutierte Beispiel für diesen Umdenkungsprozess ist der Schutz der Privatsphäre. Es war nicht die Politik, sondern das Bundesverfassungsgericht, das 1983 in Weitsicht in seinem Volkszählungsurteil durch die Definition eines neuen Grundrechts, des Rechts auf informationelle Selbstbestimmung, gestalterischen Einfluss genommen hat. Doch können wir nicht auf diesem Stand stehen bleiben. Die normative Verteidigung der Grundrechte durch Ge- und Verbote, überwacht von einer technikfernen Bürokratie, ist anachronistisch geworden. Selbstschutz, Datensparsamkeit, Technikkompetenz sind einige (eher kulturelle) Antworten auf die neuen Herausforderungen. Unter der Überschrift Grundrechtsschutz durch Verfahren und Technik stehen normative Antworten. In jedem Fall ist die Politik gefordert: Sie muss die Weichen stellen, Fördergelder verteilen, Bildungsprogramme auflegen, Gesetze machen, den gesellschaftlichen Diskurs vermitteln.

Die Verteidigung der räumlichen und personellen Privatsphäre à la Volkszählung ist nur ein wichtiger Aspekt. Es geht vor allem um die Neudefinition der sozialen Rollen der Menschen in einer neuen informationstechnisch global gewordenen Umwelt. Informationelle Selbstbestimmung setzt Zugang zu Informationen und deren demokratische Nutzung voraus. In einem solchen umfassenden Sinn sind die klassischen Grundrechte unserer Verfassung noch nicht hinreichend klar neu bestimmt in einer Gesellschaft, die von der Automation des Denkens und Kommunizierens gekennzeichnet ist.

Man durfte nun gespannt sein, was die in modernem, zivilgesellschaftlichem und technikbegeistertem Gewand daher kommende rot-grüne Regierung auf den Weg brächte. Die ersten Signale waren deprimierend: Die neue Regierung präsentierte die nicht fertig gewordenen Ladenhüter der alten in fast unverändertem Gewand, etwa bei der Novellierung des Bundesdatenschutzgesetzes oder der Strafprozessordnung. Der Unterschied zwischen alter und neuer Mitte war nicht auszumachen. Nach einer Phase der ungläubigen Fassungslosigkeit haben sich die technikorientierten Bürgerrechtler gefasst. Sie beginnen ihre Vorstellungen über die gesellschaftlichen Probleme von Morgen und über die möglichen Problemlösungen zu artikulieren.

Perspektiven

Die Neudefinition der Grundrechte darf man nicht Philosophen und Juristen und schon gar nicht den Protagonisten eines ungehemmten Technikmarktes überlassen. In einer Demokratie muss dies das Anliegen der betroffenen Menschen sein. Mit Versuch und Irrtum tasten sich diese an die neue elektronisch vernetzte Lebenswelt heran und erleben die Wichtigkeit der klassischen Grundrechte im neuen Kontext. Diese politische Gestaltungsaufgabe wurde bisher von Noch-Hinterbank-PolitikerInnen erkannt. Doch der offizielle Regierungsmoloch bewegt sich, auch wenn dabei der Grundrechtsschutz vorwiegend als Akzeptanzproblem und die Techniknutzung als Sicherheitsproblem verstanden wird. Wenn über die Freigabe der Kryptografie, ja gar über deren breite Einführung und Förderung, über die Schaffung sicherer informationstechnischer Infrastrukturen und über (elektronische) Informationsfreiheit diskutiert wird, sind plötzlich auch Regierungsmitglieder gefragt. Plötzlich entdecken sogar konservative Politiker, dass »Privatheit« eine zentrale Rahmenbedingung für die Informationsgesellschaft ist.

Bisher fand der gesellschaftliche Diskurs hierüber hinter verschlossenen Türen und in eher informellen Zirkeln statt. Da dies nicht so bleiben darf und soll, luden bürgerrechtlich orientierte Organisationen und Institutionen zu der Tagung am 18./19. Februar in Berlin ein. Nicht nur dort standen, sondern generell politisch stehen auf der Tagesordnung: die Modernisierung des Datenschutzrechtes, die Eingrenzung der technischen Arbeitnehmerkontrolle, neue Impulse für Wissenschaft, Bildung und Wirtschaft, z.B. durch »Schulen ans Netz«, die Zulassung und Förderung des Selbstschutzes der Bürger in der Telekommunikation bei gleichzeitiger Zurückhaltung bzgl. hoheitlicher Überwachung, die Regulierung des transatlantischen und globalen Datenverkehrs, der Erlass eines umfassenden Informationsfreiheitsgesetzes, die Stärkung des Verbraucherschutzes im E-Commerce, die Rüstung gegen den Information Warfare. Große Würfe kann es heute nicht mehr geben. Daher muss jeder bereit sein, von allen anderen zu lernen. Politik, Bürgerrechtsspektrum, Wissenschaft, wirtschaftlich Interessierte und Technikfreaks müssen gemeinsam über die politischen und rechtlichen Rahmenbedingungen einer grundrechtlich orientierten demokratischen Informationsgesellschaft diskutieren.

Abdruck mit freundlicher Genehmigung

Die Beiträge der Datenschutz-Tagung von DVD, FIfF und anderen in Berlin vom 18./19.2.2000 finden sich im Heft 4/1999 der DANA (http://www.aktiv.org/DVD)

Hans-Hermann Schild:
Die Novellierung des Datenschutzes in einem zwei Schritt-Modell

Ute Bernhardt:
Kundendaten als Ware: Datenschutz und Verbraucherschutz als Wirtschaftsfaktor

Ute Bernhardt/Ingo Ruhmann:
Information Warfare als neue Bedrohung der Grundrechte

Thilo Weichert:
Der elektronisch überwachte Hausarrest kommt

Thilo Weichert:
Gesundheitsreform – Einstieg in die pseudonyme Datenverarbeitung?

Beschluß des DGB-Bundesvorstandes:
Eckpunkte zum Arbeitnehmerdatenschutz

DVD-Vorstand, Bonn

Der Stellenwert des modernen Grundrechtdiskurses

Erfahrungen mit der Politik

Die Tagung »Grundrechte in der Informationsgesellschaft« verfolgte das Ziel, alle Beteiligten der Informatisierung unserer Gesellschaft an einen Tisch zu bekommen: Bürgerrechtsorganisationen, Verbraucherverbände, Gewerkschaften, Wirtschaft, Verwaltung, Datenschutzbeauftragte, Wissenschaft – und vor allem auch die Politik. Ergebnis des gemeinsamen Gesprächs sollten Kontakte, mehr gemeinsame Sprache, die Klärung eigener Positionen und das Voranbringen einer vielleicht gemeinsam für notwendig erkannten Politik sein. Die Resonanz der Teilnehmerinnen und Teilnehmer der Tagung lässt vermuten, dass dieses Ziel ansatzweise erreicht worden ist – abgesehen von einem Punkt: Der Versuch, die Ordnungs- und Wertediskussion über die Informationsgesellschaft in die Politik hineinzutragen, scheiterte – kläglich. Da es von Aussagekraft, ja vielleicht sogar symptomatisch sein dürfte, wie sich die Politik zu und auf der Tagung verhielt, lohnt es sich, zunächst im Stile eines Chronisten zu dokumentieren:

I. Zusagen – Absagen

Der erste Eindruck war äußerst erfreulich: Was zu schwarz-gelben Zeiten nie denkbar gewesen wäre, schien fast eine Selbstverständlichkeit zu sein. Für die Überschrift »Informationstechnikpolitik der Bundesregierung« konnten ohne großes Federlesen hochkarätige Vertreter gewonnen werden; die Staatssekretäre Schapper, Geiger und Catenhusen aus den Bundesministerien des Innern, für Justiz und für Bildung und Forschung sagen spontan zu. Zweifellos war es hierfür förderlich, dass Tagungsort und Regierungssitz identisch waren. Aber auch die Erkenntnis in die Relevanz des Themas und eine gewisse Sympathie hierfür waren offensichtlich vorhanden.

Anders die Reaktion der Fraktionen der im Bundestag vertretenen politischen Parteien. Angesichts der Kurzfristigkeit der Planung von Tagespolitikern wurden sämtliche Bundestagsfraktionen ca. 2 Monate vor der Tagung mit der Bitte um Benennung einer Vertreterin bzw. eines Vertreters zur abschließenden Podiumsdiskussion eingeladen.

Wenige Tage später ging das Fax des SPD-Bundestagsabgeordneten Jörg Tauss ein, in dem dieser seine Teilnahme als medienpolitischer Sprecher seiner Fraktion bestätigte. Tags drauf kam das nächste Fax von Michaele Hustedt, energiepolitische Sprecherin der Fraktion Bündnis 90/Die Grünen. Sie teilte mit, aus zeitlichen Gründen sei ihr eine Teilnahme an der Tagung nicht möglich; da aber das Thema sehr interessant sei, sollten wir die Tagungsunterlagen zur Verfügung stellen. Für das Gelingen wünschte sie uns alles Gute. Wieder kurz danach teilte uns ein Anruf aus dem Büro der Bundestagsvizepräsidentin Antje Vollmer (B'90/Grüne) mit, dass Frau Vollmer aus Termingründen leider nicht teilnehmen könne. Angesichts dieser nicht gerade einschlägigen Absagen bedurfte es zweier Telefonate, um das Kommen des datenschutzpolitischen Sprechers der Fraktion B'90/Grüne, Cem Özdemir, zugesagt zu bekommen.

Auch die PDS reagierte umgehend – per Email. Die Einladung sei zuständigkeitshalber an die medien- und technologiepolitische Sprecherin, Frau Angela Marquardt, weitergeleitet worden: »Auch wenn sich Frau Marquardt hinsichtlich ihrer fachpolitischen Tätigkeit für Ihre Veranstaltung interessiert, muss sie Ihnen mitteilen, dass sie den von Ihnen genannten Termin nicht wahrnehmen kann ... End of forwarded message«. Das konnte doch nicht alles gewesen sein von der Partei des demokratischen Sozialismus?! Da wir nicht annahmen, »dass ein derart zentrales politisches Thema nur von einer Abgeordneten Ihrer Fraktion vertreten werden kann«, baten wir um Benennung einer anderen Vertreterin bzw. eines Vertreters. Eine Antwort erfolgte nicht.

Gespenstische Züge hatte die Reaktion der CDU-Fraktion: Drei Wochen vor der Veranstaltung noch ohne Antwort, fragten wir in der Fraktionsgeschäftsstelle telefonisch nach. Das Gespräch lief bei einer Mitarbeiterin auf, die nach wenigen Sätzen dieses abhängte, um die andere Leitung zu bedienen. Nach gut fünf Minuten konnte dann endlich das Anliegen vorgetragen werden. Das Schreiben der DVD war nicht bekannt; es ließ sich weder in der Eingangsdatei unter dem Absender, noch unter DVD oder TU Berlin noch bei anderen weiterverbundenen MitarbeiterInnen finden. Wer zuständig sei, konnte uns auch nicht mitgeteilt werden. Insgesamt dauerte allein dieser erste telefonische Kontaktversuch etwa eine halbe Stunde und war insofern ergiebig, als wir gebeten wurden, die Einladung nochmals zuzusenden. Dies taten wir auch, an den Obmann der Fraktion, Herrn Marschewski, nachrichtlich an die Geschäftsstelle. Eine telefonische Rückfrage wenige Tage später blieb erfolglos; man wolle sich wieder melden. Nach weiteren vier antwortlosen Tagen fragten wir erneut nach, worauf uns bedauernd mitgeteilt wurde, der Anruf käme leider zu spät; die entsprechende Fachsitzung der Fraktion, auf der hätte gefragt werden können, sei gerade vor zwei Stunden zu Ende gegangen. Herr Marschewski und Herr Prof. Scholz hätten anderweitige Termine; außerdem finde an dem Wochenende in Berlin vom dortigen Landesverband eine Parteiversammlung wegen des Parteispendenskandals statt. Man bedauere außerordentlich.

Ähnlich, aber nicht gleich, die F.D.P.-Fraktion: keine Reaktion bis drei Wochen vor der Tagung, kein Wiederauffinden der Einladung, erneutes Anschreiben an den Obmann Jörg van Essen, nachrichtlich an die Geschäftsstelle. Anders als die christlich-demokratisch chaotische Abfertigung, wurden wir äußerst freundlich bedient. Man wollte sich um einen Vertreter bemühen, was offensichtlich auch passierte. Aber drei Tage vor der Veranstaltung musste man uns bedauernd mitteilen, sämtliche Versuche seien misslungen. Weder Prof. Schmidt-Jortzig, der zunächst vorgesehen war, noch Hans-Joachim Otto, noch Frau Sabine Leuthäuser-

Schnarrenberger hätten gewonnen werden können. Wiederum wurde uns versichert, das Thema sei außerordentlich wichtig.

Die Podiumsdiskussion drohte angesichts des Fehlens von CDU/F.D.P./PDS zur einseitigen Angelegenheit zu werden. Aber es kam noch krasser: Drei Stunden vor dem Termin ereilte uns die Nachricht, Cem Özdemir sei die Stimme versiegt – nicht politisch, sondern aus Gesundheitsgründen. Was blieb, war eine – zweifellos engagierte und unterhaltsame – Talk-Show mit dem SPD-Bundestagsabgeordneten Jörg Tauss.

II. Der Auftritt der Staatssekretäre

Wirkte die parlamentarische Ebene ernüchternd mangels Präsenz, so war dies in inhaltlicher Hinsicht der Fall bzgl. der ministeriellen Ebene. Nicht, dass das, was die Staatssekretäre vortrugen, falsch gewesen wäre – vieles war diskussionswürdig und -bedürftig, von der Tendenz her sogar zu begrüßen. Enttäuschend war aber das sichtlich fehlende Engagement von Herrn Schapper, nicht zuletzt angesichts seiner persönlichen Historie, in der u.a. mehr als eine Episode die Funktion des Hamburgischen Datenschutzbeauftragten ausmacht. Insgesamt frustrierend war die Konzeptionslosigkeit in sämtlichen drei Vorträgen: Résumées des Vollbrachten und Absichtserklärungen sollten nicht alles sein, was so große Häuser wie das Innen-, das Justiz- und das Wissenschaftsministerium zu Wege bringen. Etwas Zukunft Weisendes und etwas Grundsätzliches zu erwarten, war doch wohl nicht übertrieben. Es ist nicht der persönliche Fehler der Staatssekretäre, wohl aber ein strukturelles Defizit der vertretenen Ministerien, dass sie keine über die Tagespolitik hinausgehenden Analysen, geschweige denn Visionen vortrugen. Dass hieran Bedarf im Hinblick auf die Politik besteht, haben die anderen Plenarvorträge der Professoren Lutterbeck, Däubler, Büllesbach und Garstka gezeigt, ebenso wie die Arbeitsgruppen. Nur hatten die Staatssekretäre keine Zeit, sich mit den dort vorgetragenen Überlegungen auseinanderzusetzen; sie hatten (abgesehen von Herrn Catenhusen) nicht einmal die Zeit, sich einer anschließenden Diskussion zu stellen.

III. Schlussfolgerung und Fragen

Weniger Eigenbezogenheit und mehr Bereitschaft zum fachlichen Dialog würde der Qualität der Politik zweifellos sehr förderlich sein. Dass nicht nur die Diskussion über die politischen Inhalte zu Wünschen übrig ließ, sondern auch die Inhalte selbst, stellte sich bei der Tagung eindeutig heraus. Die äußere Präsentation der Politik hinterließ einen schalen Eindruck. Dieser Eindruck sagt wohl mehr aus über das bestehende Problembewusstsein bei den Politikern als die Texte der Vorträge. Die Beiträge der sonstigen ReferentInnen und der Diskussionen ergab jedoch: Grundrechtsschutz in der Informationsgesellschaft mag derzeit noch kein aktuelles Thema für die real existierende Politik sein, wohl aber ist es ein brisantes Thema für viele andere in einer sich rasant weiter entwickelnden – demokratisch, freiheitlich und rechtsstaatlich konzipierten – Gesellschaft. Spannende Anregungen, Forderungen und Ideen wurden auf der Tagung als Fragen an die Politik formuliert:

- Welche neue demokratische Funktion kann die (vor allem sich in elektronischen Netzen realisierende) Informationsfreiheit hinsichtlich der staatlichen Verwaltung einnehmen?
- Wie steht es mit der Transparenz und Informationsfreiheit in der Wirtschaft angesichts der Konvergenz von staatlicher Verwaltung und Wirtschaft?
- Welche Bedeutung hat die Konzentration privater (informationstechnischer) Macht für die Gewährleistung der Grundrechte?
- Wo bleibt das Recht, allein gelassen zu werden (right to be let alone) in einer transparenten, globalen informatisierten Gesellschaft?
- Welche Privacy Policy ist in einem europäischen Staatengebilde einzuschlagen im Spannungsbogen zwischen Selbstregulierung (des Marktes) und staatlicher Aufsicht?
- Welchen Einfluss hat darauf die Globalisierung des Informations- (technik-) Marktes?
- Welche Rolle spielen die Menschen als Verbraucher und Arbeitnehmer; welche Rolle spielen Verbraucher- und Arbeitnehmerverbände?
- Sollte es tatsächlich (wie von Jürgen Garstka angedeutet) einen Grundrechtsschutz für Maschinen als Boten der Menschen geben?
- Welche Werte muss unser Bildungssystem im Interesse demokratisch-freiheitlicher Rechtsstaatlichkeit und individueller Selbstbestimmung transportieren?
- Was gehört an sozialem, technischem, strukturell-organisatorischem und (bürger-)rechtlichem Know-How zur Vermittlung von Medienkompetenz?
- Lässt sich der Verlust an Individualität in einer zur Überwachung tendierenden Informationsgesellschaft durch Schaffung und Gewährleistung pseudonymer Kommunikationsformen und individuell definierter Rollen realisieren?
- Welches sicherheitstechnische Bewusstsein und welche organisatorische und technische Strukturen sind nötig, um das Funktionieren einer informationstechnikbasierten Risikogesellschaft sicherzustellen?
- Welche Rolle spielt der Einzelne, spielt der Staat, spielen internationale Zusammenhänge zur Gewährleistung informationstechnischer Sicherheit?

und sicherlich nicht die letzte, aber eine zentrale Frage:

- Wie kann das Versagen der Politik bei der Beantwortung der obigen Fragen behoben werden?

Die Tagung brachte tatsächlich mehr Fragen als Antworten. Zwischen den unterschiedlichsten Beteiligten, Reichen und Armen, Mächtigen und Ohnmächtigen, Technikern und Juristen, Studenten und Praktikern ... wurde diskutiert; es wird und muss weiter diskutiert werden. Die Frage, wann diese Diskussion kontrovers zwischen Politikerinnen und Politikern geführt werden wird, harrt noch der Beantwortung.

Eva Hornecker

Behördenverkehr in Bremen ab jetzt mit Chipkarte

? schneller ? leichter ? durchsichtiger

Eine Podiumsdiskussion der Regionalgruppe Bremen

Bremen ist eine der drei bundesdeutschen Städte, die den Zuschlag zum Modellversuch media@komm erhalten haben (neben Esslingen und Nürnberg). Untersucht und prototypisch erprobt wird in diesen parallelen Versuchen die Einführung von Chipkarten in verschiedenen Bereichen der Behörden. Nachdem sich die Bremer Regionalgruppe schon seit längerem mit dem Bremer Modell befaßt, organisierte sie für den 11 Mai eine öffentliche Podiumsdiskussion. Teilnehmer waren: Herbert Kubicek, Informatik Professor an der Uni Bremen und Organisator des Projektes; Uwe Schläger, Vertreter des Landesbeauftragten für den Datenschutz und Bernd Robben für das FIfF; die Moderation übernahm Ralf E. Streibl. Kurzfristig sagte die senatorische Behörde ihren zugesagten Vertreter mit der Begründung ab, sie fühle sich durch Herrn Kubicek adäquat vertreten.

Trotz schönstem Wetter fanden sich fast 50 Zuhörer ein, weit mehr als erhofft; darunter offenbar auch viele Personen von außerhalb des Uni-Umfeldes. Die Veranstaltung begann mit einem längeren Vortrag von Prof. Kubicek über das Projekt, gefolgt von Stellungnahmen der anderen Podiumsteilnehmer sowie einer Diskussion zwischen Publikum und Podium.

Herbert Kubicek erläuterte den Hintergrund des Projektes. Studien hätten ergeben, daß Menschen das Internet vor allem für Behördenkontakte nutzen. Formularserver und Online-Formulare ersparen jedoch nur wenige Behördengänge, da weiterhin persönliche Unterschriften nötig sind. Die rechtliche Voraussetzung für digitale Signaturen als Unterschriftersatz wurde 1998 geschaffen. Durchgeführt wird das Bremer Projekt durch eine eigens gegründete Gesellschaft, an der neben Sparkasse und lokalem ÖPNV auch zwei Softwarehäuser beteiligt sind. Zentraler Gedanke ist, daß für den Erfolg des Projekts gleichzeitig benötigt werden:

a) eine Plattform zur Steuerung und Abwicklung der Verfahren,

b) attraktive Anwendungen, und

c) technische Zugangsmedien für die Bürger.

Ein Anwendungsszenario ist z.B. das Ummelden nach einem Umzug. Mit der Chipkarte würde sich ein Bürger am eigenen Rechner oder an einem öffentlichen Terminal bei einer zentralen Verwaltungsstelle (Bürgerbüro, Ortsamt) identifizieren und die Aktionen/Formulare auswählen, die er ausführen will (sich anmelden, Auto, Hund, Strom, Rundfunkgebühren etc.). Ein Teil der Daten kann automatisch von einem Formular ins andere übertragen werden, Folgeaktionen können angestoßen werden. Indem Anwendungsbündel geschaffen werden, ist statt mehrerer Behördengänge keiner oder maximal einer notwendig. Für Bürger sind solche Bündel ›Umzug und Wohnen‹, ›Studium‹, ›Heirat‹ und ›Freizeit‹ (Ticketreservierung als attraktive Anwendung). Hauptanwender der Karte sind jedoch professionelle Mittler, für die ebenfalls Anwendungsbündel geschaffen werden, z.B. Rechtsanwälte, Notare und Steuerberater sowie Architekturbüros, die z.B. Bauanträge stellen etc.

Die Chipkarte verwendet asymmetrische Verschlüsselungsverfahren mit öffentlichen und privaten Schlüsseln zum Verschlüsseln, Entschlüsseln und Signieren. Registrierungsstellen vergeben Schlüssel an die Bürger und Trust-Center der Telekom verwalten die Schlüssel, um z.B. Signaturen überprüfen zu können. Der Bürger verschlüsselt im Verkehr mit Behörden jedes Formular mit dem öffentlichen Schlüssel der entsprechenden Behörde. Dies trenne die Daten voneinander und erfülle das Zweckbindungsgebot des Datenschutzes.

Das Projekt wird in drei Phasen ablaufen. Von 1999 bis 2002 wird eine eigene Signaturkarte in der Kommunikation zwischen Steuerberatern und Finanzamt sowie Rechtsanwälten und Gerichten erprobt. Da die Sparkasse Bremen ab 2000 sowieso Geldkarten einführt, kann diese ohne allzuviele Zusatzkosten um Signatur und Zusatzapplikationen erweitert werden. Ab 2002 wird die ec-Karte mit der Geldkarte integriert. Media@komm nutzt also die vorhandenen Ressourcen der Sparkasse mit. Ein vorteilhafter Seiteneffekt sei, so Kubicek, daß man damit an das bestehende Vertrauen der Bankkunden in die Bank und ihre vorhandenen Gewohnheiten anknüpfen könne. Viele Verwaltungsvorgänge verlangen zudem das Bezahlen einer Gebühr. Die Integrierung vermeide das Herumhantieren mit mehreren Karten während eines Vorgangs und appelliere so an die Bequemlichkeit der Bürger.

Da nicht alle Bürger die notwendigen technischen Fähigkeiten für den elektronischen Behördenverkehr erlernen werden, sei mit einer Quote von vorerst 20 % bei der Anwendung durch Bürger zu rechnen. In den USA läge die Sättigungsgrenze bei 40 %. Die Chipkarte solle den gewohnten Umgang mit Behörden nicht ersetzen, sondern erweitern. Dies ergebe sich von selber, da viele Formulare so kompliziert

seien, daß sie ohnehin nicht ohne Hilfe ausfüllbar seien. Daher solle es so etwas wie ›betreute Nutzerplätze‹ in Ortsämtern und Bürgerämtern geben, sowie Call-Center. Als Vorausgriff auf die Kritik an der Einführung von Chipkarten betonte Herbert Kubicek, daß die Chancen und Risiken von Chipkarten eine nicht entscheidbare Frage seien, es käme auf die Funktionen und die innere Organisation der Verwaltungsvorgänge an. Da es keine Partizipation per se gebe (ohne konkreten Grund), sei daran gedacht, Beteiligungsverfahren dort zu integrieren, wo es sich sozusagen ergibt. Eine solche Möglichkeit seien solche Veranstaltungen, wie wir sie mit der Podiumsdiskussion organisiert hätten.

Der **Vertreter des Landesbeauftragten für den Datenschutz, Uwe Schläger**, lobte in seinem Statement das Projekt für die Einbindung der Datenschützer, die von Anfang an die Soll-konzepte prüfen. Da das Projekt bundesweite Bedeutung habe – eines der drei Pilotprojekte soll bundesweit erweitert werden – gäbe es die Möglichkeit stellvertretend Sicherheitsmechanismen durchzudiskutieren. Das Bremer Projekt könne zudem beweisen, daß die qualifizierte deutsche Signatur nach deutschem Signaturgesetz durchführbar und wirtschaftlich machbar sei, was von der EU bezweifelt wurde (das europäische Signaturgesetz stellt schwächere Auflagen als das deutsche). Die Datenschutzprobleme deuteten sich jedoch an unerwarteten Stellen an, oft im Detail. Beispielsweise sei die Plattform ursprünglich gedacht worden als reine Weiterleitungsstelle, so als ob man einen Brief in einen verschlossenen Umschlag stecke. Probleme ergeben sich aber, wenn Bürger auch nachts Formulare ausfüllen, die Behörde aber nicht rund um die Uhr besetzt ist. In vielen Anwendungen sind nämlich Plausibilitätskontrollen notwendig, beispielsweise ob eine Adresse tatsächlich existiert. Daher muß ein Teil der Daten auf der Plattform gespiegelt werden, was komplizierte technische Lösungen erfordert, um den Datenschutz zu gewährleisten. Zudem müßten etliche Gesetze geändert werden, um die Verfahren zu vereinfachen oder die elektronische Signatur als Ersatz für das persönliche Erscheinen zu erlauben.

Der **Vertreter der FIfF-Regionalgruppe, Bernd Robben**, konzentrierte sich in seinem Statement auf die Auswirkungen von Mediatisierung und Informatisierung und die kulturellen und sozialen Folgen. Diese Folgen seien noch völlig unbekannt. Daher ging es ihm darum, das Blickfeld zu öffnen und zu sensibilisieren.

Bremen sei auf dem Weg in die Informationsgesellschaft. Die Hoffnung, mit virtuellen Städten zur Demokratisierung beizutragen, sei gescheitert. Als erfolgreicher erwiesen sich Projekte zu Service und Wissenstransfer, wie ›bremen.de‹. Eine Veränderung durch die Maschinisierung sei z.B., daß die Qualität der Produkte durch die automatisierten Systeme gewährleistet würde (ungeachtet der hohen Abfall- und Ausschußraten) und nicht mehr durch menschliche Kompetenz. Dies sei ein System der »organisierten Unverantwortlichkeit« (Ulrich Beck). Die Chipkarte ersetze Bürokratisierung durch Maschinisierung. Damit fielen menschliche Unwägbarkeiten weg – sowohl menschliches Mitgefühl wie Schikane.

Die Maschine ist jederzeit erreichbar und damit flexibel. Sind wir auf diese Flexibilisierung jedoch vorbereitet? Eine wichtige Frage sei, was wir mit der gewonnenen Zeit machen. Zwar würden Behördengänge gespart, andererseits würde die Freizeit und »Familienzeit« nun auch für den Umgang mit Behörden genutzt und damit aufgeweicht. Das alte Goethewort »Alles zu seiner Zeit an seinem Ort« gelte nicht mehr. Zudem seien die neuen Verfahren frei von Kontakten mit Menschen. Damit trügen sie zur Beschleunigung, Individualisierung und Anonymisierung bei.

Zusammengefaßt seien die wichtigsten Fragen:

- welche Folgen hat der Ersatz von Bürokratie durch Maschinisierung? (Stichworte »organisierte Unverantwortlichkeit«), Was wird aus den besonderen Bedürfnissen von Personengruppen? (individuelle Ausnahmen)
- Gibt es eine Zerstörung des öffentlichen Raums?
- Inwieweit wird zu Beschleunigung und Anonymisierung beigetragen?

Nach diesen drei Stellungnahmen begann eine rege **Diskussion mit dem Publikum**. Ein Teilnehmer wies darauf hin, zu fragen, wer die Verlierer seien. Wo wird vorhandene Infrastruktur zerstört? Bei der Einführung der Bankautomaten sei ebenfalls versprochen worden, daß dies ein zusätzliches Angebot sei, das nicht zu Personaleinsparungen führen würde. Was wird aus dem Bettler vor dem Bahnhof, wenn alle nur noch eine Geldkarte haben? Angesichts knapper Haushaltskassen sei es kaum vorstellbar, daß es nicht zu einer Verdrängung in der Verwaltung kommt, meinte Bernd Robben. In seinem Schlußwort erwähnte auch Kubicek, daß eine Verwaltungsreform mit Mitteleinsparung bereits beschlossen ist. Weiterhin wurde die Befürchtung genannt, daß irgendwann die Gebühren erhöht werden für diejenigen, die persönlich zur Behörde gehen und beraten werden wollen.

Eine weitere Frage war, ob es überhaupt möglich sei, eine zentrale Anlaufstelle für alle Behördenkontakte anzubieten. Zum einen könne der dortige Berater nicht alle möglichen Formulare so gut kennen, wie spezialisierte Beamte. Zum anderen sei dies ein datenschutzrechtliches Problem. Uwe Schläger gab zu, daß das Bürgerbüro auf datenschutzrechtliche Grenzen stößt, wenn derselbe Beamte alle Lebenslagen betreuen soll. Dies sei ein weiterer Grund, die Anwendungen in einigermaßen unkritische Pakete zu bündeln. Dem wurde entgegengehalten, daß es gelegentlich Gründe gibt, z.B. bei einer Ummeldung nicht sofort allen Behörden die gleiche Information zu geben. Es bestehe die Gefahr, durch workflow-artige Abläufe einen impliziten Zwang zu schaffen. Bernd Robben stellte die Frage, wie groß die Gefahr einer Zusammenlegung von Karten sei. Es sei schon auffällig, daß nach dem Zurückstellen der AsylCard-Pläne durch die Bundesregierung nun in Bayern geplant wird, ausgerechnet in Nürnberg – einer der media@komm-Städte – eine AsylCard zu testen.

In Frage gestellt wurde auch das Argument, die Chipkarte solle bequem für die Bürger sein. Viele Behördenvorgänge werden vom Einzelnen nur sehr selten benötigt. Dann aber steht dieser jedesmal neu vor dem Problem, mit der Technik und mit dem Formular klarzukommen, sich durch Fehlermeldungen hindurchzukämpfen und auszuprobieren. Wenn von den Projektverantwortlichen ausgesagt werde, diese neue Technik solle die alte nur ergänzen, nicht ersetzen, stellen sich zwei Fragen: Wer bezahlt das Ganze? Und: Wer verdient daran? Diese Kritik wurde von Kubicek bestätigt. Der Haupteffekt tritt bei den Mittlern auf, die häufig die gleichen Vorgänge durchführen. Es profitieren vor allem neue Servicebereiche. Beispielsweise hätten sich einige Spe-

ditionen selber bei den Projektträgern gemeldet.

Wie steht es mit Technikfolgenabschätzung und Bürgerbeteiligung im Projekt? Kubicek wiederholte, daß gerade die hohe Flexibilität eine Ungewißheit über mögliche Folgen erzeugt. Die Projektträger würden daher versuchen, Beteiligung und Datenschutz in einem »lernenden Prozeß« zu integrieren. Da die klassische Technikfolgenabschätzung der technischen Entwicklung immer hinterherhinke, fand Bernd Robben dies eine relativ überzeugende Lösung. Allerdings schiene es, als ob bei media@komm im Vordergrund eher Akzeptanzfragen stünden. Kubicek entgegnete, für ihn gebe es keinen Gegensatz zwischen Akzeptanzerhöhung und Technikfolgenabschätzung. Man könne Datenschutzprobleme vermeiden, gerade um die Akzeptanz zu erhöhen. Aus dem Publikum kam die Einschätzung, die Durchführung des Projektes spiegele eine Beschleunigung wieder. In der zu Anfang des Projektes gemachten Umfrage seien die Bürger zwar gefragt worden, ob sie Behördengänge gerne online erledigen wollen, wurden aber nicht zu ihren Gründen befragt. Zudem werde nun mit den Mittlern, mit Steuerberatern etc. getestet, statt mit Bürgern. Die Umsetzung orientiere sich nicht an Bürgerbeteiligung und öffentlichen Tests. Kubicek erläuterte, daß sich die Bürger häufig nicht an Beteiligungsverfahren beteiligen, weil sie keinen Anlaß dazu sehen. Sozialpsychologisch sei Beteiligung eine Last und Aufwand. Daher werde in dem Projekt zuerst ein Prototyp gebaut und dann (im August/September) ein Beteiligungsverfahren gestartet. Die professionellen Nutzer seien allerdings leichter zu beteiligen, da deren Interesse größer sei. Auch hier bedankte er sich wieder bei der FIfF-Regionalgruppe für diese Veranstaltung, die Beteiligung herstelle.

Im Gespräch nach der Veranstaltung nannte Herr Kubicek ein strukturelles Problem. Da es bereits ein Begleitprojekt gibt, daß die drei Pilotprojekte vergleichend bewertet, sähen die kommerziellen Projektpartner keinen Bedarf für weitere Begleitforschung. Es stünden daher nur geringe Mittel projektintern zur Verfügung.

Wie steht es mit der Freiwilligkeit? Ein Teilnehmer nannte das Beispiel Mensa-Karte, die zwar freiwillig sei, wo aber durch die geringe Anzahl an Bar-Kassen ein impliziter Zwang zur Benutzung besteht. Kubicek konnte diese Frage nicht langfristig beantworten. Allerdings gibt es Gleichbehandlungsgrundsätze, die z.B. unterschiedliche Gebühren verbieten. Letztendlich sei dies eine Frage der politischen Kontrolle.

Eine Zuhörerin stellte die Frage, wieviele Behördengänge sich überhaupt elektronisieren lassen. Häufig müsse man etwas vorlegen und erhalte auch wieder etwas zurück, einen Ausweis oder ein Dokument. Kubicek gab zu, daß von den untersuchten 100 Verfahren (die selber bereits nur ein Bruchteil der existierenden sind) nur 20 sinnvoll elektronisierbar sind. Der Rest sei zu widerspenstig. Hier stellt sich uns die Frage, ob dies den Aufwand rechtfertigt. Zumindest der normale Bürger profitiert demnach kaum, wohl aber die professionellen Mittler und Serviceanbieter. Doch auch wenn 20 Verfahren sehr wenig erscheinen, läßt sich daraus noch nichts über die endgültig sich ergebende Durchdringung der Verwaltung durch elektronische Behördenkontakte aussagen. Ungeklärt blieb weiterhin völlig, ob media@komm in irgendeiner Weise zur Transparenz der Verwaltung beitragen wird.

Zum Abschluß bat Ralf Streibl alle Podiumsteilnehmer, ihre **Vision, wie das Leben von Bürgern in Bremen 2010** aussehen werde, zu beschreiben.

Bernd Robben sah zwei Szenarien. Das erste sei eine (kafka'eske) Informatisierung und Maschinisierung. Alte Menschen fielen dabei heraus und die Begehrlichkeiten von Unternehmen, Polizei und Staat unterlaufen den Datenschutz. Das zweite Szenario übernimmt die positiven Utopien des Projektes – einen schnelleren und leichteren Umgang mit Verwaltungen, in denen das entlastete Personal für Beratung zur Verfügung steht. Beide Szenarien seien gleich unrealistisch. Er bevorzuge es jedoch zu träumen und phantasievoll über Konsequenzen nachzudenken, wie z.B. den Bettler vor dem Bahnhof.

Uwe Schläger glaubt, daß der Anteil von Dienstleistungen und Kommunikation über das Internet wachsen werden. Die »Meßlatte« für den Datenschutz müsse weiterhin so hoch hängen wie bisher. Personenbezogene Daten, wie z.B. auf der AsylCard, müßten von Chipkarten verschwinden. Gelöst werden müsse das Problem, wie ein leichter Zugang für alle Bürger gewährleistet werden kann (Access for All).

Herbert Kubicek meinte, daß die Umgestaltung der Kommunikations- und Lebensgewohnheiten 20 bis 25 Jahre brauchen werde. Eine Verwaltungsreform mit Mitteleinsparung werde vollendet sein. Der Service- und Rundum-Service-Gedanke werde wachsen, Mittler zwischen Bürger und Verwaltung würden eine wichtige Rolle spielen. Viele würden die Chipkarte als bequem empfinden, manche Bürger werden sich die Technik nicht leisten können. Wichtig sei es, Medienkompetenz zu vermitteln. Er empfahl den Zuhörern, sich auf der Website der Projektträger (www.bos-bremen.de) über den aktuellen Stand und die geplanten Beteiligungsverfahren zu informieren.

Ralf Streibl wies auf die Unterschiede zwischen den Modellprojekten hin. Im Nürnberger Versuch werde eine neue Chipkarte entwickelt und der Datenschutz wäre bisher noch kaum berücksichtigt worden. Da noch lange unklar sein wird, welcher der Modellversuche bundesweit umgesetzt werden wird, wären Veranstaltungen nötig, in denen die Projekte vergleichend vorgestellt würden. Weiterhin notwendig seien Beteiligungsverfahren und Diskussionen. Denn die Fragezeichen im Titel der Veranstaltung stehen immer noch da.

Ute Bernhardt

Von Namen und Nummern

Zur ersten Wahl der Internetverwaltung – ICANN

Für die einen ist es der Startschuß zur globalen Internetregierung und beispielhaft für Demokratie im Internet überhaupt, für die anderen ist es die bloße Besetzung eines Verwaltungsgremiums, dessen allgemeine öffentliche Anteilnahme und Begeisterung eher Verwunderung auslöst.

Unbestreitbar ist, dass das Internet verkörpert durch das World Wide Web sowie verschiedener anderer netzbasierter Dienste und Technologien mittlerweile die Basis für die weitere Entwicklung vieler wichtiger Bereiche ist. Ob es um Aus- und Weiterbildung, Wirtschaft, Demokratie, Kommunikation und Freizeit geht, das Internet ist das zentrale Werkzeug und Medium, dass alle Bereiche des menschlichen Lebens in zunehmend stärkerem Maße berührt. Eine Weiterentwicklung vieler Bereiche oder eine Modernisierung ist teilweise nur durch die Integration des Internets in Bestehendes vorstellbar. Da die Bedeutung und die Funktion des Internets zunimmt und sich dies sowohl global als auch in einem enormen Tempo entwickelt, ist es nur logisch, dass nun auch der Ruf nach Regeln, Transparenz, Mitbestimmung und Demokratie für das »Netz der Netze« von den Internetnutzern lauter wird.

Neue Türschilder – wer »kontrollierte« das Internet bisher?

Die Adressierung zur Internetkommunikation basierte in den Anfängen auf einer Datenbank, die der »Internetpapst« Jon Postel im Auftrag des U.S. Department of Defense (DoD) aufbaute. Gleichzeitig organisierte er die Diskussion um die technische Weiterentwicklung des Internets. Um diese zunehmende Arbeit zu erledigen, baute Postel die Internet Assigned Numbers Authority (IANA) auf, die vom DoD ab 1977 über einen Vertrag mit der University of Southern California offiziell mit diesen Arbeiten betraut wurde. Mitte der 80er Jahre entwickelte IANA daraus ein hierachisches System zur Assoziierung von Namen mit IP-Nummern, das Domain Name System (DNS).[1]

Mit der Öffnung des aus dem ARPANET und dem parallel dazu entwickelten wissenschaftlichen NSFNET der National Science Foundation (NSF) zusammen gewachsenen Internet auch für Nicht-WissenschaftlerInnen durch ein Gesetz aus dem Jahr 1992 setzte die stürmische Entwicklung des Internets ein. Die NSF kümmerte sich um die Weiterentwicklung und die Berücksichtigung der zunehmenden wirtschaftlichen Interessen am Internet. Regelungen zum Namens- und Adressraum lagen nun im Aufgabenbereich des Department of Commerce. Nun wandelten sich die Bedürfnisse und auch die Ausrichtung.

Schon 1993 beauftragte die NSF die Firma Network Solutions mit dem Management der DNS-Registrierung unter Kontrolle der IANA. Nach ersten Rechtsstreitigkeiten mit der Registrierung kommerzieller Domainnamen entstanden seit 1996 verschiedene Gremien und Aktivitäten zur Neugestaltung des Domainnamensraums. Ergebnis war u.a. zunächst die Idee eines in der Schweiz angesiedeltes internationalen Konsortiums, die aber nicht umgesetzt wurde. Statt dessen wurde 1998 ein Vorschlag von Postel zur Gründung von ICANN (Internet Corporation of Assigned Names and Numbers) vom Department of Commerce aufgegriffen und schrittweise umgesetzt.

Der Weg für ICANN wurde frei, nachdem die University of Southern California 1998 ihre Pflichten zur Verwaltung des Domain Name System aus einem DoD-Vertrag an ICANN abtrat, das seinerseits vom Department of Commerce mit der Entwicklung eines neuen Systems beauftragt wurde. Seit 1998 existiert ICANN als Non-Profit-Organisation nach kalifornischen Recht mit Sitz in Marina Del Rey, Californien, in demselben Gebäude, in dem Jon Postel bei IANA tätig war – lediglich die Türschilder wurden gewechselt. Die US-Regierung behielt mit diesem Neuanfang weiterhin die Fäden in der Hand.

ICANN hat für die Umsetzung der wichtigsten Aufgabenkomplexe verschiedene Untergruppen gebildet:

- Die Address Supporting Organization (ASO) befaßt sich mit dem System der IP-Adressen als Ganzes;
- Die Domain Name Supporting Organization (DNSO) kümmert sich um die Namensvergabe einfacherer, umgangsprachlicher Namen;
- Die Protocol Supporting Organization (PSO) kümmert sich um die Vergabemodi für IP-Nummern.

Geleitet wird ICANN von einem Übergangsgremium, das von Postel vor seinem unerwarteten Tod berufen wurde. Ab September 2000 werden dann alle vereinbarten Aufgaben der Internet-Administration an ICANN übergehen.

ICANN markiert also das Ende des Übergangs des Internets von einem Netz von Wissenschaftlern und Militärs zu einem Netzwerk, in dem kommerzielle Interessen eine Rolle spielen. Zwar ist die Frage nach der Regelung der Domainnamen vergleichsweise unwichtig, vergleicht man dies mit der begrenzten Zahl der IP-Nummern. Die für attraktive Domainnamen gezahlten Preise zeigen aber die gewaltigen wirtschaftlichen Interessen, die auf ICANN einwirken. Je mehr vor allem Markennamen im Netz eine Rolle spielten, umso größer wurde das entsprechende Interesse an der Mitwirkung und Mitgestaltung des Netzraums. Ernsthafte Konzepte, die neben kommerziellen Interessen auch andere Regulierungsmöglichkeiten vorschlagen, werden weiterhin entworfen.[2]

Wenn Verlage wie Bertelsmann, Spiegel und Heise, aber auch Telekommunikationsunternehmen mit Slogans wie »wer kontrolliert das Internet?« und die »erste Internetverwaltung legitimiert durch alle Internetnutzer« erfolgreich die deutsche Internet-Nutzerschaft mobilisiert haben, an der ICANN-Wahl teilzunehmen, dann liegt der Verdacht nahe, damit könnte das Interesse verbunden sein, auf die Besetzung des ICANN-Direktoriums auch Einfluss zu nehmen.

Alles im Griff?

Zielvorgabe für ICANN ist eine Leitungsstruktur aus 19 Direktoren. Neben dem Präsidenten von ICANN sind dies neun Direktoren, die von den Supporting Organisations benannt werden. Neun weitere Direktoren werden von den einfachen Mitgliedern von ICANN gewählt, den sogenannten at-large-members. Von diesen neun gewählten Direktoren werden im ersten Schritt nur fünf gewählt – für jeden Kontinent eine Person. Für jede der fünf Regionen sind jeweils sieben Kandidaten zulässig. Fünf davon wurden vom ICANN-Nominierungskomitee bereits vorgeschlagen. Die restlichen zwei Kandidaten gehen als Sieger aus Vorwahlen hervor, die zwischen all jenen abgehalten werden, die sich selbst nominieren. Für die eigentliche Wahl als Kandidaten zugelassen werden dann aber nur die zwei Bewerber, die in den Vorwahlen von mindestens zwei Prozent der ICANN-Mitglieder ihrer Region unterstützt wurden und deren Unterstützer aus mindestens zwei unterschiedlichen Ländern kommen.

Wenigstens ist bei ICANN wahlberechtigt, wer bei ICANN Mitglied ist. Aufnahme bei ICANN findet, wer eine reale und eine Mailadresse hat, Gebühren fallen derzeit nicht an. Diesen Schritt vollzogen auch 158.000 jener 300 Millionen Erdenbürger mit Internetanschluß – also immerhin 0,53 Promille. Dabei überdurchschnittlich stark vertreten sind Mitglieder aus vier Ländern: Japan, China, Deutschland und USA.

Die Kandidaten stießen nicht überall auf Entgegenkommen. Kritik an den vom ICANN-Nomierungskomitee aufgestellten Kandidaten kam auch vom CPSR, die sich die einzelnen Kandidaten genauer ansahen. Keiner der fünf von ICANN benannten europäischen Kandidaten für den ICANN-Vorsitz scheint Internet-Nutzer zu repräsentieren. Neben zwei Technikexperten sind die anderen drei Kandidaten MitarbeiterInnen bei der Französischen Telekom, der Deutschen Telekom und der Internationalen Handelskammer.[3]

Ob die Selbstnominierung auch anderen Kandidaten ins Gremium hilft, wird nicht allein die Wahl zeigen, sondern auch die Reaktion von ICANN. Die Kandidaten für die weiteren zwei ICANN-Plätze wurden bis Ende August durch Selbstnominierung aufgestellt. Ein Bild von den 73 europäischen Kandidaten kann man sich durch die Beantwortung eines KandidatInnen-Fragebogens machen. Die Schar der KandidatInnen ist ein bunter Haufen mit recht unterschiedlichen Interessen an ICANN. Die Anerkennung der einzelnen unabhängigen KandidatInnen durch ICANN steht noch aus. Die Entwicklung der at-large-Mitgliederschaft und deren Rolle im Direktorium macht ICANN von den Ergebnissen einer Studie abhängig.[4]

Demokratie als Mißverständnis

Zusammen genommen heißt dies, dass ICANN über das Wahlprocedere, die Kandidatenanerkennung sowie die zukünftigen Möglichkeiten der Mitglieder zur Mitarbeit entscheidet. Schon von dem Interesse an dieser Wahl wurde ICANN überrascht – die Öffentlichkeitsarbeit für die ICANN-Wahl machten andere. ICANN war nur von der Registrierung von weniger als 10.000 Personen ausgegangen.[5]

Hintergrund dafür ist die Selbstsicht von ICANN als technisches Gremium. Sowohl ICANN- Chief Policy Officer Andrew McLaughlin als auch der Interimsdirektor von ICANN Europa, Hans Kraaijenbrink erklärten, ICANN sei keine Regierung und daher auch keine Demokratie.[6] Die Wahl sieht Kraaijenbrink als Teil eines politischen Kompromisses der ICANN-Auftraggeber, also der US-Regierung. Ausschlaggebend für die Arbeit von ICANN sei die Stabilität der technischen Infrastruktur und die Kompetenz der Direktoren zur Umsetzung dieser Aufgabe.

Zugute halten muß man ICANN, dass dort niemand je behauptet hat, es gehe bei der ICANN-Wahl um die Wahl einer Internetregierung oder irgend eine andere demokratisch zu legitimierende Funktion. Im ICANN-Leitungsgremium versammelt sind allerdings auch diejenigen, die bisher schon von der Öffentlichkeit unbeachtet das Internet aufgebaut und weiterentwickelt haben. Dies waren allerdings nicht diejenigen, die das Internet heute für ihre kommerziellen Zwecke nutzen wollen.

Die in ICANN gesetzten Erwartungen und die Auseinandersetzungen um dessen Rolle zeigt, wie geschickt der Schachzug der US-Regierung mit dem Übergang von der IANA zu ICANN war. Einerseits kam es ihr offensichtlich darauf an, die eindeutige Kontrolle der U.S.-Administration über zentrale Strukturen des Internets zu überführen in eine Form, die weder ein offizielles zwischenstaatliches Gremium – möglicherweise unter Aufsicht der UN oder anderer internationaler Gremien – noch eine rein kommerziell ausgerichtete Organisation ist. Andererseits erlaubt es die Vielzahl von Einwirkungsmöglichkeiten der etablierten ICANN-Leitungsstruktur, die Entwicklung nicht außer Kontrolle geraten zu lassen.

Die Vielfalt jener Institutionen, die zur ICANN-Wahl aufgerufen haben, wollen ihrerseits durch öffentliche Aufmerksamkeit verhindern, dass die Entwicklung der Internet-Verwaltung zurückgedreht wird oder zu einem Gremium mutiert, in dem nur wenige große Player die Richtung bestimmen.

Fazit

Auch nach der Wahl wird ICANN weder demokratisch legitimiert sein noch eine demokratische Struktur haben. Einziger Effekt der Wahl ist der Beginn eines Prozesses größerer Transparenz bei der Weiterentwicklung des Internets. Verglichen mit der heutigen Situation ist dies ein wichtiger Schritt zur zukünftigen Gestaltung des Internets. Der Erfolg dieser Entwicklung hängt davon ab, ob es gelingt, die Aufmerksamkeit auch dann noch auf die Arbeit von ICANN zu lenken, wenn der Wahlevent vorbei ist und die eigentliche Arbeit beginnt.

---

1 Eine der ausführlichsten Übersichten über die Entstehung von ICANN und die damit verbundenen Rechtsprobleme stammt vom Rechnungshof der USA, vgl.: http://www.pfir.org/gao-icann.pdf

2. Eine interessante Neugründung ist »People for Internet Responsibility« an der Lauren Weinstein und Peter G. Neumann beteiligt sind, vgl.: http://www.pfir.org

3 vgl.: http://www.cpsr.org/internetdemocracy

4 So ICANN in einem Statement vom 31.7.2000, http://www.icann.org/announcements/icann-pr31jul00.htm

5 ebd.

6 Vgl. zu McLaughlin: http://www.heise.de/newsticker/data/jk-19.06.00-000/, zu Kraaijenbrink: http://www.spiegel.de/netzwelt/politik/0,1518,81720,00.html

ICSC 2001 International Conference on Social Computing October 1 – 3, 2001 University of Bremen, Germany

CALL FOR PAPERS

Governing the Network Society

PURPOSE

In recent decades, the use of information and communication technology has transformed the way of life and work of many people all over the world. While the Internet has become the most important instrument for organizing that change, we see that in some parts of the world, many people do not even have access to a computer. Ironically, while »connected« people partake in discussions about the evolution of the »networked society«, those who are not connected are excluded from this discussion. As a result, the technological, cultural, and social developments will probably continue without the participation of large numbers of people, and the imbalance will extend with growing speed and unforeseen consequences. The main questions the conference is dealing with are: What are the social impacts of the emerging information and communication technology worldwide? Is it meaningful to speak about the »network society«? How can we govern it in a fair way?

The conference will serve as an international forum for scientists, leading experts, technical professionals, and users involved in research and development. They will gather together to discuss the benefits, challenges, and risks of information and communication technology for the future society. At the same time this international conference is an attempt to bring together those organisations involved in topics of computers and society.

The conference will include keynote addresses, invited lectures, contributed papers, posters, tool demonstrations, panel discussions, and satellite events on a wide range of topics in this area. The conference is meant to attract both academics as well as everybody working as an expert with information and communication technology.

SCOPE

Work
Computers, the workplace, and participatory design
Automation and the future of work
Mobile work in virtual companies
Collaboration and surveillance

Society
Computers and society
Equal opportunity
Technological and cultural challenges
Challenges and risks of the information society
Global information society and vulnerability
Special conditions in developing countries

Policy
Fair net governance
Social impact of e-commerce
Cyberrights and cyberethics
The future of copyright
National policies

CONFERENCE LANGUAGE
English

CONFERENCE SITE
Bremen, Germany, is an ideal setting for this October conference. The city is celebrated for its physical beauty, its independent politics, and as the home of the fairy tale, »The Town Musicians of Bremen«. Beck's beer is made here, and you will enjoy the parks, the historic buildings (e.g. the famous town hall), the fine restaurants, and the many open air markets.

PRESENTATION OF PAPERS
The full papers submitted for review should be no more than ten (10) pages in length and should be written in the format to be found under http://www.springer.de/comp/lncs/index.html. Send your submission preferably via email to icsc2001@informatik.uni-bremen.de. Paper versions of your submission should be sent to the conference secretariat. Your paper should be received by January 10, 2001. Notification of acceptance will be emailed; all other author information will be available on our webpage. Special arrangements can be made for all who do not have access to the internet. Camera-ready manuscripts and registration payments are due May 10, 2001.

POSTERS AND DEMONSTRATIONS
Besides full papers, participants may present posters or tool demonstrations. In this case, a 150-word abstract should be submitted.

PANEL DISCUSSIONS
A 500-word abstract should state the objectives of the panel, its scientific or educational importance, and a brief summary of the area of emphasis for each panel member. The abstract should also identify the panel chair and the panel members.

SATELLITE EVENTS
Workshops, seminars, meetings may be organized by interested groups or societies as special events, preferably before or after the conference. A 500-word abstract should state the objectives, con-

tent, scientific importance and methodology for conducting the workshop and the target audience.

PROCEEDINGS
The conference proceedings are intended to be published as Springer Lecture Notes in Computer Science (LNCS).

INTERNATIONAL PROGRAMME COMMITTEE

Jacques Berleur
Facultes Universitaires N.D. de la Paix, Namur, Belgium

Subhash Bhatnagar
Indian Institute of Management, Ahmedabad, India

Susanne Bodker
Aarhus University, Denmark

Andrew Clement
University of Toronto, Canada

Joan Greenbaum
LaGuardia Community College, Long Island City, USA

Dieter Klumpp
Alcatel SEL Stiftung, Stuttgart, Germany

Hans-Jörg Kreowski
University of Bremen, Germany, Chair

Karl-Heinz Rödiger
University of Bremen, Germany, Chair

Ina Wagner
Vienna University of Technology, Austria

Marsha Woodbury
University of Illinois at Urbana-Champaign, USA

CO-ORGANIZERS AND CO-SPONSORS

Gesellschaft für Informatik, Fachbereich Informatik und Gesellschaft (GI-FB 8)
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF)
IFIP Technical Committee on Computers and Society (IFIP TC 9)
Computer Professionals for Social Responsibility (CPSR)
Informationstechnische Gesellschaft, Fachbereich Informationsgesellschaft und Fokus-Projekte (ITG-FB 1)

IMPORTANT DEADLINES

January 10, 2001
All submissions (full papers and proposals for posters, tool demonstrations, panel discussions, and satellite events)

March 10, 2001
Notification of acceptance

May 10, 2001
Submission of camera-ready papers and registrations

CONFERENCE SECRETARIAT

ICSC 2001
University of Bremen
Dept. of Mathematics and Computer Science
attn Mrs. Marlott Hederich
P.O. Box 33 04 40
D-28334 Bremen
Germany
Phone: (+49 421) 218-24 88
Fax: (+49 421) 218-33 08
E-mail:
icsc2001@informatik.uni-bremen.de
www:
http://icsc2001.informatik.uni-bremen.de

FIfF-Beteiligung an ICSC 2001

Schon vor vielen Jahren wurde von einigen FifF-Mitgliedern die Idee diskutiert, dass der Fachbereich Informatik und Gesellschaft der Gesellschaft für Informatik (GI FB 8) und das FIfF auf deutscher Seite insbesondere im Zusammenhang mit CPSR (Computer Professionals for Social Responsibility) eine internationale Konferenz zu den gesellschaftlichen Auswirkungen der Informatik organisieren sollten. Dieses Projekt wird nun mit der International Conference on Social Computing (ICSC 2001) verwirklicht, bei der neben den bereits genannten Organisationen auch die International Federation of Information Processing mit dem Technical Committee on Computer and Society (IFIP TC 9) und die Informationstechnische Gesellschaft mit dem Fachbereich Informationsgesellschaft und Fokus-Projekte (ITG-FB 1) beteiligt sind.

In Politik, Wirtschaft und großen Teilen der Wissenschaft verspricht man sich von der Informations- und Kommunikationstechnik den »Himmel auf Erden«: Neue Jobs vertreiben die Massenarbeitslosigkeit, Informationen sind immer und überall sofort und mühelos verfügbar, alle sind jederzeit erreichbar, die Arbeit wird einfacher, angenehmer und interessanter, das Leben schöner, die Informationsgesellschaft – oder wie auch gern gesagt wird: die Wissensgesellschaft – ist angebrochen. In den USA, Japan und in der Europäischen Union werden weder Kosten nach Mühen gescheut, die neuen Technologien zu befördern. Informations- und Kommunikationstechnik wird zunehmend in immer weiteren Bereichen von Wirtschaft und Gesellschaft eingesetzt, die weltweite Vernetzung wird mit Schwung vorangetrieben, die Studierenden stürmen neuerdings das Studienfach Informatik und alle ihre Bindestrich-Varianten.

Aber was ist dran an den Hoffnungen, Erwartungen, Träumen? Was ergibt eine nüchterne Analyse der Situation? Wie lassen sich die ungleichen Entwicklungen innerhalb der Staaten und weltweit vermeiden? Macht es Sinn von »Informationsgesellschaft« oder »network society« zu sprechen? Die Konferenz ICSC 2001 ist als Forum gedacht, um diese Fragen zu diskutieren. Wir hoffen, dass sich viele FIfF-Mitglieder daran beteiligen werden, dass wir viele von euch vom 1. bis 3. Oktober nächsten Jahres unmittelbar nach der FifF-Jahrestagung in Bremen begrüßen können. Nähere Informationen finden sich im Call for Papers in diesem Heft und auf der Web-Seite icsc2001.informatik.uni-bremen.de.

Hans-Jörg Kreowski und Karl-Heinz Rödiger

Schwerpunkt

Ute Bernhardt und Ingo Ruhmann

IT-Sicherheit – eine griechische Tragödie

Die abstrakte Warnung vor der Verletzlichkeit der Informationsgesellschaft scheint mittlerweile in handliche Problempakete zerlegt. Gegen Computerviren helfen Virenscanner, Sicherheitslöcher in Software werden regelmäßig mit Softwarepatches ausgebessert. Den Schutz »kritischer Infrastrukturen« gegen konzertierte Angriffe hat der Staat zu seiner Aufgabe gemacht. Wer noch Fragen hat, kann sich an Beratungsunternehmen wenden.

Die Herstellung von IT-Sicherheit ist zu einem Problem des Endanwenders geworden. Der systemische Charakter dieses Problems wird nur noch vereinzelt sichtbar. Der als Y2K-Problem bezeichnete Übergang zum Jahr 2000 zeigte die Folgen eines flächendeckenden Konstruktionsfehlers von Software für das Funktionieren der gesamten IT-Infrastruktur. Diesmal half kein Patch für einen Abschnitt eines millionenfach eingesetzten Softwareprodukts, diesmal ging es um eine millionenfach individuell implementierte Softwarelösung, nach der Stück für Stück gesucht werden musste.

Y2K – Keine Pause für Sisyphus

In den Prognosen und Szenarien zum Y2K-Problem wurden bisweilen Auswirkungen in apokalyptischen Ausmaßen beschrieben. Den Jahreswechsel verbrachten IT-ExpertInnen von Regierungen, Banken, Energieversorgern, Einsatzleitstellen, militärischen Frühwarnzentren und vielen anderen in ihren Krisenzentren. Nachdem der Jahreswechsel ohne den befürchteten großen Crash vorüberging, wurden höhnische Kommentare laut, man sei auf eine umsatzsteigernde Aktion der IT-Industrie hereingefallen.

Reingefallen war man jedoch nur auf die Mechanismen der Medienöffentlichkeit, für die keinen Wert hatte, was nicht den hochgesteckten Katastrophenerwartungen entsprach. Das globale Bankensystem konnte nicht ausfallen, weil der Interbankenhandel einfach ausgesetzt wurde. Große deutsche Chemieunternehmen fuhren ihre umweltkritischen Anlagen herunter. Krankenhäuser operierten mit laufenden Notstromaggregaten. Allen Unkenrufen zum Trotz waren vorher in vielen Teilen von Wirtschaft und Verwaltung Hard- und Software ausgewechselt worden. Mit 6-stelligen Summen startete das Wirtschaftsministerium im Herbst noch eine Aufklärungskampagne zur Umrüstung für kleine und mittelständische Unternehmen. Die Bundesregierung konnte sich zum Jahreswechsel zuversichtlich zeigen, weil in den entsprechenden Gremien klar war, wie weit die Umstellung – ob Fehlerbehebung, Systemumstellung oder Abschaltung – gediehen war. Große Unternehmen – wie die Banken – prüften ihre IT-Systeme bereits seit 10 Jahren. Nach Schätzungen der Gartner Group sind allein in den USA 600 Milliarden Dollar für die Behebung des Y2K-Fehlers aufgewandt worden. Die Umstellungsarbeiten sind außerdem immer noch nicht abgeschlossen. In diesem Jahr werden die als nicht kritisch klassifizierten Systeme umgestellt.[1]

Und natürlich gab es zum Jahreswechsel Softwareprobleme: ein ausgefallenes japanisches Kernkraftwerk, unkontrolliert am Himmel trudelnde Satelliten, Stromausfall in einem afrikanischen Staat, fehlerhafte Buchungen bei Fluggesellschaften, fehlerhafte Kassensoftware bei einer großen Kaufhauskette. Doch diese erschienen als Probleme einzelner Staaten und Individuen und brachten nicht die Menschheit als Gesamtes in Gefahr. Spötter behaupten, dies seien etwa so viele Computerprobleme gewesen, wie an jedem normalen Tag. War diese Prophylaxe also umsonst?[2]

Kassandras des Cyberspace

Mit der Erleichterung über das Ausbleiben einer Katastrophe tritt die Frage nach der Verletzlichkeit der Informationsgesellschaft wieder in den Hintergrund. Nach dem die Defizitanalysen zum Y2K-Problem in die Schubladen gewandert sind, fällt lediglich der absolute Mangel an Informationen zur Art und Weise auf, welche Schäden ohne Umstellungsmaßnahmen gedroht hätten und wie diese Maßnahmen ausgesehen haben. Nur Einzelfälle gelangten an die öffentlichkeit. Gravierendes Beispiel hierzulande war der Totalausfall des Berliner Einsatzleitsystems der Feuerwehr,[3] der mindestens drei Tote forderte.

Zum mangelnden Problembewußtsein vor dem Y2K gesellt sich nun danach mangelnder Erfahrungsaustausch. Trotzdem allen Beteiligten und auch der interessierten öffentlichkeit die Abhängigkeit von funktionierenden IT-Systemen eindringlich vor Augen geführt wurde, hat sich die Diskussion um die systematische Verminderung der Verletzlichkeit der Informationsgesellschaft seit Ende der 80er Jahre nur geringfügig weiterentwickelt.

In ihrem grundlegenden Werk beschrieben Roßnagel, Wedde, Hammer und Pordesch 1989 ein Szenario, das weder etwas von seiner Aktualität eingebüßt hat, noch durch andere Sze-

1. Der eigentliche Test kommt noch. in: Süddeutsche Zeitung, 3.1.2000, S. 23
2. Es lebt. Wie konnte die Digitalwelt den Jahr-2000-Infekt überstehen? In: Süddeutsche Zeitung, 8./9.1.2000, S. 15
3. Richard Sietmann: Dumm gelaufen? Anatomie eines Computer-GAUs. in: c't, Heft 13, 2000, S. 216-226

narienentwürfe ersetzt wurde.[4] Darin brach in der informations- und kommunikationstechnologisch voll versorgten Stadt Düsselberg des Jahres 2019 durch den Ausfall von drei Kommunikationsvermittlungsstellen das Chaos aus. Ohne Datenaustausch brach der von Leitrechnern gesteuerte Verkehr zusammen, die per Datenleitung gesteuerte Warenzulieferung für produzierende Unternehmen ebenso wie für den Supermarkt an der Ecke funktionierte nicht mehr. Ohne Lagerhaltung brachen Produktion und Versorgung zusammen. Doch auch vorhandene Waren konnte niemand mehr kaufen, denn der elektronische Zahlungsverkehr, der das Bargeld weitgehend abgelöst hatte, war nicht mehr möglich. Polizei und Rettungsdienste konnten weder alarmiert noch koordiniert werden. Ohne Fernwirken und -messen konnten weder Brände noch Einbrüche erkannt werden. Es kam zu Einbrüchen und Plünderungen.

Wenn sich dieses Szenario liest wie viele der zum Y2K publizierten Schilderungen der Konsequenzen, so liegt dies zum einen an der Qualität der Vorausschau. Zum anderen läßt sich dank der Entwicklung des Internets und der dadurch viel enger gewordenen Verkopplung verschiedener Lebensbereiche ein viel weiter gehendes Schadensszenario entwickeln. Doch gehört dies allenfalls zum Repertoire jener, die über die Folgen von Information Warfare auf die zivilen IT-gestützten Infrastrukturen nachdenken.

Damit bewahrheiten sich wiederum die Ideen der Gruppe um Roßnagel, die noch von verschiedenen Problemursachen ausgingen. Nicht nur der vorsätzliche Mißbrauch, sondern auch fehlerhafte Konstruktion und Bedienung dieser IuK-Systeme waren für sie Ursachen dieser Gefahren. Ihrer Bewertung nach können die Gefahren bei Ausfall dieser IT-Systeme unverantwortbar groß werden, weshalb diese Systeme unter allen Umständen gegen Fehler und Störungen gesichert werden müssen. Fehlerfreie Systeme wird es auch in Zukunft nicht geben, doch kann wenigstens gegen den vorsätzlichen Mißbrauch stärker als bisher vorgegangen werden.

Möglichkeiten zur Umgehung technischer Mißbrauchssicherungen werden auch organisatorische Schutzmaßnahmen notwendig machen. Um den Mißbrauch zu erschweren, sah die Autorengruppe 1989 voraus, werden IT-Fachleute verstärkt Sicherheitsüberprüfungen unterzogen. Um den Mißbrauch durch Externe zu verhindern, wird es zu geheimdienstlicher Ausspähung und polizeilichen Aktionen gegen alle, die möglicherweise etwas gegen IT-Systeme unternehmen könnten, kommen.

Genau dies findet sich heute bei den US-Einrichtungen zum Schutz kritischer Infrastrukturen gegen sogenannte Cyberterroristen. Als Cyberterrorismus werden dabei generell Information Warfare-Aktivitäten durch Einzelne oder kleine Gruppen verstanden, genauer: »Anyone with the capability, technology, opportunity, and intent to do harm«.[5] Mit den heute im Internet frei angebotenen Manipulationswerkzeugen ist so gut wie jeder technisch nicht völlig laienhafte Internet-Nutzer zu schwerwiegenden Eingriffen in IT-Systeme in der Lage.

In einem Staat, in dem fast alle BürgerInnen Zugang zu IT-Systemen haben, ist aus diesen Argumentationsweisen zu folgern, alle Möglichkeiten der Überwachung und Kontrolle umfassend gegen die Mehrzahl der BürgerInnen einzusetzen. Die Umstände werden es dabei notwendig machen, Freiheitsrechte bis hin zu einem faktischen Grundrechtsschwund abzubauen. Bei dem Konflikt zwischen der Wahrung von Grundrechten des Individuums und der Sicherheit der Allgemeinheit vor Ausfall lebenswichtiger IT-Systeme werde nach Ansicht der Gruppe um Roßnagel auch das Bundesverfassungsgericht letztlich eine Güterabwägung zugunsten der Sicherheit treffen müssen.

Das Resümee dieser Überlegungen der Autorengruppe war 1989, daß ein Weg in die Informationsgesellschaft unter diesen Bedingungen nicht sozialverträglich ist. Das Resümee heute lautet, dass wir weder aus dem eher technisch gelagerten Y2K-Problem für die Zukunft gelernt haben, noch haben wir die letzten 10 Jahre dazu genutzt, die Probleme der Verletzlichkeit der Informationsgesellschaft auf eine sozialverträgliche Weise anzugehen. Statt dessen nehmen dank Information Warfare und Cyberterrorismus die Spielräume sozialverträglicher Gestaltung rapide ab.

Prometheus der universellen Maschine

In mythologischer Vorzeit hielten es die Götter für besser, der Menschheit das Wissen um die Nutzung des Feuers vorzuenthalten. Auch bei der Informatik lassen sich Nutzen und Schadenspotential nicht immer trennen. Die Zuständigkeit für die Bewertung der Folgen eines Einsatzes wird der Disziplin zugeordnet, die die IT-Systeme schafft. Professionelle Ethik-Kodices – allen voran der der association for computing machinery (acm), in Deutschland der Kodex der Gesellschaft für Informatik (GI) – verpflichten deshalb IT-Experten auf korrektes Arbeiten und vor allem zur Loyalität gegenüber dem Arbeitgeber in Form der Vermeidung von Schäden. Auch die in den USA immer wieder verfolgte Idee einer Zulassung von Softwareingenieuren verfolgt unter anderem einen ähnlichen Problemlösungsansatz, der einen Entzug der Zulassung beinhaltet, sofern der IT-Experte sein Wissen zu schädigenden Aktionen eingesetzt hat.

Die Grenzen einer solchen Selbstverpflichtung zeigen sich in dem Maße, wie das Programmierwissen nicht mehr auf wenige High-Tech-Länder begrenzt, sondern weltweit verfügbar ist. Der »I-love-you-Virus« zeigte zuletzt, dass Schadensverursacher heute beispielsweise aus philippinischen Programmierschulen kommen und mit einer

4. Alexander Roßnagel; Peter Wedde; Volker Hammer; Ulrich Pordesch: Die Verletzlichkeit der »Informationsgesellschaft«. Herausgegeben vom Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen, in der Reihe Sozialverträgliche Technikgestaltung, 1989.

5. http://www.pccip.gov/backgrd.html

Berufsethik allein nicht unter Kontrolle zu bringen sind.

Folgen haben derartige Aktionen auf die Form der Schadensregulierung. Die deutschen »Hackergesetze« stellen die schadensverursachende Manipulation von IT-Systemen unter Strafe. Die Überlegungen der EU zur Computerkriminalität, das sogenannte Cybercrime-Abkommen, weitet dies auf Nutzung und Verfügung über Werkzeuge aus, mit denen Sicherheitslöcher aufgespürt werden können. Die im deutschen Recht noch vorgesehene Möglichkeit IT-Systeme ohne Schädigungsabsicht auf Schwachstellen zu prüfen, würde damit unterbunden.

Gefährlich ist die prinzipielle Stoßrichtung dieser Initiative. Eigenart der Informatik ist es, dass für jede Sicherheitslösung ein Gegenmittel konstruiert werden kann. Solange der Computer als universelle Maschine verfügbar ist, läßt sich ein Programm entwerfen, mit dem bestehende Sicherheitslösungen umgangen werden können. Die freie Programmierbarkeit des Computers ist genauso die Grundlage seines Erfolgs wie die Ursache seiner Verletzlichkeit.

Treibt man den Gedanken an das Verbot der Verfügbarkeit sicherheitsrelevanter Software auf die absurde Spitze, so steht am Ende der Sicherung des Computers vor Manipulation die Kontrolle über Programmierwerkzeuge, also Programmiersprachen und Compiler.

Trotz einiger Tendenzen in diese Richtung sind weder die Kontrolle über Programmierer noch die über Programmierwerkzeuge eine ernst zu nehmende Perspektive zur Herstellung von IT-Sicherheit. Sollen heute nicht die Sachzwänge für einen zukünftigen Grundrechtsabbau geschaffen werden, muss die Gestaltung von IT-Systemen an anderen Zielen orientiert werden. Demokratieerhaltende konstruktive Ansätze zur Entwicklung von IT-Systemen bilden rechtliche Anforderungen[6] oder allgemeiner auch soziale Regeln[7] auf IT-Systeme ab.

Demokratie statt Plutokratie

Eine Lösung für IT-Sicherheit liegt damit sicherlich nicht in repressiven Ansätzen. Die theoretischen Gestaltungsmodelle für die Systementwicklung finden in der Praxis jedoch kaum Anwendung. Eine Lösung liegt daher eher zwischen diesen Polen.

Aus der Informatik sind Werkzeuge und Methoden bekannt, um sicherere Systeme zu entwickeln. Die Praxis mit Open Source liefert Alternativen zu den herkömmlichen unsicheren Systemen. Zugleich ist bei Open Source die Entstehung einer IT-Sicherheitskultur in Ansätzen zu beobachten. Wegen der Offenheit und damit der Prüfbarkeit von Sicherheitsaspekten unterstützen das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Bundesministerien für Inneres sowie das für Wirtschaft und Technologie (BMI und BMWi) Open Source-Projekte. Mit diesen Ansätze werden die Grundlagen dafür gelegt, um der Tendenz zur Kontrolle entgegenzuwirken. Geändert hat dies nichts daran, dass sich vor allem die großen Hersteller von IT-Systemen erfolgreich dagegen wehren konnten, irgendeine Form der Haftung oder Qualitätskontrolle für ihre Produkte normativ zu verankern. Damit hat die IT immer noch eine rechtliche Sonderrolle, bei der die Fehlerfreiheit eines Produkts nicht vorausgesetzt werden kann. Mit Open Source entsteht ein Ansatz zu verbesserter Qualität, dessen Bedeutung für die gesamte Branche sich jedoch erst noch zeigen muss.

Eine unzuverlässig arbeitende Informationstechnik als infrastrukturelle Grundlage einer Informationsgesellschaft konfligiert mit den Pflichten einer staatlichen Daseinsvorsorge. Eine Technik, die bei deren Ausfall ein zivilisiertes Zusammenleben gefährdet, bietet nicht die Sicherheit, um eine demokratische Informationsgesellschaft für alle gesellschaftlichen Interessen zu gestatten. Daseinsvorsorge setzt aber auch Hilfe zur Selbsthilfe und strukturelle Unterstützung im Sinne einer Chancengleichheit zwischen unterschiedlichen Marktteilnehmern voraus.

Dies setzt neben der Schaffung eines grundlegenden Problembewußtseins die Verfügbarkeit technischer Alternativen voraus. Voraussetzung für Alternativen ist der Erhalt und die Unterstützung von Vielfalt, die bisher vor allem durch die Forschung entwickelt wurde. Wenn Vertrauen die Basis der Informationsgesellschaft darstellt, so müssen die notwendigen Voraussetzungen geschaffen werden. Das muss auch heißen, vertrauenswürdige staatliche und nichtstaatliche Institutionen mit den notwendigen Ressourcen auszustatten, um eine Vertrauenskultur zu schaffen. Ultima ratio des Vertrauens in einen Rechtsstaat ist der Schutz individueller Grundrechte. Das bedeutet auch, als Grundverpflichtung der IT-Sicherheit rechtliche Mindestnormen zu definieren, wie dies die Forderung nach einem IT-Sicherheitsrahmengesetz illustriert.[8] Zusammen genommen heißt dies, den Interessen der Marktmächte demokratische Prinzipien entgegenzusetzen.

Von all diesen vielfältigen Aufgaben zur IT-Sicherheit ist bislang nur ein Bruchteil angegangen. Die Entwicklung der Informationsgesellschaft läßt nicht noch einmal 10 Jahre Zeit, um den weiter wachsenden Defiziten zu begegnen.

Fortsetzung des Editorial

Wenn es um die Gestaltung verläßlicher IT geht, so lehrt die Vergangenheit, dass die meisten Versuche Besserung aber keine Abhilfe bringen.

Auch der Versuch der repressiven Sicherung von IT gegen ihre Benutzer kann diese Lücke nicht schließen. Zerstörtes Vertrauen in die Sicherheit von IT-Systemen ist nicht wieder gut zu machen. Die Mehrheit der Nutzerinnen und Nutzer wird sich wichtigen Einsatzbereichen verweigern – E-Commerce ist ein Beispiel dafür. Marit Köhntopp beschreibt, dass die Einbeziehung vertrauenswürdiger Instanzen schon in den Entwicklungsprozess von IT-Systemen die Grundlage darstellt, um verlorengegangenes Vertrauen wieder herzustellen.

Die Verletzlichkeit der Informationsgesellschaft fordert die Verantwortung der InformatikerInnen heraus. Sie müssen sich nicht nur den gesellschaftlichen Konsequenzen der Sicherheitsdefizite ihrer Arbeit stellen. Es ist ihre Pflicht, eine grundrechtskonforme Gestaltung der Informationstechnik technisch auch zu realisieren.

Ute Bernhardt

6. Friedrich-L. Holl: Das Konzept der Ordnungsmäßigkeit von Informations- und Kommunikationssystemen. Dissertation. Paderborn, 1997
7. vgl. Volker Hammer: Normative Anforderungsanalyse am Beispiel der verletzlichkeitsreduzierenden Technikgestaltung; siehe Beitrag in diesem Heft
8. Ingo Ruhmann: Konsequenzen aus dem Jahr 2000 Problem; in: DuD, Nr. 7, 1999, S. 409-411

Christiane Schulzki-Haddouti

Kritische Infrastrukturen

Attacken auf Computernetze können nicht nur Firmen, sondern ganze Volkswirtschaften ruinieren. Während die USA bereits Milliarden in die Abwehr des Cyberwar investieren, denken deutsche Politiker gerade mal über mögliche Maßnahmen nach.

Bundeswirtschaftsminister Werner Müller beispielsweise ist überzeugt, dass »Unternehmen, die nicht in der Lage sind, ihre sensiblen Daten gegenüber Zerstörung, Diebstahl, Manipulation oder Ausspähung zu schützen, über kurz oder lang aus dem Wettbewerb ausscheiden« werden.

Die Bundesregierung selbst schützt sich mit einem Hochsicherheitsnetz, dem Informationsverbund Bonn-Berlin (IVBB) vor Hackattacken und Cyberspionen. Aus Sicherheitsgründen wurde ausschließlich von deutschen Firmen wie Siemens gebaut. Die meisten Unternehmenchefs in Deutschland kümmern sich jedoch nicht um die Sicherheit ihrer Netze. Für Norbert Pohlmann, Vorstandsvorsitzender des IT-Sicherheitsverbands Teletrust, ist klar: »Wenn der Chef keine Vorgaben macht, tun auch die Mitarbeiter nichts.« Immerhin zwei Drittel der deutschen Unternehmen gaben in einer Umfrage als Grund an, dass eine Zertifizierung »zu zeitaufwendig« und »zu kostspielig« sei.

Pohlmann plädiert dafür, dass die Unternehmen mehr Geld in Sicherheit investieren. Zum Beispiel nach US-Vorbild in privatwirtschaftliche Zentren, die Informationen über neue Viren austauschen und Abwehrmassnahmen entwickeln. Denn bis heute gibt es kein nationales Frühwarnsystem. Allein die Computer-Notfallzentren in Universitäten und Industrie, die CERTs, kooperieren locker mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Künftig soll die Zusammenarbeit zwischen den CERTs und dem BSI besser koordiniert werden. Doch Stefan Schneiders, Stratege in Sachen Informationssicherheit beim Münchner Siemens-Konzern sieht das nüchtern: »Das läuft nun unter einer neuen Überschrift. Die Industriefirmen tauschen sich schon jahrelang regelmäßig aus.«

Bereits seit drei Jahren beschäftigt sich auch eine kleine Arbeitsgruppe namens »Kritische Infrastrukturen« im BSI mit den Gefahren des Cyberwar. Zwar wurde eine erste Fassung ihres Berichts bereits bekannt, doch veröffentlicht ist er immer noch nicht. Zu den Empfehlungen gehört jedenfalls der Aufbau privater Informationszentren. Doch nicht nur aufgrund knapper Haushaltskassen, sondern auch aufgrund des gravierenden Fachkräftemangels steht dieses Projekt in den Sternen.

Auch empfehlen sie den Aufbau eines nationalen Alarmzentrums. Seine Aufgabe: Verfahren und Methoden entwickeln, um Angriffe auf Computer zu entdecken und auszuwerten, Betroffene zu alarmieren und Krisenmanagement zu betreiben. Falls die Meldestrukturen dieses Meldewesens für Alarmierungszwecke ungeeignet sind, »ist auch die Gründung eines nationalen Alarmzentrums in Erwägung zu ziehen«, heißt es in der noch nicht verabschiedeten jüngsten Version des Bericht, die immer noch nicht veröffentlicht wurde.

Die wenigen »Computer Emergency Response Teams« (CERTs) kooperieren bislang nur locker mit dem zuständigen BSI. Ein nationales Hacker-Frühwarnsystem gibt es in Deutschland, anders wie in den USA nicht. Die Idee mit dem Meldezentrum kommt Norbert Pohlmann, Vorstandsvorsitzender des IT-Sicherheitsverbands Teletrust, entgegen. Er wünscht sich, dass die Firmen nach Vorbild der USA private, straff organisierte Notfallzentren, die Informationen über neue Netz-Gefahren austauschen und Abwehrmassnahmen entwickeln.

Stefan Schneiders, Stratege für Informationssicherheit beim Münchner Siemens-Konzern, sieht in dem Meldezentrum jedoch eher eine PR-Aktion, da sich »die Industriefirmen schon jahrelang regelmäßig austauschen«. Die Einrichtung eines deutschen NIPC könnte noch etwas auf sich warten lassen. Denn die Kritis-Arbeitsgruppe empfiehlt in ihrem Bericht zuvor eine »fundierte Risikoanalyse« durchzuführen, die die Bedrohungen und Schwachstellen der kritischen Infrastrukturen untersucht. Sie soll auch potenzielle Schäden identifizieren und sie hinsichtlich Höhe und Eintrittswahrscheinlichkeit bewerten. Erst dann kann festgestellt werden, für welche Risiken die Betreiber einer Infrastruktur allein verantwortlich sind, und bei welche Risiken der Staat gefordert ist. Ebenso soll ein Plan für Abhilfe- und Schutzmaßnahmen entwickelt werden.

Generell solle der Staat als Vorbild handeln: »Für die kritischen Infrastrukturen, die sich in der Verantwortung des Bundes befinden« ist ein verbindlicher Plan zu erstellen, heißt es in dem Papier, darin sollen die kritischen Infrastrukturen benannt und notwendige Aktivitäten festgelegt werden. Auch müssen nationale und internationale Gesetze und Verträge überprüft werden, um zu sehen, ob sie einer Bedrohung der kritischen Computersysteme standhalten.

Anders ist das in den USA. Dort wird nicht mehr gekleckert, sondern geklotzt: Anfang diesen Jahres kündigte die Clinton-Regierung eine Erhöhung des Etats auf 2 Milliarden Dollar an. Das Geld fließt in die Aus- und Weiterbildung von Sicherheitsexperten innerhalb der Regierung sowie in die Forschungs- und Entwicklungsarbeit für Computersicherheit. Auch dem Fachkräftemangel auf dem Computerbereich will die Regierung entgegentreten: Computerstudenten erhalten Stipendien, wenn sie sich verpflichten, nach Abschluss des Studiums für die Regierung zu arbeiten. Um die Abwanderung hochqualifizierter Beamte in die Wirtschaft zu verhindern, werden ab nächstem Jahr staatliche IT-Experten nicht mehr mit dem Beamtentarif von 30.000 US-Dollar, sondern mit 100.000 US-Dollar entlohnt.

Für den US-Experten Wayne Madsen ist klar, dass der staatliche Kampf gegen Hacker, Cyberterroristen und feindliche Staaten der Politik gelegen kommt: »Das Verteidigungsministerium braucht nach dem kalten Krieg neue Feinde«. Der ehemalige NSA-Angestellte, der heute als Lobbyist für die Bürgerrechtsorganisation EPIC in Washington arbeitet, weiß, wie sich die Regierung auf den Cyberwar vorbereitet:

So hat das FBI das so genannte »National Infrastructure Protection Center«

(NIPC) eingerichtet, das Bedrohungsszenarien für alle möglichen Arten von Angriffen entwickelt – vom Eindringen in die Produktionssysteme einer Autofirma bis zum Angriff auf Stromversorgungssysteme oder Mailsysteme von US-Botschaften. In einer Datenbank werden Bedrohungen, Taktiken und Aktivitäten gesammelt und ausgewertet. Gefüttert wird sie mit Informationen aus den Geheimdiensten, den zivilen und militärischen Regierungsbehörden sowie dem privaten Sektor. Das NIPC wertet die Informationen aus und leitet sie zielgerichtet weiter.

Für das nächste Jahr plant das FBI unter dem Codenamen »Casa de Web« eine Datenbank, die Audiodateien, Abhörprotokolle, sowie deren Übersetzungen und Berichte speichern kann. Ein anderes Programm unter dem Codenamen »Digital Storm« soll den FBI-Agenten den Online-Zugriff auf gespeicherte Abhörbänder ermöglichen. Mit den Datenbanken können die Agenten Text und Sprache nach Schlüsselwörtern durchsuchen und Stimmprofile identifizieren.

Bereiten sich die USA bereits seit drei Jahren gezielt auf den Cyberwar vor, existiert in Deutschland nicht einmal eine Strategie. Als Clinton die 2 Milliarden zusagte, setzte Innenminister Otto Schily gerade einmal eine Task-Force aus Mitarbeiter des Bundesinnenministeriums, des Bundesamts für die Sicherheit in der Informationstechnik (BSI) sowie des Bundeskriminalamtes ein. Sie soll Bedrohungen für Deutschland analysieren und Gegenmassnahmen entwickeln. Bislang hat sie lediglich einen 15-Punkte-Katalog vorgestellt, von dem Fachleute sagen, dass er keinen neuen Ansatz verfolge.

Tatsächlich setzt das Innenministerium auf das Cybercrime-Abkommen, das derzeit vom Europa-Rat vorbereitet wird. Mark Richards, Verbindungsbeamter des FBI und des US-Justizministeriums in Brüssel, sagte, dass es »offensichtlich« sei, »dass wir effektive Regelungen entwickeln müssen, um uns gegenseitig in maximaler Kooperation, soweit dies uns aufgrund der nationalen Gesetze möglich ist, zu unterstützen.« Zu den wichtigsten Vorschlägen für das geplante Cybercrime-Abkommen (siehe anderen Beitrag in der FifF-Ko) gehören das Verbot von Hackerprogrammen, die Befugnis von Behörden Zugriff auf die Passwörter für einen Verschlüsselungsschlüssel zu erhalten, das Verbot des Besitzes kinderpornographischer Bilder sowie die Verpflichtung von Internetprovidern Kundendaten zu sammeln, um letztlich anonyme Remailer zu verhindern.

Kritische Infrastrukturen

Stromversorgung
1997 brachten 35 Spezialisten eines Red-Teams der US-Geheimdienste in einem Planspiel mit Hilfe von im Internet kursierenden Hacker-Tools weite Teile der US-Stromversorgung zum Erliegen.
Quelle: Center for Strategic and International Studies (CSIS): Cybercrime, Cyberterrorism, Cyberwarfare – Averting An Electronic Waterloo. 1998 (www.csis.org)

Militär
1998 unterbrachen zwei Jugendliche in Kalifornien die Truppenverlegung an den Golf unter der Regie des israelischen Hackers »The Analyzer«
Quelle: Center for Strategic and International Studies (CSIS): Cybercrime, Cyberterrorism, Cyberwarfare – Averting An Electronic Waterloo. 1998 (www.csis.org)

Gesundheitssystem
1994 veränderte ein britischer Hacker die Rezepte auf dem Rechner eines Krankenhauses – ohne die Aufmerksamkeit einer Krankenschwester wäre ein neunjähriger Junge durch die entstandene hochgiftige Mixtur gestorben.
Quelle: Studie »Kosten und Nutzen der IT-Sicherheit«, UIMC/BSI, 2000.

Verkehrssystem
1993 rast eine Lufthansa-Maschine in Warschau über die Landebahn hinaus. Ursache: Aufgrund eines Softwarefehlers setzte die Schubumkehr nicht rechtzeitig ein.
Quelle: Bericht der Ressort-Arbeitsgruppe Kritis, 03. Dezember 1999.

Energieversorgung
Im Juni 1999 schalten sich in der Nähe von Seattle/USA die Pumpen einer Benzin-Pipeline aufgrund eines Ausfalls des Steuercomputers nicht ab, zwölf Minuten lang ergießt sich Benzin in einen kleinen Fluss. Ein Funken löst eine Explosion aus. Die Folge: Drei Todesopfer.
Quelle: Bericht der Ressort-Arbeitsgruppe Kritis, 03. Dezember 1999.

Banken und Versicherungen
Der Anbieter einer falschen Website nahm 190.000 US-Dollar von 100.000 Investoren ein, die er mit dem Angebot einer imaginären High-Tech-Start-Up erzielt hatte.
Quelle: Center for Strategic and International Studies (CSIS): Cybercrime, Cyberterrorism, Cyberwarfare – Averting An Electronic Waterloo. 1998 (www.csis.org)

Telekommunikation
1997 Anschläge auf zentrale Netzknoten der Deutschen Telekom legen Kommunikationseinrichtungen des Frankfurter Flughafens lahm, das Klinikum der Universität Frankfurt wird von der Außenwelt abgeschnitten.
Quelle: Computerspionage. Risiken und Präventionen, Bundeswirtschaftsministerium (Hg.), Juli 1998.

Ingo Ruhmann

Papierberge ohne Ende

Schutz kritischer Infrastrukturen in Deutschland

Nachdem im Februar erstmals bis dato geheime Arbeitsergebnisse der AG KRITIS, Arbeitsgruppe zum Schutz kritischer Infrastrukturen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auf der FIfF-Tagung »Grundrechte in der Informationsgesellschaft« vorgestellt wurden, geistert die Existenz dieser Gruppe durch die Medien.[1] Der folgende Beitrag stellt die Hintergründe und Arbeitsergebnisse dieser AG KRITIS vor.

Jede Dollarmilliarde, die ein Ausfall von IT-Systemen kostet, bringt den Betroffenen für kurze Zeit die Bedeutung des Begriffes der Verletzlichkeit der Informationsgesellschaft zu Bewußtsein. Weil solche Schadenshöhen in aller Regel aber nur aufaddiert werden, nachdem wieder ein neuer Computervirus um die Welt ging, wird IT-Sicherheit vorschnell auf den Schutz vor Angriffen reduziert.

Angriffe auf IT-Systeme und der Schutz davor spielt seit einigen Jahren nirgendwo eine prominentere Rolle als in den USA, deren Militärs das Ausnutzen von Sicherheitslücken in IT-Systemen zu einem wichtigen Element für Information Warfare halten. Seit Mitte der 90er Jahre spielt der Schutz der eigenen IT-Infrastrukturen vor einem so genannten »elektronischen Pearl Harbour« eine zunehmende Rolle. Zur Risikoanalyse und Ausarbeitung von Gegenmaßnahmen setzte US-Präsident Clinton im Juli 1996 mit der Executive Order 13010 die Presidential Commission on Critical Infrastructures Protection (PCCIP) ein, die mit großem Expertenaufwand im Oktober 1997 einen umfangreichen Bericht vorlegte.[2]

Als kritische Infrastrukturen wurden dort Kommunikationsnetze, Energie- und Wasserversorgungsnetze, das Bankensystem, die Verkehrsinfrastruktur und die Notfall- und Behördendienste gesehen,[3] die jeweils spezifischen Gefährdungen ausgesetzt sind. Zum Schutz dieser Infrastrukturen wurden wiederum auf Anordnung des Präsidenten[4] verschiedene Einrichtungen gegründet. Die beiden wichtigsten sind das zu Strafverfolgungszwecken beim FBI eingerichtete National Infrastructures Protection Center (NIPC) und das Critical Infrastructure Assurance Office (CIAO), dem die Aufklärung der Öffentlichkeit obliegt. Ergänzt werden die staatlichen Maßnahmen durch Aktivitäten des privaten Sektors und einigen Forschungs- und Entwicklungsarbeiten.

Die Papierberge der AG KRITIS

In der Bundesrepublik brauchte es gewisser Anstöße von außen, um ähnliche Fragen wenigstens untersuchen zu lassen. Noch im Mai 1997 vertrat die Bundesregierung in einer Antwort auf eine Kleine Anfrage der Bündnisgrünen im Bundestag die Auffassung, eine der Kommission des US-Präsidenten zum Schutz kritischer Infrastrukturen vergleichbare Gruppe sei »nicht erforderlich«.[5] Nur etwa sechs Wochen nach dieser Antwort ging allerdings vom Bundesinnenministerium die Initiative zur Etablierung eines heute vom Bundesamt für Sicherheit in der Informationstechnik (BSI) federführend koordinierten Arbeitskreises »kritische Infrastrukturen« (AG KRITIS) aus, um genau diese Fragen untersuchen zu lassen. Erklärt wird dieser schnelle Sinneswandel heute damit, dass es gar keinen gegeben habe: Über das Ziel hätte Einigkeit bestanden, lediglich Umfang und Arbeitsaufwand der US-Kommission seien nicht auf Deutschland übertragbar gewesen.

So nahm im Sommer 1997 die AG KRITIS die Arbeit mit einer Erhebung der Lage im Verantwortungsbereich der einzelnen Bundesressorts auf, um in der Folge jedoch wenig von sich reden zu machen. An Anlässen für entsprechende politische Aktivitäten hätte es nicht gemangelt. 1998 und '99 gab es größere Virenfälle, die Bewältigung der Computerprobleme zum Jahr 2000 stand vor der Tür. Die Multimediaenquete des Deutschen Bundestages verabschiedete 1998 einstimmig einen ausführlichen Bericht zum Thema IT-Sicherheit, in dem – im Bewußtsein der Lage in den USA – eine nationale Sicherheitsinfrastruktur gefordert wurde, um »den vielfältigen Bedrohungsformen, wie sie mit dem Begriff Information Warfare zum Ausdruck kommen, geeignete Schutz- und Abwehrstrategien entgegenzusetzen«.[6]

Währenddessen erarbeitete die AG KRITIS unter Ausschluss der Öffentlichkeit eine Problemdarstellung und einige Vorschläge zur Problembehebung. Im parlamentarischen Raum und in Fachkreisen wurde nicht mehr bekannt, als dass die von den Fachleuten erarbeiteten Papiere der AG zu umfangreich und zu technisch ausgefallen seinen und erst in eine öffentlich vermittelbare Form gebracht werden müßten. Diese galt nach Fertigstellung allerdings wieder als zu wenig sachbezogen. Auf diese Weise soll inzwischen eine insgesamt zweistellige Anzahl verschiedener Kurz- und Langversionen entstanden sein. Offiziell abgenommen oder veröffentlicht ist auch drei Jahre nach Gründung der AG KRITIS keines der Papiere.

FIfF lupft den Vorhang: Ergebnisse von KRITIS

Bei dieser Ausgangslage versprach der erste öffentliche Auftritt des Koordinators der AG KRITIS, Joachim Weber (BSI) in der AG Information Warfare der Berliner Grundrechte-Tagung (vgl. dazu den Beitrag von Thilo Weichert in diesem Heft auf S. 4) bisher verborgene Einblicke in die Arbeit dieses Gremiums.[7]

Wie schon das US-Vorbild identifiziert die AG KRITIS als Bedrohungsziele die öffentlichen Versorgungsinfrastrukturen und weitet lediglich den Bereich der Gesundheitsversorgung etwas aus. Der Fokus der Bedrohung liegt ebenfalls nicht ausschließlich auf der Manipulation von Außen, sondern trägt der Tatsache Rechnung, dass Hacker und Viren je nach Studie nur zwischen 3 und 15% der schadensverursachenden Ereignisse ausmachen. Die überwiegende Mehrzahl von Computerausfällen und Datenzerstörung wird durch fehlerhafte Software und deren Nutzung verursacht.

Im Kern lassen sich die Ergebnisse der AG KRITIS als Schwachstellenanalyse verstehen. Diese fällt für den öffentlichen und privaten Bereich ausgesprochen unterschiedlich aus. Innerhalb der Bundesverwaltung brachte die Analyse die schon aus den Berichten des Bundesrechnungshofes bekannten deutlichen

Unterschiede in der Wahrnehmung von Sicherheitsrisiken. Die Ergebnisse für den privaten Sektor lassen nicht nur auf ein mangelndes Problembewußtsein, sondern zugleich eine mangelnde Bereitschaft schließen, sich zumindest im Rahmen der AG KRITIS mit dem Thema auseinanderzusetzen.

Undeutlich blieb die Antwort auf die eigentlich interessantes Frage nach den Bedrohungspotentialen. Die entsprechenden Einrichtungen in den USA halten jeden für einen potentiellen Cyberterroristen, der »über die Fähigkeit, Technologie, Möglichkeit und Absicht verfügt, Schaden anzurichten«.[8] Mit den heute im Internet frei angebotenen Manipulationswerkzeugen ist so gut wie jeder technisch nicht völlig laienhafte Internet-Nutzer zu schwerwiegenden Eingriffen in IT-Systeme in der Lage. Diese Ausweitung erhöht schlagartig die Zahl potentieller Gegner in einem Information Warfare und steigert die Bedrohung, gegen die wiederum militärische Antworten gesucht werden.[9] Nach Ansicht der AG KRITIS scheint dies nicht auf Deutschland übertragbar. Festlegen will sich aber auch niemand: So gilt einerseits die Bedrohungslage als entspannter, andererseits wird der Kosovokrieg herangezogen, um mögliche Risiken zu illustrieren.

Zentrales Problem scheint damit vor allem die mangelnde Bereitschaft der Wirtschaft zur Kooperation zu sein, die schon die Bestandsaufnahme erschwert hat. Die Lösungsvorschläge konzentrierten sich im Wesentlichen auf das weitere Sammeln von Informationen und das Erstellen von Bedrohungsanalysen – Aktivitäten, die bereits zu den genuinen Aufgaben des BSI für die IT-Infrastruktur der Bundesbehörden gehören.

Fazit

Solche Ergebnisse zur Lage der IT-Sicherheit in Deutschland könnten von jedem versierten IT-Sicherheitsunternehmen stammen. Dies kann nicht überraschen, wenn der Auftrag der AG KRITIS eine Beschreibung der IT-Sicherheitslage in Deutschland gewesen ist. Die Ergebnisse sind weniger aufregend als verschiedene Berichte des Bundesrechnungshofes der vergangenen Jahre und politisch weniger richtungsweisend als der zitierte Bericht der Bundestagsenquete. Die Ergebnisse liefern vor allem keine Erklärung, mit der sich sowohl die Heimlichtuerei bei der Arbeit der AG KRITIS als auch der Aufwand zur Erstellung größerer, aber unveröffentlichter Papiermengen begründen läßt.

Allenfalls der zwiespältige und abwartende Umgang mit dem Jahr-2000-Problem läßt einen Grund erahnen, Ergebnisse einer IT-Sicherheitskommission des Bundes nicht vor dem Jahr 2000 zu publizieren – schließlich wäre die Blamage groß gewesen, hätte es zum Jahreswechsel größere Schäden und einen dicken Bericht mit einer allgemeinen Analyse zu IT-Sicherheitsfragen gegeben. Doch auch nach dem 1.1.2000 konnte sich das Bundsinnenministerium nicht zu einem KRITIS-Bericht entschließen. Statt dessen gab die Berliner Tagung den Rahmen für einen kleinen Versuchsballon ab, der anschließend von den wichtigsten Presseerzeugnissen aufgegriffen wurde.

Mit dem Enquetebericht zu IT-Sicherheit liegt seit 1998 ein vom gesamten Bundestag getragenes politisches Grundsatzpapier zur Weiterentwicklung der IT-Sicherheit in Deutschland vor. Das Jahr 2000-Problem und danach Ereignisse wie der I-Love-You-Virus haben das Problembewußtsein geschärft. Dieses Klima hätte einer Debatte um IT-Sicherheit die nötige Aufmerksamkeit gesichert. Dieser Zeitpunkt wurde vertan. Die AG KRITIS stellt sich damit bei aller ordentlichen fachlichen Arbeit als politisch mißglückter Ansatz heraus, die Debatte um das Thema IT-Sicherheit ernsthaft voranzubringen.

1 Vgl.: Der Krieg der Mäuse; in: Der Spiegel Nr. 14/2000, S. 48-52
2 PCCIP: Critical Foundations. Protecting America's Infrastructures, Washington, Oct., 1997; http//www.pccip.gov/report_index.html
3 http://www.ciao.gov/
4 Zur erlassenen Presidential Decision Directive 63 vgl.: PDD 63: Protecting America's Critical Infrastructures; www.ciao.gov/63factsheet.html
5 Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Dr. Manuel Kiper: Lage der IT-Sicherheit in Deutschland, Bt.-Drs. 13/7753, Frage 38
6 Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft. Deutschlands Weg in die Informationsgesellschaft. Deutscher Bundestag (Hg.): Sicherheit und Schutz im Netz, Vierter Zwischenbericht der Enquete-Kommission, Bonn, 1998, S. 198
7 Mittlerweile ist eine Kurzversion der AG Kritis Ergebnisse unter http://cryptome.org/Kritis-12-1999.html
8 So die Definition unter http://www.pccip.gov/backgrd.html, Übers.: d.A.
9 vgl. dazu: Ingo Ruhmann: Cyberterrorismus – Das Internet unter Kriegsrecht? In: Sicherheit und Frieden, Heft 2, 2000, S. 144-149

padeluun und Rena Tangens

Big Brother Award

Eine kleine Meldung im Webmagazin TELEPOLIS[1] versprach Grosses: »FoeBuD: Wir machen das!«

Big-Brother-Preis bald in Deutschland. FoeBuD [http://www.foebud.org/], der Bielefelder Verein für sozialverträgliche Technikgestaltung, will im nächsten Frühjahr den Big-Brother-Preis nach Deutschland holen. Gegenüber Telepolis kündigte padeluun für den Verein an, die Verleihung in Kooperation mit anderen Organisationen organisieren zu wollen: »Wir machen das!«.Thilo Weichert, Vorsitzender der Deutschen Vereinigung für Datenschutz (DVD [http://www.aktiv.org/DVD/]) sagte eine Beteiligung bereits zu. Eventuell werden sich auch das FIfF- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung – sowie der CCC der Aktion anschliessen. Erstmals wurde der Preis unter grossem Medienecho vor einem Jahr von der Bürgerrechtsorganisation Privacy International anläßlich des fünfzigsten Jahrestages von George Orwells »1984« an Behörden, Firmen und Projekte verliehen, die »das meiste getan haben, um die Privatsphäre zu verletzen«. Im April 1999 wurde er erstmals in den USA, in London der UK Big Brother 1999 und auch in Österreich verliehen.«

Immerhin.

Big Brother Award Deutschland

England, Österreich und auch die USA haben es vorgemacht, nun soll es ihn auch in Deutschland geben: Den »Großen Bruder Preis«. Jeweils eine Firma, Organisa-

tion oder Institution wird oder werden ausgeguckt, die in einer Art mit personenbeziehbaren Daten umgeht, die den legalen, aber illegitimen Gebrauch (auch von dritter Seite) ermöglicht, fördert oder (heraus)fordert. Der Big Brother Award Deutschland soll eine Aufforderung zum öffentlichen Dialog für mehr Technologieakzeptanz sein.

Initiator und Organisator des Big Brother Award Deutschland ist der FoeBuD e.V.[2] in Bielefeld. Es sollen möglichst alle Organisationen, die sich in Deutschland mit der Thematik Datenschutz / Bürgerrechte beschäftigen, einbezogen werden, damit die Fachkompetenz aller dieser Organisationen zusammenfließen kann. Somit ist die Möglichkeit gegeben, dass die Zusammenarbeit über diesen Anlass hinaus Wirkung entfalten kann.

Die Figur aus dem Science Fiction Roman »1984« von George Orwell gab dem Preis, der in Großbritannien seinen Ursprung hat seinen Namen.[3] Obwohl im Buch Orwells vor allem die Angst vor dem (faschistischen) Überwachungsstaat thematisiert wird und die Datenmacht heute eher in privater Hand liegt, haben wir uns entschlossen – auch wegen der internationalen Zusammenarbeit – den Namen beizubehalten.

Warum einen Big Brother Award?

Datenschutz ist die Voraussetzung dafür, dass neue Technik akzeptiert wird. Der Schutz des Bürgerrechts auf Privatsphäre ist wichtig. Nicht nur der legale Umgang mit Daten, sondern auch der legitime Umgang damit beschäftigt die Menschen. Deutschland hat – sicher auch durch die Erfahrungen mit dem Dritten Reich angespornt – ein anerkannt gutes Datenschutzgesetz. Dennoch existieren viele Lücken und Schlupflöcher; z. B. was den Datenexport in datenverarbeitende Länder ohne Datenschutzgesetz, wie die USA, betrifft. Den Datenschutzbeauftragten fehlen oft die Mittel – und im Bereich der Datenverarbeitung in privaten Firmen – auch die Handhabe, um eingreifen zu dürfen oder zu können.

Datenschutz war lange Jahre ein Thema, das nur wenig Beachtung in der Öffentlichkeit fand. Vielen war die Materie zu komplex – zumal die meisten Menschen keinerlei Erfahrungen mit Datenbanken und deren Verfügbarkeit hatten. Heute, nach der Ausbreitung des Internet und Heimcomputern in fast jedem jungen Haushalt, können viele Menschen ahnen, welche Gefahren das Sammeln und Verknüpfen von Daten in sich birgt. Hier fehlt konkrete Aufklärung. Diffuse Ängste verhindern bisher eine allgemeine Akzeptanz z. B. neuer Bestellwege und wirkt sich sogar als Bremse im von Selfmade-Propheten so geliebten eCommerce aus.

Hier kann der Big Brother Award Deutschland katalysierend wirken: Er spricht Mißstände aus, die sowohl die Industrie, als auch die VerbraucherInnen zum Nachfragen, –denken und –bessern anregen können.

Presse und Medien bekommen Thema, aktuellen Anlaß, Bilder, Töne und Menschen geliefert, die den öffentlichen Diskurs anregen können. So ist zum Beispiel angedacht, einfache und verständliche didaktische Modelle zur Darstellung der Problematik zu erarbeiten und der Presse zur Verfügung zu stellen.

Wie sieht die Verleihung aus?

Die Verleihung wird öffentlich stattfinden. Es ist daran gedacht in einem gehobenen Kulturambiente (Theater) eine Feierstunde abzuhalten. Der Preis selber wird jeweils von unterschiedlichen Künstlerinnen oder Künstlern hergestellt (dieses Jahr von – so die Planung – Peter Sommer). Kultur soll hier als Vermittlerin einer für die Betroffenen unangenehmen Wahrheit dienen. Die Institution, die den Preis gleichzeitig mit der Erklärung der Gründe erhält, wird zur Verleihung Redezeit eingeräumt bekommen. Sie erhält somit nicht nur die Möglichkeit, Stellung zu beziehen, sondern kann auch über Konsequenzen reflektieren. Unsere Erfahrung zeigt, dass die Problematik oftmals gar nicht klar ist, und Unternehmen erst durch Dritte auf Missstände und Unschönes hingewiesen werden. Sollte ein Unternehmen, eine Organisation oder sonstige Institution die Redezeit nicht annehmen, ließe sich auch dies in den Medien thematisieren.

Ein Rahmenprogramm mit Kabarett oder einer kurzen Aufführung einer Theatergruppe und eine Musikdarbietung, die das Thema reflektieren, runden das Geschehen ab. Hier bietet sich auch ‚Material' für Kameras und Mikrofone, das die Berichterstattung etwas bunter gestalten kann.

Eingeladen werden neben Presse und Medien Honoratioren und Interessierte.

Wir haben bereits Zusagen von Leitmedien, dem Big Brother Award Deutschland große Aufmerksamkeit zu widmen. In Fact: Häufig wird angefragt, wann es denn endlich was konkretes gäbe. Dazu komme ich weiter unten.

Wie wird entschieden?

Es wird eine Jury aus Mitgliedern der beteiligten Organisationen zusammen gestellt. Diese wird über den genauen Ablauf entscheiden. Das bisher angedachte Prozedere stellen wir uns wie folgt vor:

- Die beteiligten Organisationen reichen Vorschläge ein
- Der Jury werden ggf. vom FoeBuD bereits redaktionell bearbeitete Vorschläge vorgelegt. Jedes Jurymitglied hat die Möglichkeit die Rohdaten zu überprüfen.
- Die Jurymitglieder sind verpflichtet Angaben nachzurecherchieren
- Die Anzahl der Jurymitglieder ist ungerade.
- Die Jurymitglieder sind zur Verschwiegenheit verpflichtet. Es ist ihnen nicht gestattet aus Ihrer Tätigkeit für den Big Brother Award Deutschland Vorteil zu ziehen (z. B. Aktienhandel mit Anteilscheinen betroffener Firmen ist innerhalb einer noch zu bestimmenden Frist untersagt).
- Es ist nicht möglich, ein rein objektives Urteil zu fällen. Da der Big Brother Award Deutschland eine Aufforderung zum öffentlichen Dialog sein soll, kann auch die erwartete Dialogbereitschaft ein Kriterium sein. Alle Kriterien, die die Verleihung bedingen, werden von der Jury schriftlich dargelegt.
- Innerhalb der Jury wird geheim abgestimmt. Gegenseitige Beeinflussung und Stimmenkauf dürfen nicht möglich ist.
- Eventuell wird mehr als ein Preis vergeben oder es erfolgen Nennungen. Zu überlegen ist, ob auch Nominierungen (mit Begründung) veröffentlicht werden sollten. Auf jeden Fall müssen dann aber auch Kommentare der Betroffenen möglich sein. »And the Looser is ...«
- Oberste Regel: Fair Play.

Wie setzt sich die Jury zusammen?

Es ist angedacht, daß verschiedene Organisationen den Big Brother Award Deutschland mittragen und die Jury stellen. Als im letzten Jahr (Herbst 1999) die Medien die Nachricht vom Big Brother Award Deutschland verbreiteten (siehe Anlage), haben sich spontan Menschen und Organisationen zur Mitarbeit bereit erklärt.

Publikumsbeteiligung und -preis

Über die Website www.big-brother-award.de (auch adressierbar unter www.bigbrotheraward.de) können alle, die das wollen, Vorschläge einsenden. Einsendungen sind auch per herkömmlicher Post möglich. Alle in Frage kommenden Vorschläge werden nachrecherchiert. Nichts wird ungeprüft übernommen. Auf der Website können Interessierte ein Votum für den Publikumspreis abgeben. Die Jury selbst soll sich nicht an Popularitäten orientieren.

Termin

Die Verleihung findet am 26.10.2000 statt. Es wird überleget, ob eine Synchronisation mit den Organisationen in Österreich, England und der Schweiz wünschenswert ist. Hierfür wäre der oben genannte Termin unerläßlich. Wir sind in der Termingestaltung nicht ganz frei, da die gewünschte Location (Theater) nicht zu jedem Zeitpunkt zur Verfügung stünde.

Wer ist der Organisator?

Der FoeBuD e.V. wurde 1987 als »Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs« in Bielefeld gegründet. Bekannt wurde er durch seine politische Vernetzungsarbeit im Zerberus-Netz inklusive der Mitarbeit an der Software; die Erfindung der »Mediencafés«; die Veranstaltungsreihe PUBLIC DOMAIN zu Themen aus Zukunft und Technik, Wissenschaft und Politik, Kunst und Kultur; das Friedensnetzwerk ZaMir, das in den Ländern des kriegsführenden Jugoslawiens aufgebaut wurde sowie das »Promoten« und die Herausgabe der deutschsprachigen Anleitung des Verschlüsselungsprogramms PGP. Mitglieder des FoeBuD berieten die Enquetekommission »Zukunft der Medien« des Deutschen Bundestages und erhielten 1998 den Medienpreis »Sinnformation« der Grünen Bundestagsfraktion.

Aus welchen Töpfen kommen die Finanzmittel?

Im Rahmen der Förderung der Technologieakzeptanz sollen die benötigten Mittel (ca. 170.000 DM) aus dem Etat des Bundeswirtschaftsministeriums kommen. Jede beteiligte Organisation ist gehalten, sich am Eigenanteil zu beteiligen. Speziell die erste Veranstaltung, die als Pilotprojekt gelten mag, ist aus eigenen Mitteln zu finanzieren. Denkbar wäre es auch, wenn die Veranstaltung jedes Jahr von einer anderen Organisation ausgeführt werden würde.

Die Realität

Jetzt erst nach der Sommerpause kann mit der Umsetzung richtig begonnen werden. Auch beim FoeBuD sind die Resourcen knapp; nach wie vor ist ernsthafte politische Arbeit, die neben dem Mainstream läuft schwierig und bedarf des Verständnisses vieler, die mit eingebunden sind. Der oben genannte Etat ist für dieses Jahr nicht vorhanden. Er wird auch nicht durch Zusammenlegen von Geld der beteiligten Organisationen zusammen zu bringen sein. Auf diese Art ist es evtl. möglich, einen Teil der reinen Sachkosten abzufedern. Und bis dahin muss mit den Resourcen gearbeitet werden, die eben vorhanden sind.

Hoffen wir mal, daß die kleinen vorhandenen Etats nicht nur für Spiel+Spaß draufgehen, sondern auch noch ernsthaft und trotzdem nicht langweilige politische Arbeit möglich ist.

You're welcome: www.big-brother-award.de
(padeluun)

1 www.heise.de/tp
2 www.foebud.org
3 www.privacy.org

Christiane Schulzki-Haddouti

Bundesregierung nimmt Stellung zu Cybercrime-Abkommen

Der Europarat arbeitet seit längerem an einem »Übereinkommen über Datennetz-Kriminalität« (Convention on Cyber Crime), das mittlerweile schon in der 19. Entwurfsfassung (http://conventions.coe.int/treaty/en/projets/cybercrime.htm) vorliegt. Damit wollen die EU-Mitgliedsstaaten gemeinsam mit den dem Europarat angeschlossenen Staaten wie den USA, Japan, Kanada oder Südafrika gezielt gegen Online-Kriminalität vorgehen. Auf dem Programm stehen das Verbot von Hackertools, bestimmte Vorgehensweisen zur Überprüfung von Email-Inhalten, das Einfrieren von Kommunikationsdaten (Artikel 16 und 17) und ein gemeinsames Vorgehen gegen Kinderpornographie.

Offizielles Ziel des Übereinkommens ist es, einen »gemeinsamen strafrechtlichen Mindeststandard« im Bereich des Computer- bzw. Telekommunikationsstrafrechts zwischen den Mitgliedsstaaten zu erreichen. Zum anderen wollen die Staaten »gemeinsame Grundlagen für effektive und rasche strafrechtliche Ermittlungen« erarbeiten, die den Zugriff

auf »relevante Computerdaten« ermöglichen.

Reif für das Führungszeugnis

Besonders umstritten ist Artikel 6: So soll die Produktion, der Verkauf, das Bereitstellen für die Nutzung, der Import strafrechtlich verfolgt werden können, wenn es sich um Passwörter, Zugangscodes, Mittel wie Computerprogramme handelt, deren primärer Zweck es ist, Daten und Systeme auszuspähen und zu verändern. Auch der Besitz kann schon strafbar sein, wenn üble Absichten dahinter stehen.

Ebenfalls soll es nach Artikel 10 künftig von strafrechtlichem Belang sein, wenn urheberrechtsgeschützte Werke ohne Befugnis per Computer genutzt und verteilt werden. Die strafrechtliche Seite ist hierbei von erheblicher Bedeutung: Eine illegale MP3-Kopie im jugendlichen Übermut gezogen – und schon ist der künftige Cybertäter reif für den Eintrag ins Polizeiliche Führungszeugnis. Dies entspricht schon seit langem den Forderungen der Musikindustrie, die sich mit dieser Verschärfung jedoch bislang nicht durchsetzen konnte.

Ungewohnte Öffentlichkeit

Den SPD-Bundestagsabgeordneten Jörg Tauss (www.tauss.de) wurmte es, im Herbst von den Arbeiten aus der Presse erfahren zu müssen und wandte sich Anfang Juni mit einer kleinen Anfrage an die Bundesregierung. Die Antworten des Bundesjustizministeriums (http://www.bundesjustizministerium.de/) liegen seit Mitte Juni vor.

Dabei weist der parlamentarische Staatssekretär Eckhart Pick darauf hin, dass mit dem Entwurf »zum ersten Mal bisherige Ergebnisse der Beratungen eines Sachverständigenausschusses des Europarates und seiner Arbeitsgruppe« der »Öffentlichkeit zugänglich gemacht« wurden. Dies sei auch auf »das Drängen der deutschen Ausschussmitglieder zurückzuführen« und von der Bundesregierung unterstützt. Ziel sei eine öffentliche Debatte »schon vor der Umsetzung«.

Damit bestätigt Pick auch, dass die bisherigen Diskussionen unter Ausschluss der Öffentlichkeit stattfanden und derartige Abkommen, so zuletzt auch das Europäische Rechtshilfeabkommen erst veröffentlicht wurden, nachdem sie verabschiedet worden waren.

Abhören bleibt geheim

Artikel 18 und 28 wurden allerdings nicht veröffentlicht. Sie behandeln das »Abhören« und sind noch »in Diskussion«. Hier geht es nicht um Regelungen zum Abhören von Telekommunikation, sondern von Computern und Datenleitungen. Diskutiert wurden sie bereits in den berüchtigten Enfopol-Papieren, versuchsweise umgesetzt in verschiedenen Entwürfen zur Telekommunikationsüberwachungverordnung.

Andy Müller-Maguhn, Sprecher des Computer Chaos Clubs, gegenüber Telepolis: »Hier muß auch dem Beobachter mit der größtmöglichen Naivität gegenüber der Eindruck aufkommen, man habe etwas zur verbergen.«

Verhandlung ist Regierungssache

Nicht-Regierungs-Organisationen sind bislang am Erörterungsprozess allerdings nicht beteiligt. »Dass man hier von seitens der Bundesregierung nicht einmal entsprechenden Diskussionsbedarf sieht, werte ich als Indikator für die Tatsache, daß man sich mit dem Entwurf der Cyber Crime Convention inhaltlich noch gar nicht auseinandergesetzt hat«, kritisiert Müller-Maguhn.

Federführend ist innerhalb der Bundesregierung das Justizministerium bei den Verhandlungen. Ebenfalls beteiligt sind der Bundesdatenschützer Joachim Jacob (http://www.bfd.bund.de/), das Bundeskriminalamt (www.bundeskriminalamt.de), das Bundesamt für Sicherheit in der Informationstechnik (BSI – www.bsi.de) sowie der Bundeskulturbeauftragte Michael Naumann (http://www.heise.de/tp/deutsch/inhalt/co/1545/1.html). Direkt an den Gesprächen in Straßburg sind ein Vertreter des Justizministeriums sowie des Bundeskriminalamtes. Seit Herbst 1999 sind auch die Landesjustizverwaltungen beteiligt, die Stellungnahmen von Richtern und Staatsanwälten einholten. Bis Ende des Jahres sollen die Ausschussarbeiten abgeschlossen sein.

Chaos Computer Club fordert Förderung von Angriffswerkzeugen

Für Müller-Maguhn »erschreckend« ist hierbei, »daß die Auseinandersetzungen mit dem Entwurf der Cyber Crime Convention und die bisherigen Abstimmungsprozesse innerhalb der Bundesregierung offenbar frei jeglichen technischen Sachverstandes stattgefunden haben.«

Einem Richter erscheine es noch einleuchtend, ein Angriffswerkzeug zu verbieten. Doch, so Müller-Maguhn weiter: »Jeder, der sich ein bisschen mit Technologie auskennt, weiß, dass ein Verbot von Angriffssoftware nicht nur völlig sinnfrei, sondern im Gegenteil sogar kontraproduktiv ist, weil damit ein Werkzeug zur Überprüfung der Sicherheit von Systemen kriminalisiert wird.« Er fordert deshalb die Bundesregierung auf, »im Interesse der Sicherheit von Systemen gerade die Erstellung solcher Software und ihres Einsatzes – auch innerhalb der Bundesregierung – zu fördern«.

Der gedankliche Unterbau

Als Ausgangspunkt für das Übereinkommen dient laut Pick die Empfehlung (89) 9 des Europarates über Computerstraftaten mit dem Bericht des Lenkungsausschusses des Europarates und Leitlinien für den nationalen Gesetzgeber und die Empfehlung (95) 13 über informationstechnologische Probleme des Strafverfahrensrechts.

Berücksichtigt wurde auch der Zwischenbericht der Enquete-Kommission »Zukunft der Medien« zur »Sicherheit und Schutz im Netz«. Dabei kritisiert Müller-Maguhn, dass man das Dokument »aufgrund eines offensichtlich rein juristischen Blickwinkels wohl nicht verstanden« habe, dort allerdings einen Absatz gefunden habe, der eine juristische Maßnahme wie Strafen für die Erstellung beziehungsweise Verbreitung von Viren für eventuell sinnvoll hält.

»Intensive« Rolle der USA

Kein Wort verliert Pick allerdings zu den Empfehlungen der G-8-Arbeitsgruppe High-Tech-Kriminalität, die den Europarat seit Jahren zuarbeitet. Geleitet wird diese Arbeitsgruppe bis heute von einem hohen Beamten des US-Justizministeri-

ums. Das US-Justizministerium ist jedoch neben dem US-Innenministerium und dem FBI »als beim Europarat zugelassener Beobachter von Anfang an intensiv beteiligt«. Amerikanische Wünsche seien berücksichtigt worden, »insbesondere um eine gute vertraglich gesicherte internationale Zusammenarbeit zu gewährleisten«.

Für Müller-Maguhn ist die Handschrift der amerikanischen Regierung »deutlich« zu erkennen. Müller-Maguhn: »Der amerikanische Einfluss auf das Geschehen wird hier schlicht mit Verweis auf die sinnvolle globale Kooperation verharmlost.« Anstatt Maßnahmen zur Sicherheit zu ergreifen, sei es die »favorisierte Vorgehensweise der amerikanischen Regierung« einfach Angriffswerkzeuge zu verbieten und staatliche Netzüberwachung zu fordern. Er bezweifelt, dass es im deutschen Justizministerium dafür überhaupt ein Problembewusstsein gibt.

Dörte Neundorf

Jugendschutz im Internet

Technische Möglichkeiten

Einleitung

Das Internet stellt mit seiner schnellen und direkten Publikation von Inhalten, die ohne Vermittlung direkt vom Autor zum Leser gelangen, den Jugendschutz vor neue Herausforderungen. Weder greifen die bekannten Kontrollmechanismen, die bisher immer auf menschliche Mittler setzten – Videotheken, Kinokassen, Zeitschriftenhändler –, noch läßt sich der Jugendschutz im internationalen Kontext mit nationalen rechtlichen Vorschriften durchsetzen. Andererseits wächst durch die große Menge von Informationen, die im Internet publiziert werden, die Menge des potentiell jugendgefährdenden Materials beträchtlich.

Um diesen Entwicklungen Rechnung zu tragen, wurden mit dem Informations- und Kommunikationsdienste-Gesetz (IuKDG) 1997 auch neue Jugendschutzregelungen in Deutschland eingeführt. Der Ansatz dabei war, daß sich die Indizierung gemäß dem geänderten »Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte« (GjS) jetzt auch auf Inhalte von Webseiten beziehen kann. Zusätzlich wurde ein neuer Absatz in das GjS aufgenommen, wonach eine indizierte Schrift nicht »durch elektronische Informations- und Kommunikationsdienste verbreitet, bereitgehalten oder sonst zugänglich gemacht werden« darf.

Im Kontext der Evaluierung des IuKDG sollte die im Auftrag des Bundesministeriums für Wirtschaft und Technologie von der Secorvo Security Consulting GmbH erstellte Studie »Jugendschutz und Filtertechnologien im Internet« untersuchen, welche technischen Möglichkeiten zur Umsetzung von Jugendschutz im Internet existieren, sie auf ihre Eignung zu überprüfen und Vorstellungen zu entwickeln, wie diese Techniken so erweitert werden können, daß eine sinnvolle technische Unterstützung des Jugendschutzes im Internet möglich ist. Als Randbedingungen waren dabei die technische und organisatorische Machbarkeit, der rechtliche Rahmen und die psychologisch-soziologische Durchsetzbarkeit zu berücksichtigen.

Schon vor Beginn der Studie war klar, daß der Gefährdung auf technischem Wege allein – durch Filterung der Information – nicht begegnet werden kann. Analog zu herkömmlichen Medien ist eine Umgehung rein technisch-organisatorischer Maßnahmen immer möglich. Als Baustein in einem Gesamtkonzept aus Technik und (medien-)pädagogischer Begleitung von Kindern und Jugendlichen durch Eltern und Lehrer kann sie aber – Funktionsfähigkeit vorausgesetzt – den Jugendschutz sinnvoll unterstützen. vor diesem Hintergrund sollte die Betrachtung der technischen Aspekte geschehen.

Der folgende Artikel faßt die Ergebnisse der Studie zusammen.[1] Da die Arbeiten an der Studie bereits im letzen Jahr abgeschlossen wurden, werden in einem zusätzlichen Abschnitt einige aktuelle (Weiter-)Entwicklungen zusammengefaßt.

Ausgangslage

Alle in der Geschichte der Kommunikation vor der Verbreitung des Internet eingesetzten Verfahren zur Publikation von Informationen waren entweder auf einen sehr kleinen Teilnehmerkreis beschränkt oder benötigten die Kooperation mehrerer Individuen zur Produktion und Verbreitung der Inhalte.

Das Internet ist eine Verkürzung dieser Kette: Es kommt zur direkten Kommunikation zwischen Autor und Leser, die eine vereinheitlichte Kommunikationsinfrastruktur nutzen. Diese Infrastruktur ist rein technisch und hat damit im Gegensatz zu herkömmlichen Publikationsverfahren keinerlei Einfluß auf die veröffentlichten oder kommunizierten Inhalte. Auch das Wissen um die Inhalte liegt ausschließlich bei Autor und Leser; es gibt keine zwischengeschalteten Instanzen. Im einzelnen heißt das:

- Die Inhalte können von jedem Nutzer, also auch von Kindern und Jugendlichen, jederzeit abgerufen werden, keinerlei Abläufe (»Fernsehprogramm«) oder transportbedingte Verzögerungszeiten schränken diese Freiheit ein.
- Es gibt keine zwischengeschalteten Kontrollen zwischen Anbieter und Abrufer (wie z.B. Videotheken, Fernsehsender oder Kinobetreiber im Falle des Mediums »Film«).
- Die Wahrscheinlichkeit eines zufälligen Abrufes von (unerwünschten) Informationen ist weitaus größer als bei herkömmlichen Medien.
- Für Anbieter und Abrufer gelten häufig verschiedene Regulative; eine Durchsetzung von rechtlichen Vorschriften ist also schwierig.

So ist zum Beispiel ein Zugang zu jugendgefährdendem – speziell pornographischem –Material leicht möglich, wenn

explizit danach gesucht wird. Suchvorgänge nach einfachen Schlagwörtern – »Sex«, »Porno«, »Gewalt« – liefern eine große Anzahl von einschlägigen Treffern. Spezielle Newsgroups oder besondere Ratgeber liefern weitere Links auf erotische Seiten, von denen eine Verzweigung auf jugendgefährdende Seiten einfach möglich ist.

Neben dem absichtlichen Aufsuchen solcher Angebote besteht eine hohe Wahrscheinlichkeit von Zufallstreffern: Auf häufig aufgerufenen Seiten – Telefonverzeichnisse, Suchmaschinen – findet sich Werbung für Erotikanbieter. In eigentlich »harmlosen« Newsgroups werden entsprechende Nachrichten veröffentlicht, die Hinweise z.B. auf Erotikanbieter enthalten und den Browser z.T. direkt zum Öffnen der jeweiligen Einstiegsseite veranlassen. Und schließlich können auch Suchvorgänge nach harmlosen Schlüsselwörtern zu Verweisen auf jugendgefährdende Angebote führen, wenn in diesen Seiten absichtlich irreführende Schlagwortangaben vorgenommen wurden.

Zwar müssen jugendgefährdende Seiten in Deutschland zugangsbeschränkt sein. Im Ausland gilt dies jedoch für einen Großteil der entsprechenden Seiten nicht. außerdem lassen sich solche Zugangsbeschränkungen meist durch Eingabe einer Kreditkartennummer oder einer anderen Zahlungsverbindung zumindest zeitweise umgehen.

Technische Möglichkeiten

Technische Ansätze

Die Unterbindung der Übertragung bestimmter Inhalte im Internet kann auf verschiedenen Ebenen geschehen:

Die Verbindung kann physikalisch getrennt werden. Damit ist jeder Datentransfer unmöglich. Für den Jugendschutz hieße das, Kindern generell den Zugriff auf das Internet zu untersagen.

Es können IP-Adressen oder Ports blockiert werden. Damit werden ganze Server nicht mehr erreichbar.

Schließlich kann auf der Anwendungsschicht eingegriffen und einzelne URLs oder Message-IDs gefiltert werden.

Die ersten beiden Ansätze sind zur Inhaltsfilterung ungeeignet, da hier immer ganze Teilbereiche des Internets mit sehr inhomogenen Inhalten gleichzeitig gesperrt werden. Um einzelne »Inhalte«, d.h. z.B. einzelne Seiten oder sogar nur spezielle Bilder auf einer Seite zu filtern, ist der Eingriff auf der Anwendungsschicht der einzig gangbare Weg, da nur hier überhaupt eine Chance besteht, eine paßgenaue Filterung zu erreichen.

Kategoriensysteme

Um eine Filterung von Inhalten zu realisieren, ist eine Einordnung der einzelnen Seiten (bzw. ihrer Elemente) in Kategorien erforderlich. Die Definition der Kategorien hat entscheidenden Einfluß auf die Einordnung, da sie die Möglichkeiten der Differenzierung vorgibt.

Die Kategorien können dabei einfach sein (»jugendgefährdend« , »nicht jugendgefährdend«), die Jugendgefährdung feingranular bewerten oder die Information detailliert inhaltlich beschreiben. Auch rein formale Kategorien (»nur Text«, »enthält Java«) sind von technischer Seite aus denkbar und können zur Grundlage einer Filterung gemacht werden.

Ein solches System von Kategorien kann proprietär für ein Produkt definiert und damit nur dort verwendet werden (wie die mit kommerziellen Programmen mitgelieferten Listen). In diesem Falle haben Außenstehende wenig Einfluß auf die Einstufung und die Kategoriendefinition. Manchmal sind beide Vorgänge nicht einmal nachvollziehbar. Das System kann aber auch öffentlich sein – d.h. das System und insbesondere die Kriterien für die Einstufung sind frei verfügbar und können von jedem Internet-Autor verwendet werden.[2]

Bei der Definition eines Kategoriensystems sollten nicht nur statische, sondern auch dynamische Seiten berücksichtigt werden; es sollte außerdem der Vielfalt möglicher Angebote möglichst gerecht werden. So ist z.B. eine Möglichkeit zu finden, ein ständig wechselndes Nachrichtenangebot mit Kriegsbildern korrekt zu kategorisieren (»Nachrichten«: immer gleich zu behandeln? – »Gewalt«: für Kinder zu sperren? – »politische Information«: für Kinder zugänglich?).

Werden die Einordnungen nicht zentral in einer Liste gesammelt, sondern verteilt auf den Internetseiten selber gespeichert, ist eine Vorschrift zur Übertragung dieser Einstufungen, eine Art »Übertragungsprotokoll« erforderlich. Öffentliche Kategoriensysteme basieren meist auf dem W3C-Standard von PICS (*Platform for Internet Content Selection*)[3].

Inhaltliche Einstufung

Ist ein Kategoriensystem definiert oder hat man sich anderweitig auf ein systematisches Vorgehen zur Einstufung von Internetseiten geeinigt, kann der eigentliche Vorgang der Einstufung vom Autor der Seite selbst, von einem von Autor und Leser verschiedenen Dritten, von der Internet Community (d.h. als Sammlung der Einstufungen von vielen Personen) oder vom Abrufer (d.h. dem Administrator des lokalen Rechners, also z.B. Eltern oder Lehrer) vorgenommen werden.

Die Entscheidung für eine bestimmte dieser Instanzen wirkt direkt auf den mit der Einordnung verbundenen Aufwand, aber auch auf die Korrektheit der so entstehenden Einstufungen ein.

So ist die Korrektheit im Sinne des Abrufers besonders gut, wenn er alle Einstufungen selber vornimmt. Der Aufwand zur Bearbeitung des gesamten Internets ist allerdings extrem hoch.

Im Gegensatz dazu ist der Aufwand für den Autor, bei der Verfassung einer Seite auch noch eine Einstufung vorzunehmen, verhältnismäßig gering. Allerdings ist die Einstufung weniger einheitlich und beinhaltet versehentliche und absichtliche Fehleinstufungen. Daher wird sie größerer Überprüfung von seiten der Abrufer bedürfen und die darauf basierende Filterung eine höhere Fehlerquote aufweisen.

Vom Aufwand her in der Mitte liegen Einstufungen durch Dritte. Dies kann ein Kompromiß für einen Abrufer sein, der den Autoren der Seiten nicht vertraut, aber einem Rating Service seiner Wahl. Andererseits kann gerade durch eine umfassende Einstufung vieler Internet-Seiten durch einen einzigen Rating-Service dieser zum Quasi-Standard werden und damit die Möglichkeit haben, durch Verschiebung der Maßstäbe oder absichtliche Falscheinordnungen die Filterergebnisse zu beeinflussen und dem Endbenutzer Teile seiner freien Auswahl aus der Hand zu nehmen.

Die Ergebnisse der Einordnung können auf verschiedene Weise für den Endbenutzer verfügbar gemacht werden. Besonders einfach ist die Vorgabe einer Positivliste, die alle »erlaubten« Seiten enthält; nicht in der Liste aufgeführte Seiten werden nicht angezeigt. Dieser Ansatz ist als sehr sicher im Hinblick auf den Zugang zu jugendgefährdendem Material einzuschätzen, versteckt aber große – auch für Kinder interessante – Teile des Internets. Er eignet sich also nur für solche Kinder,

bei denen der potentielle Schaden diese Einschränkung rechtfertigt.

Das umgekehrte Prinzip – Negativlisten von nicht anzuzeigenden Seiten – schützt wiederum nur vor bekanntem jugendgefährdendem Material. Hier werden weiterhin Seiten mit potentiell jugendgefährdendem Inhalt angezeigt. Andererseits ist die Einschränkung für die sonstige Internetnutzung geringer.

Einige existierende Programme arbeiten außerdem mit automatischen Verfahren, die aus Text und Bildern Ableitungen über die Eignung der Seite für Kinder vornehmen. Diese Verfahren sind jedoch insgesamt nicht zuverlässig genug, um sie als alleiniges Mittel zur Inhaltsfilterung zu empfehlen.

Als letzte und technisch zuverlässigste Methode ist es möglich, die formalen Einordnungen, die z.B. vom Autor selbst erstellt wurden, mit der Seite zu übertragen oder von einem Server abzurufen. Damit entfällt die Notwendigkeit einer zentralen Einordnungsinstanz, die die genannten Probleme aufweist.

Auswahlprozeß

Liegt eine Einstufung einer Seite vor und ist sie – durch Eintrag in eine entsprechende Liste oder einen Vermerk auf der Seite selbst – technisch verfügbar, kann auf dieser Basis ausgewählt werden, welche Seiten am Endsystem für ein Kind angezeigt werden und welche nicht. Im allgemeinen wird man dazu ein Filterprogramm verwenden, daß so konfiguriert ist, daß es eine bestimmte Auswahl aus einem oder mehrere Kategoriensystemen anzeigt und alle anderen nicht.

Entscheidend für diese Auswahl ist der Ort, an dem sie vorgenommen wird:

Läuft der Prozeß lokal unter der Aufsicht des Administrators des Endrechners (Eltern, Lehrer) ab, hat der Administrator die Filterung vollständig unter eigener Kontrolle. Er kann damit auf Basis der eigenen Vorstellungen eine Konfiguration der Filterung vornehmen. Auch ist keine Weitergabe von Benutzerdaten an andere Stellen erforderlich. Außerdem ist eine lokal ablaufende Filterung die einzige Möglichkeit, auch verschlüsselt ablaufende Kommunikation zu filtern.

Alternativ kann der Auswahlprozeß auf einem Server – z.B. beim Internetprovider – ablaufen. Die Konfiguration kann lokal vorgenommen und an den zentralen Rechner übertragen werden. Wird die Konfiguration hingegen zentral durchgeführt, verliert der Abrufer zumindest z.T. die Möglichkeit zu einer eigenen Kontrolle der Filterung. Solche Systeme sind daher nur sinnvoll, wenn dies explizit beabsichtigt ist (z.B. in Schulen, wo der Filterprozeß auf dem Proxy abläuft, um alle Schüler einer Klasse an den Endrechnern nur den Zugang zu nicht jugendgefährdendem Material zu gestatten).

Die Flexibilität des Filterprozesses und damit seine Anpassungsfähigkeit an die Wünsche des Abrufers kann sehr unterschiedlich sein. So ist denkbar, daß er sich nur aktivieren oder deaktivieren läßt, ohne daß die Filterung beeinflußt werden kann. Auf der anderen Seite sind auch Systeme vorstellbar, die auf Basis eines detaillierten Kategoriensystems eine feine inhaltliche Auswahl der zu sperrenden und anzuzeigenden Seiten zuläßt. Entscheidend für die Art der Filterung ist die Reaktion auf Seiten ohne Einstufung (*Sperren* oder *Anzeigen*). Da dies von den persönlichen Vorstellungen des erziehenden Abrufers abhängt, sollte diese Einstellung möglichst individuell und lokal vorzunehmen sein.

Vorhandene Produkte

Es gibt auf dem Markt bereits ein große Anzahl von Produkten, die Filterung auf die eine oder andere Art durchführen. Die meisten sind zwar in der Lage, eine Auswahl auf Basis von PICS durchzuführen. Da PICS-Einstufungen jedoch bisher wenig verbreitet sind, beruht die Hauptfunktionalität meist auf eigenen Verfahren – eigene Positiv- und Negativlisten oder »Intelligente« Verfahren zur Beurteilung einer Web-Seite.

Durch technische Tests sollte im Rahmen der Studie ermittelt werden, ob unter diesen Produkten bereits Lösungen sind, die eine zufriedenstellende technische Unterstützung des Jugendschutzes im Internet bieten. Zusätzlich sollten Anforderungen für geeignete Lösungen entwickelt werden.

Es wurden allgemeine Bedienungseigenschaften getestet, d.h. Installation, Konfiguration und die Dokumentation bzw. Hilfefunktion. Außerdem wurde die Filterfunktionalität untersucht (Positivlisten, Negativlisten, PICS, automatische Verfahren), die Filtereffektivität an einigen Beispielen überprüft und der Aufwand zur Umgehung der Sperrmechanismen ermittelt.

Im Ergebnis konnte keines der Produkte zufriedenstellen. Die vollständige Sperrung z.B. des Internetzugangs oder des News-Abrufes war zwar erfolgreich; auch nach PICS-Labeln konnte zuverlässig gefiltert werden. Die Filterung von sexuell-pornographischen Seiten war jedoch nur befriedigend, bei rassistischen und gewaltverherrlichenden Inhalten sogar völlig unzureichend. Dabei wurden englischsprachige Seiten korrekter als deutschsprachige behandelt; die deutsche Sprachfunktionalität ist nicht vorhanden oder völlig unzureichend. Z.T. sind die Programme außerdem sehr leicht zu umgehen oder zu deaktivieren. Sicherungsmechanismen für Integrität und Authentizität der Einordnungen waren nicht vorhanden.

Auch praktische Tests mit potentiellen Benutzern zeugen, daß keines der derzeit erhältlichen Filterprodukte in seinem aktuellen Stand in der Lage ist, eine zufriedenstellende Unterstützung des Jugendschutzes zu gewährleisten. Die größten Mängel sind fehlende Mehrsprachigkeit und mangelnde Transparenz der Filterkriterien. Alle derzeit existierenden Systeme sind nur einsprachig (Englisch) und beruhen in ihrer Abstufung auf dem kulturellen Hintergrund von Nordamerika. Um ein für Deutschland und Europa verwendbares System zu schaffen, ist also zumindest eine Übertragung in die jeweiligen Landessprachen erforderlich, die allerdings nicht nur eine Übersetzung durchführen darf, sondern auch Rücksicht auf die jeweiligen Kulturvorstellungen nehmen muß. Um dem grenzübergreifenden Charakter des Internet Rechnung zu tragen, ist langfristig ein mehrsprachiges und auch multikulturelles System anzustreben.

Anforderungen an eine Lösung

Insgesamt konnte also in der Studie festgestellt werden, daß einerseits kein technisches System absolute Sicherheit bieten kann; andererseits sind auch existierende Systeme vom möglichen Optimum noch weit entfernt.

Daraus könnte man ableiten, daß technische Verfahren generell kein sinnvolles Mittel zum Jugendschutz im Internet sind. Die vorgenommene Untersuchung der technischen Möglichkeiten hat jedoch gezeigt, daß durchaus Systeme vorstellbar sind, die zur Verbesserung des Jugendschutzes beitragen können – nicht als Ersatz für ein Gesamtkonzept für Medienkompentenz, aber als dessen Bestandteil.

Die geschilderten technischen Möglichkeiten erlauben eine Filterung auf vie-

lerlei Art. Entscheidend für die konzeptionellen Möglichkeiten eines jeden Systems sind immer die Instanzen, bei denen Einordnung, Kennzeichnung und Auswahl des Filterprozesses bzw. deren Konfiguration angesiedelt sind (s.o.). Durch diese werden Einflußmöglichkeiten, Verantwortungsbereiche und auch die erforderliche oder mögliche Weitergabe von persönlichen Daten definiert. Außerdem ergeben sich daraus die notwendigen und möglichen Ansatzpunkte für Manipulationsschutz und Integritätssicherung.

Zusammengefaßt kann bezüglich der technischen Möglichkeiten folgendes festgestellt werden.

- Als Grundlage für ein Filtersystem ist ein geeignetes, allgemein akzeptiertes Kategoriensystem erforderlich. Als technische Basis bietet sich PICS an; allerdings sind hier noch einige Erweiterungen notwendig.

- Die Einordnung erfolgt sinnvollerweise beim Anbieter; eine Unterstützung (allerdings nicht im Sinne einer ausschließlichen Alternative) durch Dritte ist denkbar.

- Die Kennzeichnung kann auf den Internetseiten selbst oder in separaten Listen erfolgen; in beiden Fällen ist durch Authentifizierung für eine gesicherte Übertragung bis zum Abrufer zu sorgen. Für eine solche Authentifizierung bietet sich die Nutzung einer (bereits bestehenden oder für diesen Zweck einzurichtenden) Public Key Infrastruktur an.

- Die Auswahl soll vom Endbenutzer (Erziehungsberechtigte, Lehrer) zu konfigurieren sein und aus Gründen des Datenschutzes und der Kontrolle über die Filterung auch lokal ablaufen. Dabei ist für ausreichende Manipulationssicherheit zu sorgen.

Im Rahmen der Studie wurde ein Gesamtsystem konzipiert, das diese Möglichkeiten bietet. Wesentliche Elemente sind neben den zusätzlichen Funktionen und Aufgaben bei Anbieter und Abrufer ein öffentliches Kategoriensystem und eine Koordinierungsstelle. Diese Stellen sollen neben der Aufklärung und Werbung für Jugendschutz und für die Verwendung des Systems die nötige Infrastruktur zur Verfügung stellen und weiterentwickeln und das Funktionieren des Systems beaufsichtigen.

Aktuelle Entwicklungen

An vielen Stellen wird das Thema »Jugendschutz im Internet« kontrovers diskutiert. Dabei spielen nicht nur technische Fragen, sondern auch rechtliche und pädagogische Aspekte eine Rolle.

Die beschriebenen Mängel der existierenden technischen Lösungen und die potentielle Gefahr des Mißbrauchs führen generell zu einer Verschiebung des Schwerpunktes des Jugendschutzes von organisatorischen hin zu medienpädagogischen Ansätzen. Man kann sogar aufgrund der prinzipiellen Mängel der Technik der Meinung sein, den Jugendschutz nur noch als Aufgabe der Medienpädagogik zu sehen. Die Umsetzung dieses Konzeptes würde allerdings größere Änderungen im deutschen Rechtssystem erforderlich machen.

Von Seiten der Eltern und Lehrer wächst die Besorgnis über die mögliche Gefährdung von Kindern und Jugendlichen, so daß viele Einzellösungen entstehen – seien es kleine »Kindernetzwerke« oder private Sperrlisten. Da der mögliche Aufwand dort begrenzt ist, schießen solche Maßnahmen oft über das Ziel hinaus und reduzieren den Zugang auf das Internet so drastisch, daß ein natürlicher Lernprozeß der Kinder im Umgang mit den neuen Medien ernsthaft behindert oder unterbunden wird.

Auch von öffentlicher Seite wird das Problem diskutiert und bearbeitet. So versucht die EU[4] im Rahmen des Projektes »Best Use«, eine Diskussionsplattform für Eltern, Lehrer und Hersteller zu schaffen, um die praktischen Möglichkeiten intensiv zu diskutieren. In einem Aktionsplan wird mit mehren Projekten auch die Entwicklung technischer Hilfsmittel gefördert. U.a. soll hier ein Kategoriensystem entwickelt werden. Auch von Anbieterseite gibt es Initiativen zur Entwicklung eines solchen Systems.

Auf privater Ebene organisiert ist der »Internet Content Summit« der Bertelsmann-Stiftung.[5] Neben technischen und rechtlichen Fragen wird hier auch diskutiert, wer die Verantwortung für eine Regulierung im Internet übernehmen soll (Selbst-Regulierung vs. staatliche Vorgaben).

Aufschlußreich wird sicher auch die weitere Entwicklung in Australien sein: Dort wurde im Mai 1999 ein weitgehendes Gesetz zur Kontrolle von Internetinhalten beschlossen. Internetprovider können damit verpflichtet werden, Inhalte kurzfristig vom Netz zu nehmen oder zu sperren. Das Gesetz wird heftig diskutiert.[6]

---

1 Die vollständige Studie und weiteres Material zum Thema findet sich unter http://www.secorvo.de/projekt/

2 z.B. RSACi (http://www.rsac.org) und SafeSurf (http://www.safesurf.com).

3 PICS ist selber kein Kategoriensystem, sondern ermöglicht eine formal-technische Definition solcher Kategorien und deren technische Verwendung. Es enthält außerdem Zusatzfunktionen z.B. bezüglich der »Übersetzung« verschiedener Systeme ineinander und zur Signatur in der Seite enthaltener Einstufungen (Label). Näheres auf http://www.w3.org/PICS/

4 http://www2.echo.lu/iap/, http://www2.echo.lu/best_use/best_use.html.

5 http://www.stiftung.bertelsmann.de/internet-content/deutsch/frameset_home.htm

6 http://www.efa.org.au/Issues/Censor/cens1.html

Manuel Kiper

Elektronische Kommunikation

Gläserne Betriebe – gläserne Belegschaften

Seit dem Bundesverfassungsgerichtsurteil vom 15. Dezember 1983 (Volkszählungsurteil) wird Datenschutz in Konkretisierung des Persönlichkeitsrechts des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG als Grundrecht auf informationelle Selbstbestimmung verstanden. Datenschutz als Schutz der Persönlichkeitsrechte korrespondiert heute aber auch mit der wirtschaftlichen Erfordernis der Datensicherheit, in der globalisierten Datenkommunikation die Integrität der Information und Kommunikation, die Vertraulichkeit, die Unbeobachtbarkeit, die Transparenz zur Beweissicherung etc. systematisch zu sichern.

Der Gesetzgeber hat seit 1996 mit dem Telekommunikationsgesetz, dem Teledienstedatenschutzgesetz wie mit dem Gesetz zur digitalen Signatur den rechtlichen Rahmen für Datenschutz und Datensicherheit weiter entfaltet und zugleich diesbezüglich Verschärfungen im Strafgesetzbuch vorgenommen. In den Unternehmen ist das Wissen um die neuen gesetzlichen Rahmensetzungen und Detailvorschriften auf seiten des Managements, der DV-Verantwortlichen wie auf seiten der Interessenvertretungen und der Beschäftigten höchstens in Ansätzen vorhanden. Gleichzeitig werden Datenschutz und Datensicherheit für den wirtschaftlichen Erfolg vieler Unternehmen wie für das funktionsfähige Handeln von Behörden immer wichtiger. Die Ausweitung von Mobil- und Telearbeit, die Durchsetzung von Telebanking und E-Kommerz wie die Entwicklung des gesamten Elektronischen Geschäftsverkehrs wird ohne entsprechende Verstärkung des persönlichen Datenschutzes wie der betrieblichen Datensicherheit nicht erfolgreich zu bewerkstelligen sein.

Das kürzliche Vorhaben von Mister Minit, die Mitarbeiter permanent mit Video zu überwachen, wurde zwar vom Kaufhof-Konzern abgeblockt. Eine solch offensichtliche lückenlose Überwachung des Verhaltens der Beschäftigten ist in Deutschland nicht zulässig. Die obersten Gerichte, Bundesarbeitsgericht wie Bundesverfassungsgericht schließen zwar im Einzelfall, insbesondere bei erheblicher Verdachtskontrolle, eine punktuelle und vorübergehende Video- wie auditive Überwachung nicht aus. Generalisierte Videobeobachtung oder Abhören haben sie aber grundsätzlich als mit dem Persönlichkeitsrecht und dem Recht auf informationelle Selbstbestimmung nicht vereinbare Kontrolle für unzulässig erklärt.

Entsprechend hat das Bundesarbeitsgericht im Oktober 1997 entschieden, dass im beruflichen Bereich auch das Recht am gesprochenen Wort als Teil des allgemeinen Persönlichkeitsrechts zu gewährleisten ist.[1] Und zuvor schon hatte das Bundesverfassungsgericht geurteilt, dass ein Telefonüberwachungssystem, mit dessen Hilfe der Arbeitgeber alle dienstlichen wie privaten Telefongespräche seiner Arbeitnehmer aufzeichnen und abhören kann, einen Eingriff in den Schutzbereich des allgemeinen Persönlichkeitsrechts darstellt.[2] Allein die Tatsache, dass ein Telefongespräch »in der Sphäre eines Arbeitsverhältnisses« geführt wird, erlaubt es einer weiteren Person (z.B. dem Personalchef oder dem Abteilungsleiter) also keineswegs ohne Zustimmung des Gesprächspartners mitzuhören oder mithören zu lassen.

Die in Computernetzen und digitalen Telefonanlagen mögliche unsichtbare Leistungs- und Verhaltenskontrolle wird dennoch immer ausgeklügelter. E-Mails können an verschiedenen Servern mitgelesen, das individuelle Aufrufen einzelner Web-sites lückenlos an anderen Rechnern kontrolliert, die Bildschirmarbeit eines Mitarbeiters mit geeigneter Software für sog. Screen-shots von Vorgesetzten zeitgleich transparent gemacht werden.[3] Nach einer Studie der American Management Association überwachen in den USA bereits 27% der Großunternehmen die Mail-Aktivitäten ihrer Mitarbeiter.[4] Wie wenig anonym das Arbeiten in einer qua Internet vernetzten Welt ist, zeigte nicht zuletzt die Verfolgung des jüngsten gefährlichen Virus Melissa. Durch Rückverfolgung des sich lawinenartig ausbreitenden Virus konnte innerhalb weniger Tage sein geistiger Urheber dingfest gemacht werden.[5] Jeder Computer firmiert im weltweiten Internet unter einer bestimmten codierten Adresse, die bei jedem Datentransfer automatisch mitübertragen wird. Dadurch werden enorme Datenspuren hinterlassen.

Die privatwirtschaftliche Auswertung solch individuell zuordenbarer Datenspuren, das Data mining, wurde inzwischen sogar ein eigener lukrativer Markt.[6] Zum gläsernen Bürger und gläsernen Mitarbeiter gesellt sich der gläserne Konsument. Durch zunehmendes Angebot von Telediensten in den Unternehmen auch für ihre eigenen Mitarbeiter werden Mitarbeiter nicht nur in ihrer Arbeitsleistung, sondern auch in ihrer Kundenqualität durchsichtig.

Datenschutz- und Datensicherheitsvorschriften in der neuen Telekommunikations- und Multimediagesetzgebung

Unverändert basiert der Datenschutz in Unternehmen auf dem Bundesdatenschutzgesetz (BDSG) und Betriebsvereinbarungen. Grundlage des betrieblichen Datenschutzes für die Telekommunikation sind jedoch Gesetze, die erst in den letzten Jahren im Zusammenhang mit der sogenannten Liberalisierung des Telekommunikations-Sektors erlassen wurden. Bei diesen Gesetzen handelt es sich um vorrangige Rechtsvorschriften des Bundes im Sinne des Bundesdatenschutzgesetzes (§ 1 Abs. 4 BDSG), um Vorschriften also, die dem BDSG gegenüber Vorrang haben.[7]

Telekommunikations- und Multimediagesetzgebung

Den Anfang machte im Juli 1996 das Telekommunikationsgesetz (TKG), das den Wettbewerb im Telekommunikations-Sektor fördern und das flächendeckende Angebot angemessener und ausreichender Dienstleistungen gewährleisten soll.

Dazu kam im August 1997 das ›Informations- und Kommunikationsdienste-Gesetz‹ (IuKDG) als ein Artikelgesetz – gewissermaßen ein Gesetzesbündel –, das als Artikel 1 das Teledienstegesetz und als Artikel 2 das ›Teledienstedatenschutzgesetz‹ enthält und dessen Ziel es ist, »einheitliche wirtschaftliche Rahmenbedingungen für die verschiedenen Nutzungs-

möglichkeiten der elektronischen Informations- und Kommunikationsdienste zu schaffen«. Zusätzlich wurden im ›Mediendienstestaatsvertrag‹ noch die an die Allgemeinheit gerichteten Informations- und Kommunikationsdienste, die sogenannten Mediendienste geregelt. Die folgende Übersicht gibt einen Überblick über Definitionen und Zuordnungen von Netzaktivitäten zu unterschiedlichen Gesetzesregelungen.

Erschwerend kommt zu dieser Vielfalt an Regelungen und Definitionen hinzu, dass es auch noch Überschneidungen gibt, weil bei der Nutzung von Telediensten z.B. gleichzeitig auch Telekommunikationsdienste genutzt werden.[8] Die in den aufgeführten Gesetzen enthaltenen Regelungen können für den betrieblichen Datenschutz im Einzelfall alle von Bedeutung sein.

Neben den gesetzlichen Regelungen des Telekommunikations- und Multimediarechts sind darüber hinaus bei der Datenverarbeitung auch die verschärften Bestimmungen des Strafgesetzbuchs (StGB) zu berücksichtigen. Der neu geschaffene § 206 StGB stellt den Bruch des Fernmeldegeheimnisses unter Strafe. Verboten sind auch verschiedene Eingriffe in den Datenverkehr. § 202 a StGB stellt das Ausspähen von Daten unter Strafe. Dies umfasst nach Absatz 2 dieses Paragrafen auch die Übermittlung von Daten, also auch das ›Ausspähen‹ von eMails oder persönlichen Identifikations-Nummern.

Telekommunikationsgesetz

Das TKG befasst sich auch mit datenschutzrechtlichen Fragen. Es regelt in seinem elften Teil den Schutz des Fernmeldegeheimnisses, den Datenschutz sowie den staatlichen Zugriff auf die bei der Telekommunikation anfallenden Daten.

Zunächst soll geklärt werden, was nach dem TKG unter Telekommunikation verstanden wird. Telekommunikation wird dort definiert als der »technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikations-Anlagen.« (§ 3 Nr. 16 TKG). Damit unterliegt also auch die Kommunikation über das Internet (oder ein unternehmensinternes Intranet) den Bestimmungen des TKG.

Nun könnte vielleicht die Meinung aufkommen, die Regelungen des TKG bezögen sich nur auf spezielle Telekommunikations-Unternehmen, nicht aber auf ›normale‹ Firmen. Tatsächlich jedoch bezieht sich das TKG durchaus nicht nur auf das gewerbliche Angebot von Telekommunikation. Vielmehr unterliegen den Datenschutzbestimmungen des TKG all diejenigen, die – wie es in § 89 Abs. 1 TKG heißt – »geschäftsmäßig Telekommunikations-Dienste erbringen«. Und das wird in § 3 Nr. 5 TKG definiert als »das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht«. Nachhaltig ist das Angebot immer dann, wenn es nicht nur einmalig, sondern auf Wiederholung oder auf Dauer angelegt ist.

Die Ausweitung des Geltungsbereichs des TKG über den gewerblichen und gewinnorientierten Sektor der Telekommunikation hinaus ist also vom Gesetzgeber ausdrücklich gewollt. Dies zeigt auch die Gesetzesbegründung. Dort heißt es unter anderem: »Dem Fernmeldegeheimnis [unterliegen] damit z.B. Corporate Networks, Nebenstellenanlagen in Hotels und Krankenhäusern, Clubtelefone und Nebenstellenanlagen in Betrieben und Behörden, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind«.[9]

Jedes Unternehmen, jede Stadtverwaltung oder Universität, jedes Krankenhaus oder Hotel, das seinen Angestellten (bei Privattelefonie) oder Kunden – also einem ›Dritten‹ – regelmäßig das Telefonieren erlaubt, erbringt also »geschäftsmäßig Telekommunikation« und unterliegt somit dem TKG. Und dies gilt nicht nur für die Telefonanlage eines Betriebs, sondern auch für firmeninterne Computer-Netzwerke. Dem entspricht es, dass die im TKG angeführten strafrechtlichen Regelungen zum Schutz des Fernmeldegeheimnisses ausdrücklich durch das Anfang 1998 in Kraft getretene Telekommunikations-Begleitgesetz (TKBeglG) auch auf den Bereich firmeninterner Netze ausgedehnt worden sind.

Fernmeldegeheimnis in der Telekommunikation

Der § 85 TKG bestimmt nun, dass »der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikations-Vorgang beteiligt ist oder war«, dem Fernmeldegeheimnis unterliegen. Weiterhin erstreckt sich das Fernmeldegeheimnis auf »die näheren Umstände erfolgloser Verbindungsversuche«. Geschützt sind damit zum Beispiel auch die Verbindungsdaten eines Kommunikationsvorgangs – also wer wann, mit wem, wie lange, von wo, wohin und auf welche Weise kommuniziert hat. Damit stellt eine detaillierte Liste von Verbindungsdaten – beispielsweise über Telefonaten zu Kontrollzwecken erstellt – einen Verstoß gegen das Fernmeldegeheimnis dar. Dies gilt unstrittig immer dann, wenn die Telekommunikations-Dienste geschäftsmäßig, also regelmäßig (nachhaltig) für Dritte erbracht werden.

Zusammenfassend läßt sich sagen: Wenn und soweit vom Arbeitgeber die private Nutzung der betrieblichen Telekommunikations-Anlagen für interne oder externe Kommunikation gestattet wird, gelten sowohl das Fernmeldegeheimnis wie auch die datenschutzrechtlichen Bestimmungen des TKG. Unerheblich ist dabei, ob die Telekommunikations-Anlagen entgeltlich oder unentgeltlich zu privaten Zwecken genutzt werden dürfen. Selbst das Untersagen privater Nutzung der Telekommunikationsanlagen durch die Beschäftigten entbindet dann nicht von der Verpflichtung zur Einhaltung des Fernmeldegeheimnisses und der Datenschutzvorschriften nach dem TKG, wenn eingehende Anrufe und E-Mails – die ja auch privaten Charakter haben könnten – automatisch an die Nebenstelle vermittelt werden (Durchwahl). Nur wenn der Arbeitgeber die strikte Nutzung der betrieblichen TK-Anlagen allein für dienstliche Zwecke erzwingt und organisatorisch sicherstellt, werden in Hinblick auf die Beschäftigten nicht mehr die Merkmale eines Telekommunikations-Dienstes ›für Dritte‹ erfüllt. Damit würden dann auch die Schutzbestimmungen des elften Teils des TKG entfallen.

Rechtsprechung zum Fernmeldegeheimnis

Gestützt wird die oben entwickelte weite Auslegung des Fernmeldegeheimnisses im TKG auch durch Entscheidungen höchster Gerichte. Entsprechende Rechtsprechung hat sich hinsichtlich der Kontrolle des Telefonierverhaltens herausgebildet. So hat das BVerfG in Korrektur einer anderslautenden Entscheidung des BAG festgehalten, dass ein heimliches Mithören oder Aufzeichnen des Inhalts eines Telefonats des Arbeitnehmers dessen Einwilligung voraussetzt und dass diese nicht stillschweigend als erteilt ange-

nommen werden kann, wenn der Arbeitnehmer um die Abhörmöglichkeit weiss.[10]

Entsprechend hat das BAG bei heimlichem Mithörenlassen von Telefongesprächen eine Persönlichkeitsrechtsverletzung erkannt. Heimliches Mithörenlassen von Telefongesprächen zwischen Arbeitnehmer und Arbeitgeber ist unzulässig. Auf diese Weise erlangte Beweismittel dürfen nicht verwertet werden. Bei Mithören ist der Gesprächspartner vorher darüber zu informieren. Gesprächspartner am Telefon müssen sich nicht ihrerseits vorher vorsorglich vergewissern, dass niemand mithört.[11]

So hat auch das Bundesarbeitsgericht im Oktober 1997 entschieden, dass auch im beruflichen Bereich das Recht am gesprochenen Wort als Teil des allgemeinen Persönlichkeitsrechts zu gewährleisten ist.[12] Nach Urteil des Bundesverfassungsgerichts stellt ein Telefonüberwachungssystem, mit dessen Hilfe der Arbeitgeber alle dienstlichen wie privaten Telefongespräche seiner Arbeitnehmer aufzeichnen und abhören kann, einen Eingriff in den Schutzbereich des allgemeinen Persönlichkeitsrechts dar.[13] Allein die Tatsache, dass ein Telefongespräch »in der Sphäre eines Arbeitsverhältnisses« geführt wird, erlaubt es einer weiteren Person (z.B. dem Personalchef oder dem Abteilungsleiter) also keineswegs ohne Zustimmung des Gesprächspartners mitzuhören oder mithören zu lassen.

Bereits seit dem sogenannten ›Fangschaltungsbeschluss‹ des BVerfG war entschieden, dass betriebsbedingte Einblicke eines Diensteanbieters oder Betreibers (und dazu gehört auch das Unternehmen, das eine Telefonanlage oder ein Intranet betreibt) in Inhalte und Umstände elektronischer Kommunikation »rechtfertigungsbedürftige Eingriffe in das Fernmeldegeheimnis« sind.[14] Insofern hat auch das BAG eine Betriebsvereinbarung, die es dem Arbeitgeber bei einer ACD-Anlage[15] erlaubt, externe Telefongespräche der Arbeitnehmer in deren Gegenwart zu Ausbildungszwecken mitzuhören, in diesem Fall für zulässig erklärt.[16] Die Praxis, dass Mitarbeiter wie Kunden in Call-Centern gängigerweise extern abzuhören sind, wie es von der Panoramaredaktion im September 1999 öffentlich gemacht wurde[17], dürfte damit allerdings unvereinbar sein.

Eine Kontrolle des Telefonierverhaltens der Beschäftigten in Hinblick auf Missbrauch und Kostenverursachung wird in der Rechtsprechung andererseits für zulässig gehalten. Von unteren Arbeitsgerichtsinstanzen werden hier z.T. drastische Urteile gefällt, die allerdings vor Landesarbeitsgerichten üblicherweise nicht Bestand haben. Arbeitnehmer, die in erheblichem Umfang auf Kosten ihres Arbeitgebers privat telefonieren, können ohne Abmahnung entlassen werden, so die Entscheidung des Arbeitsgerichts Frankfurt am Main.[18] Auch das Arbeitsgericht Würzburg sah eine Kündigung ohne vorherige Abmahnung wegen vollendeten Betrugs gerechtfertigt, wenn ein Arbeitnehmer häufig auf Kosten seines Arbeitgebers telefoniert, ohne die Gespräche zu bezahlen.[19] Kündigungsgrund sah das Arbeitsgericht Frankfurt am Main auch bei unbezahlten Telefonaten mit Australien insbesondere, wenn die Arbeitnehmerin erst nach einem Computerausdruck bereit war, das Telefonat zu bestätigen.[20] Desgleichen sah das Gericht Kündigungsgrund, wenn ein Arbeitnehmer auf Kosten seines Arbeitgebers telefonisch einem Nebenjob nachgeht.[21] Andererseits hat jüngst das Arbeitsgericht Frankfurt am Main entschieden: »Ist einem ArbN die Nutzung der betrieblichen Telefonanlage zu Privatgesprächen in bestimmtem Umfang gegen Kostenerstattung erlaubt, schließt eine derartige Gestattung auch kurze Anrufe zu privaten Zwecken während der Arbeitszeit ein, solange nicht ausdrücklich etwas anderes festgelegt wurde und der ArbN nicht mit der ihm obliegenden Arbeitsleistung in Rückstand gerät. Die Ausübung eines solchen Rechts rechtfertigt auch dann nicht ohne weiteres den Vorwurf einer gegen den Arbgeb. gerichteten Straftat und eine außerordentliche Kündigung des Arbgeb., wenn der ArbN ohne Aufforderung des Arbgeb. die durch die Privatgespräche entstanden Kosten (hier: DM 66,51) nicht von sich aus erstattet«.[22] Das Oberlandesgericht Hamm entschied, dass ein leitender Angestellter durch Inanspruchnahme von Telefonsexgesprächen in »nicht unbeträchtlicher Höhe für private Zwecke« seine ihm verliehene Vertrauensstellung im Betrieb missbraucht habe und damit ohne Abmahnung entlassen werden könne.[23]

Landesarbeitsgerichtsentscheidungen hingegen sind bislang für die Beschäftigten glimpflicher ausgefallen. So entschied das LAG Niedersachsen, dass auch bei erwiesener Vielzahl von Privattelefonaten auf Arbeitgeberkosten eine verhaltensbedingte Kündigung erst zu rechtfertigen sei, wenn der Mitarbeiter vorher abgemahnt worden sei.[24] Das Landesarbeitsgericht Köln befand sogar: Erlaubt ein Arbeitgeber seinen Beschäftigten, private Telefonate von seiner Anlage aus zu führen, so darf er einem Mitarbeiter nicht kündigen, der davon »ausschweifend« Gebrauch macht, insbesondere dann nicht, wenn er durch eine »unzureichende Organisation« erst spät darauf aufmerksam wird und damit rechtzeitige Ermahnungen unterblieben sind.[25]

Insofern ist alles in allem von einem weitreichenden Schutz des Fernmeldegeheimnisses und des Datenschutzes bei Telekommunikationsvorgängen auszugehen. Nicht zuletzt sind die Mitgliedsstaaten der EU durch – hier zu Lande noch nicht umgesetzte – EG-Richtlinien dazu generell verpflichtet, »das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Kommunikationen durch andere Personen als die Benutzer« zu untersagen.

Wahrung des Fernmeldegeheimnisses bei Telefon, Telefax und eMail

Gesetzlich durch das Fernmeldegeheimnis geschützt ist – wie bereits dargelegt – nicht nur das Telefonieren, sondern jede Art der individuellen Nachrichtenübermittlung, einschließlich eMail und Telefax. Auch die Einführung eines generellen Überwachungssystems für den elektronischen Postverkehr in den Unternehmen stellt also einen Eingriff in den Schutzbereich des allgemeinen Persönlichkeitsrechts der Arbeitnehmer dar. Bei ausgesprochener Geschäftspost sind solche Eingriffe allerdings zu Kontrollzwecken zulässig. Persönlich adressierte oder z.B. an den Betriebs- oder Personalrat gerichtete oder verschickte eMails unterliegen hingegen einem Schutz vor Überwachung, nicht nur des Inhalts, sondern auch der Verbindungsdaten.

Im Hinblick darauf, dass Telefaxgeräte vielfach frei zugänglich sind und dass E-Mails zwischengespeichert werden, gewinnen hier auch die Vorschriften des § 87 TKG Bedeutung, die den Arbeitgeber zu technischen Schutzmaßnahmen zwingen, um so das Fernmeldegeheimnis zu sichern. Zwar haben Angestellte, die eingegangene Telefaxe dem Gerät – zum Beispiel einem Etagen-Telefaxgerät – entnehmen, das Fernmeldegeheimnis zu wahren und Gleiches gilt auch für den Ausdruck von Sende- und Empfangsprotokollen an einem Telefaxgerät, das von mehreren Personen genutzt wird. § 87 Abs. 1 TKG verpflichtet aber darüber hinaus den Arbeitgeber, »der eine Telekommunikationsanlage betreibt, die dem geschäftsmäßigen Erbringen von Tele-

kommunikationsdiensten dient«, zu »angemessenen technischen Vorkehrungen oder sonstigen Maßnahmen« zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten und zum Schutz programmgesteuerter Telekommunikations- und Datenverarbeitungs-Systeme gegen unerlaubte Zugriffe.

Dabei sind zum Schutz des Fernmeldegeheimnisses organisatorisch-technische Maßnahmen wie Zutritts- und Zugriffsbeschränkungen ebenso vorzusehen wie Anonymisierungs-Maßnahmen und auch Verschlüsselungen. Dies sicherzustellen dürfte in vielen Unternehmen eine Umorganisation notwendig machen, um so zum Beispiel Verbindungsprotokolle, die zur Auswertung häufig in gedruckter Form vorliegen, vor unbefugter Einsichtnahme zu schützen. Elektronische Posteingangsbücher und die Dokumentation der betriebsinternen eMail-Bearbeitung haben ebenfalls das Fernmeldegeheimnis zu wahren.[26] So dürfen beispielsweise eMails an namensbezogene Adressen (wie ›WalterMüller@t-online.de‹) nicht protokolliert werden.

Allerdings darf der Arbeitgeber nach Auffassung des Berliner Datenschutzbeauftragten einzelne dienstliche E-Mails einsehen, auch wenn sie an einen bestimmten Arbeitnehmer gerichtet sind. »Der Arbeitnehmer hat dem Arbeitgeber den Zugang zu solchen E-Mails zu eröffnen. Dagegen ist eine Auswertung des gesamten E-Mail-Verkehrs (etwa durch automatisches Scannen) durch den Arbeitgeber jedenfalls im Regelfall nicht gestattet.«[27] Ist die Kennzeichnung privater E-Mails systemtechnisch nicht vorgesehen, erstreckt sich die Geheimhaltungspflicht nach dem TKG auch auf den betrieblichen E-Mail-Verkehr. Ist hingegen die Privatnutzung des E-Mail-Systems betriebsintern mengenmäßig oder zeitlich limitiert und diese Regelung den Beschäftigten bekanntgegeben worden, sind allerdings »Missbrauchskontrollen durch das Beschäftigungsunternehmen zulässig«.[28]

Datenschutz bei Telediensten

Weil Arbeitgeber, die ihren Beschäftigten den Zugang zum Internet nicht ausschließlich für dienstliche Zwecke ermöglichen, Teledienste-Anbieter sind, gilt nicht nur das TKG, sondern auch das IuKDG. Denn nach § 3 Nr. 1 TDG sind Teledienstean bieter »natürliche oder juristische Personen oder Personenvereinigungen, die eigene oder fremde Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln«.

Das IuKDG ist – wie schon kurz erwähnt – ein Artikelgesetz, mit dem sehr unterschiedliche Fragen in einem Gesetz geregelt wurden. Anzuwenden ist das IuKDG auf Teledienste. Das sind (Artikel 1 § 2 Abs. 2 IuKDG) Telebanking und Telespiele, Verkehrs- oder Börsendaten und manches andere. Vor allem aber sind Teledienste Angebote zur Nutzung des Internets oder weiterer Netze. Demnach ist ein Arbeitgeber, der seinen Beschäftigten eine nicht ausschließlich dienstliche Internet-Nutzung ermöglicht, also ein Teledienste-Anbieter. Gleiches gilt für weitere Netze, also auch für firmeninterne Computernetze wie etwa ein Intranet. Wird hingegen in einem Konzern von einem Konzernservicebetreiber die Internetnutzung den Konzernmitarbeitern nur für betriebliche Zwecke zur Verfügung gestellt, so ist nach Auffassung z.B. des Baden-Württembergischen Innenministeriums das einzelne Beschäftigungsunternehmen Nutzer und nicht der einzelne Beschäftigte, so dass – zwar unter Mitbestimmungsvorbehalt – aber »die Daten grundsätzlich auch zur Kontrolle des Verhaltens und der Leistung verwendet werden dürfen«.[29] Dem wird von anderer Seite allerdings widersprochen und die Gültigkeit des TDG auch für unternehmensinterne Teledienste reklamiert, »gleichgültig ob dieser im einzelnen Unternehmen oder im Konzernverbund genutzt wird«.[30] Ein Zugriff des Arbeitgebers auf E-Mails kann auch »aus Gründen der Systemsicherheit, dem Schutz vor Viren und dem Schutz vor Kosten- und Netzüberlastung« nicht völlig ausgeschlossen werden.[31]

Den Datenschutz regelt das IuKDG in seinem Artikel 2, dem Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz – TDDSG). Wobei auch das TDDSG nicht zwischen firmeninterner oder -externer Kommunikation unterscheidet. Und es gilt – wie im Bundesdatenschutzgesetz – ein Verbot mit Erlaubnisvorbehalt. Das heißt in diesem Fall: Jede Datenverarbeitung ist verboten, wenn sie nicht ausdrücklich gesetzlich erlaubt ist.

Folgende **einzelne Datenschutzvorschriften** sind in **§§ 3 – 6 TDDSG** festgeschrieben:

- das Gebot der Datensparsamkeit;
- die Datenerhebung ist von der Zustimmung des Nutzers abhängig;
- der Nutzer ist von Art und Umfang der Datenerhebung zu unterrichten;
- die Nutzung ist – so weit technisch möglich und zumutbar – anonym oder pseudonym (mit einem ›Decknamen‹) zu ermöglichen;
- Nutzungsdaten, die zur Abrechnung nicht benötigt werden, sind nach Beendigung der Verbindung umgehend zu löschen;
- Abrechnungsdaten sind 80 Tage nach Rechnungslegung zu löschen;
- personenbezogene Nutzerprofile sind unzulässig und nur bei Pseudonymen erlaubt;
- eine Datenschutzkontrolle nach § 38 BDSG durch die zuständige Aufsichtsbehörde ist auch dann erlaubt, wenn keine Anhaltspunkte für eine Verletzung der Datenschutzvorschriften vorliegen.

Das heißt: Nutzungsdaten (Daten über die Benutzung einer Telekommunikations-Einrichtung) und andere nicht benötigte Daten von im Internet surfenden Arbeitnehmern müssen unverzüglich gelöscht werden. Nutzungsprofile sind unzulässig. Und das wiederum bedeutet, dass Arbeitgebern untersagt ist, Daten über die Netzbenutzung ihrer Beschäftigten auszuwerten. »Die Protokollierung der privaten Nutzung ist nur – soweit diese vorgesehen ist – zu Abrechnungszwecken gestattet«.[33] Entsprechenden Befürchtungen kann und sollte mit klaren Regelungen zwischen Betriebsräten und Arbeitgebern entgegen getreten werden.[34] Im Unterschied zu anderen Datenschutzgesetzen und -vorschriften bleibt der Datenschutz im IuKDG aber trotz dieser Regelungen wirkungsschwach, da das TDDSG nicht vorsieht, Datenschutzverstöße als Ordnungswidrigkeit zu bestrafen.

Dies heißt nun allerdings nicht, dass der Arbeitgeber jedwede Internet-Nutzung seiner Beschäftigten dulden muss. Zugangsbeschränkungen, Ahndung von Missbrauch oder Geheimnisverrat und ähnliches sind dem Arbeitgeber nicht verwehrt. Die praktische Durchführung aber muss immer auch dem weitestgehenden Schutz des Persönlichkeitsrechts der Beschäftigten Rechnung tragen. So kann der Arbeitgeber zum Beispiel Firewalls, Filter oder andere technische Mittel einsetzen, um den Zugriff auf bestimmte

Dienste und Netzressourcen zu begrenzen.

Ist die private Internet-Nutzung von Arbeitnehmern am Arbeitsplatz entweder erlaubt oder wird geduldet und wird diese auch nicht abgerechnet, darf der Arbeitgeber keine Daten über die Internet-Nutzung seiner Beschäftigten sammeln. Hervorzuheben ist auch, dass – soweit technisch möglich und zumutbar – dem Nutzer die Möglichkeit einzuräumen ist, Teledienste anonym oder unter Pseudonym zu nutzen (bei Pseudonymen sind dann allerdings Nutzungsprofile zulässig).[35] Deutlich sollte aber auch sein, dass ein Arbeitnehmer keinen Anspruch darauf hat, das Internet nach Belieben zu nutzen.

So müssen (und dürfen) auch strafbare Handlungen über E-Mail- oder Internet/Intranetnutzung nicht geduldet werden und sind insofern Missbrauchskontrollen und entsprechende Ahndung zulässig. Bei Verdacht auf strafrechtliche Vergehen von Mitarbeitern ist durch den Arbeitgeber ggf. die Polizei/Staatsanwaltschaft einzuschalten. Dies wäre z.B. gegeben, wenn ein Mitarbeiter in den Verdacht gerät, von seinem Arbeitsplatz

- (verbotene) Kinderpornografie aus dem Netz zu laden und innerbetrieblich auf seinem Computer zu speichern.[36]
- unbefugt in fremde Dateien einzudringen,[37]
- beleidigende Inhalte auf seiner Web-Site anzubieten oder,[38]
- unkommentiert Links auf beleidigende oder sonstwie strafwürdige Inhalte setzt.[39]

Mitarbeiter verstoßen somit gegen ihre arbeitsvertraglichen Pflichten, wenn sie während der Arbeitszeit nicht-dienstliche Daten an ihrem Arbeitsplatz verarbeiten. So kann z.B. die Anlage von Dateien mit sexistischen oder rassistischen Witzen und deren Überspielung an Kollegen Grund für fristlose Kündigung sein.[40] Eine systematische Überwachung der Internetaktivitäten von Mitarbeitern, wie sie die Filterprogramme von CyberPatrol, Little Brother, Spector, SurfControl und andere Software zulassen, ist zwar in den USA üblich, in Deutschland aber unzulässig.[41]

Zusammenfassung

Die systematische Überwachung, Kontrolle, Dokumentation und Auswertung des telekommunikativen Verhaltens von Mitarbeitern/innen ist weitgehend verboten, da das Fernmeldegeheimnis und das Persönlichkeitsrecht zu achten sind. Dies gilt, wenn und sofern private betriebliche Telekommunikation

- nicht verboten, sondern geduldet oder erlaubt ist
- nicht unentgeltlich erfolgt, sondern gesondert abgerechnet wird oder
- bei unentgeltlicher Nutzung nur geringfügig genutzt wird.

Bezüglich dienstlicher Nutzung der betrieblichen Telekommunikationsanlagen gilt ein **Abwägungsprozess zwischen Direktionsrecht und Persönlichkeitsrecht**.

- Mithören ohne ausdrückliche Bekanntgabe ist nicht erlaubt.
- Mitlesen von E-Mails und Dateien durch Vorgesetzte ohne vorherige Bekanntgabe ist nicht erlaubt.
- Systematische Screen-shots (z.B. mit Cyber Patrol) sind nicht erlaubt.
- Für die Mailbox des BR/PR gilt weitgehende Meinungsfreiheit.
- Darüberhinaus gibt es besonders geschützte Personengruppen wie Betriebsärzte oder Mitarbeitervertretung, deren Rechte in besonderer Weise zu wahren sind.
- Jede Einführung oder zusätzliche Nutzung von technischen Einrichtungen unterliegt der Mitbestimmung des BR/PR. Ohne Zustimmung des BR/PR sind somit auch Sanktionen hinsichtlich des telekommunikativen Verhaltens der Beschäftigten hinfällig.
- Bei Verfehlungen sind Abmahnungen normalerweise nötig.

Eine **Mitarbeiterkontrolle** über Mithören bei Telefonnebenstellenanlagen, Mitlesen von E-Mails, Installieren von Videokameras oder Auswertung der Internetprotokolle ist allerdings nicht in jedem Fall dem Vorgesetzten untersagt. Überwachung, Kontrolle, Dokumentation und Auswertung des telekommunikativen Verhaltens ist erlaubt

- zu Ausbildungszwecken
- zur Kostenreduktion
- aus Sicherheitsgründen (z.B. bei Netzüberlastung, Spionageverdacht, Virenbefall)
- wegen Verdachtskontrolle bei Diebstahl, Störung des Betriebsfriedens, Nutzung unlizenzierter Software, Suchen oder Speichern verbotener Inhalte (Kinderpornografie),
- bei begründetem Verdacht auf Verrat von Betriebsgeheimnissen oder begründetem Verdacht auf nichtdienstliche Beschäftigungen am Arbeitsplatz (Tätigkeit im Nebenjob auf Kosten des Arbeitgebers, Rotlichtsurfen etc.)

Allerdings müssen auch bei dieser nach dem Direktionsrecht sanktionierten Kontrolle Persönlichkeitsrechte der Beschäftigten, die Rechte besonders geschützter Personengruppen und die Mitbestimmung des BR/PR geachtet werden. Bei Verdacht auf strafrechtliche Vergehen von Mitarbeitern ist eigenmächtige Überwachung durch den Arbeitgeber ohne Einschalten der Polizei/Staatsanwaltschaft nicht zulässig.

Zur Regelung der betrieblichen E-Mail- und Internetnutzung sollten Betriebsräte unbedingt auf den Abschluss von Betriebsvereinbarungen drängen. Eine Handlungshilfe hierzu kann von der BTQ Niedersachsen bezogen werden. In einer solchen Betriebsvereinbarung sollten auch Fragen der Verschlüsselung von E-Mails geregelt werden.

Persönlichkeitsdatenschutz und Verschlüsselung

Datensicherheit und Datenschutz sind nämlich für weitere Internetnutzung unabdingbare Voraussetzung. Konzerne wie Siemens, Enercon oder Boehringer hatten in der Vergangenheit unliebsame Erfahrungen mit der Schnüffelei des amerikanischen Geheimdienstes NSA gemacht.[42] Dass aber auch deutsche Geheimdienste internationalen Datenverkehr abhorchen, wurde einem größeren Publikum bekannt, als Ende letzten Jahres die Geldwäsche deutscher Banken

über Lichtenstein dokumentiert wurde. Die Daten waren vom Schwarzwald aus gewonnen worden. Mit 11.272 telefonüberwachten Anschlüssen[43] wurde – zu Strafverfolgungszwecken – in Deutschland 1998 sogar – gesetzlich sanktioniert – 10-mal soviel abgehört wie in den USA.

Eine Repräsentativuntersuchung privater und beruflicher Computernutzer ergab, dass lediglich 30 Prozent der Befragten sensible Daten in ihrem Computer ausreichend gegen einen Zugriff durch Unbefugte, z.B. über das Netz, geschützt hatten.[44] Untersuchungen des BSI zeichnen eine eher noch düstere Bilanz. Demnach würden lediglich vier Prozent der Unternehmen ihre E-Mails verschlüsseln. Datensicherheit ist aber zu einem ernstzunehmenden Faktor im globalen Wettbewerb geworden. Trotz erfreulicher Anstrengungen und Beschlüsse der Bundesregierung, Datenschutz und Datensicherheit in der Wirtschaft zu verbessern, verbleibt in Hinblick auf Persönlichkeitsschutz und Sicherung von Daten und Telekommunikation in den Betrieben Handlungsbedarf.

Die Enquete-Kommission des Deutschen Bundestags hatte nach zähem Ringen bereits einvernehmlich und mit den Stimmen der CDU/CSU entgegen der US-Politik und seinerzeitigen innenministeriellen Kryptoverbots-, Abhör- und Lauschplänen die Auffassung vertreten, »daß alle Maßnahmen und Hemmnisse, die einer breiten Nutzung von Verschlüsselungsverfahren entgegenwirken, vermieden und abgebaut werden müssen«.[45] Der amerikanische Sondergesandte David Aaron versuchte bereits kurz nach Regierungsantritt Bundesinnenminister Schily wie seinen Vorgänger auf die sogenannten Key-recovery-Initiative[46] einzuschwören, die es dem amerikanischen Geheimdienst NSA erlauben würde, u.a. von Bad Aibling in Bayern aus den gesamten europäischen auch verschlüsselten Datenverkehr für amerikanische militärische wie für wirtschaftliche Interessen mitzuhören und mitzulesen. Das Bundeskabinett hat demgegenüber am 2. Juni 1999 mit den »Eckpunkten der deutschen Kryptopolitik« zumindest in den kommenden zwei Jahren jede Beschränkung der Verschlüsselung ausgeschlossen.[47] Die Bundesregierung setzt sich jetzt dafür ein, dass »Verschlüsselungsverfahren und -produkte ohne Beschränkung entwickelt, hergestellt, vermarktet und genutzt werden dürfen«. Unter www.sicherheit-im-internet.de agiert jetzt die Initiative »Sicherheit in der Informationsgesellschaft« für die Bundesregierung.

Die Beschlusslage der G-8-Staaten zur gemeinsamen Spurensuche und Strafverfolgung im Datennetz, die Ende 1998 zufällig bekannt gewordenen Pläne der EU-Innen- und Justizminister für ein europaweites Abhören unter dem Stichwort Enfopol und die Weiterverfolgung der Verabschiedung einer Telekommunikationsüberwachungsverordnung[48] lassen die dargestellte wirtschaftlich motivierte Verbesserung der IT-Sicherheit seitens der Bundesregierung allerdings als halbherzig erscheinen.

Wenn so für Arbeitgeber wie Arbeitnehmer die Verschlüsselung der betrieblichen Kommunikation notwendig und wünschenswert ist, so sind doch auch hier Einbruchstellen nicht auszuschließen. Erst kürzlich offenbarte der Chaos-Computer Club, daß Microsoft mit seiner Verschlüsselungsschnittstelle Crypto-API in allen Windows-Betriebssystemen offensichtlich eine NSA-Hintertür einprogrammiert hat.[49] Im November 1999 musste das Bundesamt für Sicherheit in der Informationstechnik (BSI) sogar vor dem bekannten Verschlüsselungssystem PGP warnen. PGP wird heute als kommerzielles Produkt von der US-Firma Network Associates vertrieben, die eng mit der National Security Agency zusammenarbeitet. Das Bundesministerium für Wirtschaft und Technologie ist deshalb im November letzten Jahres dazu übergegangen, mit der OpenSource-Gemeinde[50] zu kooperieren und ein Verschlüsselungsprojekt ohne Geheimdienst-Hintertür zu fördern. Allerdings musste das Fazit gezogen werden: »Es gibt im Moment keine einfache und sichere Lösung der eMail-Kryptografiefrage für den Privatanwender.«[51]

Trotz amtlichem Segen für Verschlüsselung wird es eine hundertprozentige Sicherheit in der elektronischen Kommunikation auch zukünftig nicht geben. Fortschritte in der Kryptografie, die Gesetzgebung der letzten Jahre wie auch die Entwicklung der Rechtsprechung haben allerdings in den letzten Jahren dazu beigetragen, den Schutz und die Vertraulichkeit des elektronisch vermittelten Wortes und anderer Informationen erheblich zu verbessern. Hierzu gehört auch die strafrechtliche Bewehrung des Fernmeldegeheimnisses. Bis und ob aber Arbeitgeber wegen Verletzung des Fernmeldegeheimnisses durch Schnüffeln in E-Mails ihrer Mitarbeiter oder Mithören privater Gespräche am Arbeitsplatz mit strafrechtlichen Konsequenzen rechnen müssen, hängt auch davon ab, dass die neuen Bestimmungen breiter bekannt und in der betrieblichen Praxis umgesetzt werden. Das diffizile Abwägen zwischen Direktionsrecht einerseits und Persönlichkeitsschutz der Beschäftigten andererseits macht ein Aushandeln von Verfahrensregeln in Form von Betriebs- und Dienstvereinbarungen erstrebenswert, um manche Konflikte von vornherein auszuschalten. Die BTQ Niedersachsen gibt hierbei Hilfestellung und bietet eine ausführliche Handlungshilfe an.

Manuel Kiper u. Bruno Schierbaum: Arbeitnehmer-Datenschutz bei Internet- und E-M@ilnutzung – Handlungshilfe-; Edition BTQ Niedersachsen Nr. 3, 71 Seiten A4, April 2000, 25,- DM

---

1 Bundesarbeitsgericht, Urteil vom 29. Oktober 1997 – 5 AZR 508/96, siehe auch:. Persönlichkeitsrechtsverletzung durch heimliches Mithörenlassen von Telefongesprächen, RDV 2/1998 S. 69-71
2 BVerfG Urteil vom 19.12.1991, BB 1992, S. 708
3 Vgl. hierzu: J. Haferkamp, Alles unter Kontrolle? in: Computer Fachwissen (CF) 12/98, S. 18-24
4 Unternehmen überwachen elektronische Post, in: Handelsblatt 3.2.00, S. 23
5 Müller, M., Vater gefunden, in: Handelsblatt 7.4.1999,
6 Vgl.: W. Fricke, Bergleute im Daten-Lagerhaus, Computer Fachwissen 4/99, S. 11-14
7 Vgl. hierzu: M. Kiper u. B. Schierbaum, Telekommunikationsgesetzgebung und Arbeitnehmerdatenschutz, in: Computer Fachwissen (CF) 8-9/99, S. 24-30
8 Vgl. G. Gounalakis u. L. Rhode, Elektronische Kommunikationsangebote zwischen Telediensten, Mediendiensten und Rundfunk, CR 8/1998, S. 487-492
9 BT-Drucks. 13/3609 vom 30.01.1996, S. 53
10 BVerfG. Beschluss vom 19.12.1991 – 1 BvR 382/85; vgl: RDV 1992, S. 128; ArbuR 5/1992, S. 158-160
11 BAG, Urteil vom 29.Oktober 1997 – 5 AZR 508/96; vgl.: Persönlichkeitsrechtsverletzung durch heimliches Mithörenlassen von Telefongesprächen, RDV 2/1998 S. 69-71
12 Bundesarbeitsgericht, Urteil vom 29. Oktober 1997 – 5 AZR 508/96, siehe auch:. Persönlichkeitsrechtsverletzung durch heimliches Mithörenlassen von Telefongesprächen, RDV 2/1998 S. 69-71
13 BVerfG Urteil vom 19.12.1991, BB 1992, S. 708
14 BVerfGE 85,386, 396f
15 Automatic-Call-Distribution-Anlagen (wie sie in Call-Centern eingesetzt werden)
16 BAG, Beschluss vom 30. August 1995, – 1 ABR 4/95 – vgl: Mithören von Telefongesprächen zu Ausbildungszwecken, RDV 1/1996 , S. 30-33
17 vgl: Skript der PANORAMA-Sendung Nr. 579 vom 23.9.1999
18 Arbeitsgericht Frankfurt am Main, 18 Ca 7436/94
19 Arbeitsgericht Würzburg, 1 Ca 1326/97
20 Arbeitsgericht Frankfurt am Main, 11 Ca 5818/95
21 Arbeitsgericht Frankfurt am Main, 14 Ca 891/95
22 ArbG Frankfurt/Main v. 24.7.99, 2 Ca 8824/98
23 OLG Hamm, 8 U 194/98
24 LAG Niedersachsen, 13 Sa 1235/97
25 LAG Köln, 6 Sa 42/98
26 Vgl. z.B. E. G. Berger u. L. Gramlich, Corporate Networks im Telekommunikationsrecht, CR 3/1999, S. 150-159
27 Arbeitgeber als Anbieter von Telediensten, Jahresbericht 1998 des Berliner Datenschutzbeauftragten, zitiert nach: GDD-Mitteilungen 3-4/99, S.3-4
28 Innenministerium Baden-Württemberg, Hinweise zum Datenschutz für die Private Wirtschaft (Nr. 37), In: Staatsanzeiger Nr. 2 vom 18.1.99, S. 13; vgl.

Hinweise zum Datenschutz, RDV 3/1999, S. 131-135, hier S. 132
29 Innenministerium Baden-Württemberg, Hinweise zum Datenschutz für die Private Wirtschaft (Nr. 37), In: Staatsanzeiger Nr. 2 vom 18.1.99, S. 13; vgl. Hinweise zum Datenschutz, RDV 3/1999, S. 131-135
30 Marcus Kieper, Datenschutzrechtliche Bewertung von Proxy-Cache-Servern, in: Datenschutz und Datensicherheit 23 (1999) S. 591-593, hier 592
31 A. Müller, Datenschutz beim betrieblichen E-Mailing, RDV 5/1998, S. 205-212, hier S. 211
32 Landesbeauftragter für den Datenschutz Niedersachsen, Datenschutz bei Tele- und Mediendiensten, Hannover, 23.08.99
33 P. Gola, Neuer Tele-Datenschutz für Arbeitnehmer? Die Anwendung von TKG und TDDSG im Arbeitsverhältnis, MMR 6/1999, S. 322-330, hier S. 329
34 vgl.: Juristen empfehlen Firmen bei E-Mails eine klare Regelung, in: Handelsblatt 3.2.00, S. 23
35 Vgl. P. Gola, Neuer Tele-Datenschutz für Arbeitnehmer? in: MMR 6/1999, S. 322-330
36 Vgl.:ArbG Braunschweig, Urteil vom 22.1.99 – 3 Ca 370/98; Ausserordentliche Kündigung wegen Kinderpornografie, Computer Fachwissen (CF) 10/99, S. 26
37 Vgl.: LAG Baden Württemberg, Urteil vom 11.1.1994 – 7 Sa 86/92; AG Osnabrück, Urteil vom 19.3.1997 – 1 Ca 639/96
38 Kündigung wegen Sammlung und Verbreitung rassistischer und sexistischer Witze per dienstlichem PC, LAG Köln, Urteil vom 14.12.1998 – 12 Sa 896/98; LAG Schleswig-Holstein, Urteil vom 4.11.1998 – 2 Sa 330/98
39 Bay. OLG, Beschluss vom 11.11.1997, 4 St RR 232/97
40 Vgl.: LG Hamburg, Urteil vom 12.5.1998 – 312 O 85/98
41 Vgl. D. Sauer, Der Chef als Detektiv, In: Internet world, März 2000, S. 60-63; Vgl. J. Haverkamp, Alles unter Kontrolle? in: Computer Fachwissen (CF) 12/98, S. 18-24
42 vgl. U. Buse u. C. Schnibben, Der nackte Untertan, in: SPIEGEL 5.7.1999; O. Schröm, Verrat unter Freunden, in: DIE ZEIT, 30. 9.1999
43 J. Jacob, Telefonüberwachung evaluieren, in: Datenschutz und Datensicherheit 23 (1999), S. 666-667
44 H. W. Opaschowski, Der gläserne Komsument. Bestandsaufnahme und aktuelle Analysen zu den Themen Multimedia und Datenschutz. British American Tobacco (Germany), Freizeitforschungsinstitut, Hamburg 1998, S. 62
45 M. Kiper, M. Meister, J. Tauss, H.-O. Wilhelm, Sicherheit und Schutz im Netz, Enquete-Kommission, a.a.O., S. 173
46 dies bedeutet: Schlüsselhinterlegung beim NSA
47 R. Reimer, Deutsche Kryptopolitik: Endlich Klarheit, Datenschutz und Datensicherheit 23 (1999), S. 7
48 Mit Datum vom 12.4.99 ist ein Eckpunktepapier für eine neue gegenüber 1998 allerdings gemilderte Telekommunikationsüberwachungsverordnung (TKÜV) bekannt geworden; der 1998er Entwurf der TKÜV aus dem Hause Rexrodt hätte für die Wirtschaft Abhörmaßnahmen in Höhe von 40 Mrd. DM erforderlich gemacht, wurde aber nach massiven Protesten seitens der Grünen wie der Wirtschaft zurückgezogen.
49 D. Borchers, Das Vertrauen verschlüsselt sich, SZ 14.9.1999, S. V2/10
50 Softwareentwickler, die die Quell-Codes offenlegen (z.B. Linux)
51 www.sicherheit-im-internet.de, Pressemitteilung vom 22.11.1999

Volker Hammer

Normative Anforderungsanalyse

am Beispiel der verletzlichkeitsreduzierenden Technikgestaltung

Zusammenfassung: Sogenannte »nicht-funktionale« soziale Anforderungen finden häufig nur schwer Eingang in die Anforderungsanalyse. Der Beitrag stellt mit der normativen Anforderungsanalyse (NORA) eine Methode vor, mit der bestimmte soziale Ziele für die Anforderungsanalyse aufbereitet und operationalisiert werden können. Die Vorgehensweise wird am Beispiel der verletzlichkeitsreduzierenden Technikgestaltung beschrieben. Danach sind nicht nur Schadenswahrscheinlichkeiten zu verringern, sondern insbesondere Schadenspotentiale zu begrenzen und Beobachtungs- und Handlungsoptionen für schwere Störfälle bereitzustellen. Das Beispiel zeigt daher auch eine wichtige Ergänzung bisheriger Ansätze der IT-Sicherheit.

Einleitung

Im Rahmen des Requirements Engineering sind für eine Systementwicklung Anforderungen aus vielen Bereichen zu berücksichtigen. Naheliegend sind die funktionalen Anforderungen aus den abzubildenden oder zu unterstützenden Geschäftsprozessen, Aspekte der Software-Ergonomie oder Maßnahmen zur Unterstützung des Systembetriebs. Insbesondere beim Erschließen neuer Anwendungsfelder oder bei Anwendungen mit hoher gesellschaftlicher Relevanz zeigt es sich jedoch, daß sich die Softwareentwickler mit sozialen Fragestellungen, beispielsweise Anforderungen aus dem Recht oder Fragen der Akzeptanz, auseinandersetzen müssen. Beispiele sind Datenschutz, Jugendschutz im Internet, Akzeptanz und rechtliche Anerkennung digitaler Signaturen oder die Verletzlichkeit von Organisationen und Gesellschaft.

Werden die aus solchen Bereichen entstehenden Anforderungen von den Systementwicklern erst in einem mühsamen Lernprozeß über mehrere Systemversionen oder gar in Auseinandersetzungen zwischen konfligierenden Parteien aufgegriffen, sind Kunden unzufrieden, verzögern sich Projekte, müssen nachträglich teure Anpassungen realisiert werden oder werden Systeme am Markt nicht akzeptiert. Die sinnvolle Technikgestaltung wird dann erst spät, vielleicht zu spät, in den nächsten Versionen erreicht. Wünschenswert ist daher eine Methode zur Anforderungsanalyse, mit der soziale Anforderungen frühzeitig identifiziert werden können.

Die *normative Anforderungsanalyse* (NORA) bietet einen Methodenrahmen, mit dem die vorlaufende Technikgestaltung für bestimmte Typen sozialer Vorgaben möglich wird. Der Beitrag beschreibt die Methode am Beispiel der verletzlichkeitsreduzierenden Technikgestaltung.[1]

Der Ansatz

Angenommen, es könnten zumindest einige weitgehend akzeptierte soziale Vorstellungen zu einem Technikeinsatz identifiziert werden. Dann könnten die Technikentwickler versuchen, die aus diesen Vorgaben ableitbaren technischen Gestaltungsvorschläge in der Implementierung zu berücksichtigen. Wenn die Vorgaben nicht in einer für die Technikentwicklung verwertbaren Form vorliegen, wäre nach einer Methode zu suchen, mit der Anforderungen im Sinne einer Spezifikation abgeleitet werden können.

Genau dies ist die Grundlage der normativen Anforderungsanalyse: Zunächst sind Ziele der Technikanwendung zu identifizieren, die eine breite Zustimmung als vernünftige Vorgaben einer Technikgestaltung erwarten lassen. Sie werden als konsentierte oder *normative Vorgaben* bezeichnet. Ausgehend von den normativen Vorgaben werden mit mehreren methodischen Schritten in einem sogenannten Kriteriensystem dann *technische Gestaltungsvorschläge* konkretisiert.

Normative Vorgaben

Die Methode der normativen Anforderungsanalyse wurde bisher mit Vorgaben aus vier verschiedenen Bereichen (sogenannten *Normbereichen*) erfolgreich eingesetzt. Jeweils konnten normative Vorgaben als Ausgangspunkt für eine Anforderungsanalyse identifiziert werden. Dabei waren unterschiedliche Techniksysteme Gegenstand der Gestaltung. Im folgenden wird ein knapper Überblick über die Entstehung und die bisher bearbeiteten Normbereiche und Technikfelder gegeben.

Recht

In mehreren Projekten für die Auswahl und Gestaltung von betrieblichen Telekommunikationsanlagen wurde von der Projektgruppe verfassungsverträgliche Technikgestaltung – provet – eine Methode zur schrittweisen Konkretisierung rechtlicher Anforderungen (KORA) entwickelt.[2] Ausgangspunkt war die Fragestellung, wie die Leistungsmerkmale betrieblicher Telefonanlagen gestaltet werden müssen, damit sie die im Grundgesetz formulierten Ziele des sozialen Zusammenlebens zumindest erfüllen (Verträglichkeit), besser aber noch fördern könnten (Nützlichkeit). Dazu wurden die relevanten Vorgaben des Grundgesetzes identifiziert und, ergänzt um konkretisierende Rechtsvorschriften, auf TK-Anlagen bezogen. Grundrechtliche Vorgaben für dieses Technikfeld ergeben sich aus dem Fernmeldegeheimnis, aus Entfaltungsfreiheit und Persönlichkeitsschutz und aus dem Eigentumsschutz.

In der Folge wurde die Methode beispielsweise für die Prüfung des rechtsgemäßen Betriebs von ISDN-Anlagen,[3] für die Zweckbindung und den Geheimnisschutz in Verzeichnisdiensten[4] und die Transparenz und Entscheidungsfreiheit in Erreichbarkeitsmanagement-Systemen[5] angewandt. Neuere Arbeiten beschäftigen sich mit der rechtsgemäßen Gestaltung im Technikfeld digitaler Signaturen.[6]

Psycho-soziale Vorgaben

In einem weiteren Projekt wurde gezeigt, daß sich der methodische Ansatz von KORA prinzipiell auch für die Technikgestaltung nach Vorgaben der psychosozialen Wirkungsforschung übertragen läßt. Dort wurde für die *anwendergerechte Gestaltung von Telekooperationstechnik* ein Ausschnitt der Vorgabe *Personenbeziehbarkeit von Telekooperationsakten* untersucht.[7] Vorgaben für die Anwendergerechtheit von Telekooperation sind beispielsweise die Unterstützung von Kommunikation und die Unterstützung von Vertrauensentwicklung und -erhalt.

Verletzlichkeit

Mit Arbeiten zur Verletzlichkeit konnte gezeigt werden, daß die Methode für einen dritten Normbereich angewendet werden kann.[8] Als normative Vorgaben wurden in diesem Normbereich die klassischen Faktoren von Risiko, »niedriges Schadenspotential« und »niedrige Schadenswahrscheinlichkeit«, um »Autonomie« und »Erfahrungsbildung« ergänzt. Das Beispiel unten legt außerdem gegenüber den herkömmlichen Ansätzen der IT-Sicherheit eine Schwerpunktverschiebung von der Schadenswahrscheinlichkeit auf das Schadenspotential nahe.

Normbereich Bildung

Zur Zeit wird eine Übertragung der normativen Anforderungsanalyse auf den Normbereich Bildung vorgenommen.[9] Als normative Vorgaben konnten hier bislang identifiziert werden: »funktionale Qualifizierung«, »extrafunktionale Qualifizierung«, »Autonomie«, »Sinnreflexion« und »Gruppenbildung«. Die Vorgaben sollen in diesem Projekt zu Gestaltungskriterien für (technische) Lernumgebungen konkretisiert werden.

Normative Anforderungsanalyse – NORA

Normative Vorgaben bilden den Ausgangspunkt und damit gewissermaßen den Anker einer normativen Anforderungsanalyse. Ihre Identifikation und Absicherung ist deshalb eine wichtige Voraussetzung für die weitere Vorgehensweise.

Wenn normative Vorgaben identifiziert werden können, sind sie allerdings häufig generalklauselartig und kaum technikadäquat formuliert (siehe die Beispiele oben). Zwischen ihnen und den gesuchten Gestaltungsvorschlägen für die Technik liegt eine große *Beschreibungslücke* (vgl. Abb. 1). Für eine Technikgestal-

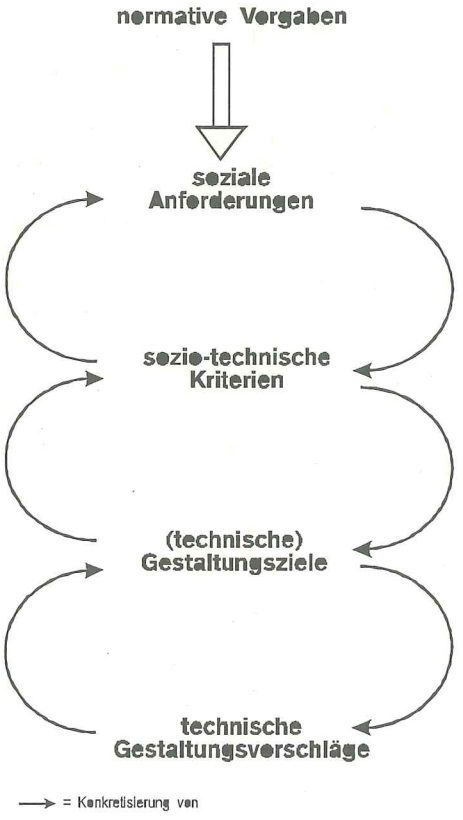


Abb. 1: Die Überwindung der Beschreibungslücke: Konkretisierungsebenen nach NORA. Technische Gestaltungsvorschläge entsprechen Anforderungen im Sinne einer Spezifikation

tung können sie daher nur mittelbar herangezogen werden.

Die normative Anforderungsanalyse bietet das notwendige Konzept, um die Beschreibungslücke zu überwinden.[10] Dazu werden die normativen Vorgaben in mehreren Schritten auf das zu gestaltende Technikfeld und das Anwendungsfeld, in dem die Technik eingesetzt werden soll, bezogen. Die Beschreibungslücke wird mit Hilfe von drei »Zwischenebenen« überwunden. Jede der Ebenen entspricht einem Modell, in dem die normativen Vorgaben (Normbereich), das Technikfeld und der Anwendungskontext mit zunehmender Techniknähe zu konkretisieren sind. Die Ebenen mit ihren Konkretisierungsbeziehungen bilden ein Kriteriensystem. Im Kriteriensystem werden auftretende Zielkonflikte möglichst nicht vorentschieden, sondern über die Ebenen mitgeführt. Dadurch wird ein möglichst großer Gestaltungsraum für die technische Lösung aufgespannt. Erst im letzten Konkretisierungsschritt müssen Entscheidungen getroffen werden, um Anforderungen für eine Spezifikation festzulegen. Mit einer anwendungs- und rollenspezifischen Konkretisierung kann dann allerdings auch sozialen Interessenkonflikten oder unterschiedlichen Bewertungen von Technikfolgen Rechnung getragen werden.

Die *schrittweise Konkretisierung* wird im weiteren für die verletzlichkeitsreduzierende Technikgestaltung dargestellt.[11]

Verletzlichkeitsreduzierende Technikgestaltung

»Klassische« Ansätze der IT-Sicherheit konzentrieren sich auf drei Grundbedrohungen und die korrespondierenden Schutzziele »Schutz der Vertraulichkeit«, »Schutz der Integrität« und »Schutz der Verfügbarkeit«.[12] Die Maßnahmen, die aus diesen Schutzzielen für die Technikgestaltung abgeleitet werden, sind weitgehend an der Technik orientiert und bemühen sich vorrangig, die Wahrscheinlichkeit von Störfällen gering zu halten (wahrscheinlichkeitsorientierte Sicherungsmaßnahmen).[13]

Anwendungsorientierte und relativierende IT-Sicherheitsbegriffe heben darauf ab, daß die trotz Sicherungsmaßnahmen verbleibenden Risiken tragbar sein sollen.[14] In der Anforderungsanalyse für Systemspezifikationen und Einsatzkonzepte muß daher berücksichtigt werden, wie Risiken von sozialen Systemen bewertet werden. Nur so kann erreicht werden, daß die Sicherungsmaßnahmen implementiert werden, die aus der Sicht der potentiell von Störungen betroffenen sozialen Systeme notwendig und wünschenswert erscheinen. Hinweise für die *soziale* Bewertung von Risiken bieten Untersuchungen aus der Psychologie, die Verfassungsverträglichkeit und Ansätze aus der Soziologie und Politologie, die im folgenden vorgestellt werden. Deren Faktoren werden herangezogen, um normative Vorgaben zu identifizieren.

Soziale Risikobewertung

Intuitive Risikokonzepte aus der Psychologie zeigen Faktoren auf, die mit einer »hohen« Risikobewertung durch Individuen korrelieren. Risiken werden intuitiv als »hoch« bewertet, wenn:[15]

- sie unfreiwillig eingegangen werden müssen,[16] unkontrollierbar, furchtbar und tödlich erscheinen, eine ungerechte Verteilung von Vor- und Nachteilen entsteht oder sie ein hohes Katastrophenpotential beinhalten (der Faktor wird als *dread Risk* bezeichnet),
- sie als nicht wahrnehmbar, unbekannt oder neuartig beurteilt werden oder ihre Wirkungen erst mit starker Verzögerung erwartet werden (*unknown Risk*), oder
- eine große Anzahl von Menschen einer Gefahr ausgesetzt sind, auch wenn der einzelne sich nicht unmittelbar bedroht fühlt (*exposure*).

Können diese Faktoren vermieden oder gering gehalten werden, ist mit einer höheren Akzeptabilität von IT-Systemen zu rechnen.

Technikanwendungen sollen mit den *Zielen des Grundgesetzes* verträglich sein oder diese fördern (Verfassungsverträglichkeit).[17] Hohe Schadenspotentiale können jedoch zu sozialen Sicherungsmaßnahmen zwingen und dadurch zu Einschränkungen von individuellen Freiheitsgrundrechten führen. Mittelbar können auch die Voraussetzungen der demokratischen Willensbildung beeinträchtigt werden. Können Störungen weitreichende Auswirkungen auf die Versorgung der Bevölkerung mit lebensnotwendigen Gütern und Leistungen haben, kann die staatliche Pflicht zur Daseinsvorsorge vernachlässigt sein. Schließlich trifft den Staat als demokratisch legitimiertes und verpflichtetes Organ des Allgemeininteresses auch eine Schutzpflicht für Leben und Gesundheit des einzelnen und zur Vermeidung von Katastrophen gesellschaftlichen Ausmaßes.

Von Vertretern aus der Soziologie, Politologie, Fehlerpsychologie und anderen Disziplinen wird ein weiterer Bewertungsansatz für Risiken vertreten.[18] Er geht vom unterschiedlichen Einfluß des Schadenspotentials und der Schadenswahrscheinlichkeit auf die *Überlebens- und Lernfähigkeit* sozialer Systeme aus. Lernfähigkeit meint in diesem Zusammenhang, daß das soziale System Kenntnisse und Fähigkeiten im Umgang mit dem technischen System erwerben und sich, falls erforderlich, durch Anpassung auf neue Bedingungen einstellen kann. Dies verbessert auch seine Überlebensfähigkeit. Niedrige Schäden verbessern zudem die Chance, daß Anwender aus Fehlern lernen können. Fehler machen zu dürfen (wegen niedriger Schadenspotentiale) ist wiederum eine Voraussetzung, um ein mentales Modell vom Verhalten von Techniksystemen zu entwickeln. Die Chancen, in Störfällen einem Human-Task Mismatch[19] mit schwerwiegenden Folgen zu entgehen, werden dadurch verbessert.

Für eine stärkere Berücksichtigung des Schadenspotentials in der Technikgestaltung spricht auch, daß die Güte der Abschätzung der beiden Dimensionen für Risikobewertungen häufig unterschiedlich ist.[20] Während künftige Schadenspotentiale vergleichsweise gut abgeschätzt werden können, liegen für die Schadenswahrscheinlichkeiten, insbesondere für neue und komplexe Systeme, häufig keine geeigneten Zahlen vor. Außerdem können die sozialen Faktoren, die die Fehler- und Angriffswahrscheinlichkeit beeinflussen, sehr großen Schwankungen unterliegen.

Normative Vorgaben

Die Ergebnisse zur sozialen Risikobewertung können in den folgenden normativen Vorgaben zusammengefaßt werden:[21]

(V1) *niedrige Schadenspotentiale:* Primär ist das Schadenspotential von IT-Anwendungen für alle potentiell betroffenen sozialen Systeme niedrig zu halten. Ausgangspunkt für die Bewertung

Zahl der Störereignisse ➲ / ⬇ Ausbreitung		einzelnes primäres Störereignis	mehrere gleiche / primäre Störereignisse
ohne Ausbreitung	einzelnes (Teil-)System	Einzelschaden	Kumulationsschaden
	viele unabhängige (Teil-)Systeme durch Ereignissteuerung	Synchronschaden	kumulierte Synchronschäden (untypisch)
mit Ausbreitung	lineare Ausbreitung	Kopplungsschaden	kumulierte Kopplungsschäden
	automatische Reproduktion	Multiplikationsschaden	kumulierte Multiplikationsschäden
	komplexe Ausbreitung	Komplexschaden	kumulierte Komplexschäden

Tabelle 1: Schadenstypen in Abhängigkeit vom Störungsverlauf

des Schadenspotentials muß dabei die künftige Abhängigkeit sozialer Funktionen vom Techniksystem sein.

(V2) *niedrige Schadenswahrscheinlichkeit:* Als zweite Komponente von Risiken ist die Schadenswahrscheinlichkeit zu betrachten. Sie wird in den meisten Ansätzen der IT-Sicherheit vorrangig verfolgt, ohne daß dies im Rahmen der Risikobewertung begründet wird.

(V3) *Autonomie:* Risiken sollen freiwillig übernommen werden können. Potentiell betroffene soziale Systeme müssen die Höhe ihres Risikos bestimmen und an veränderte Bewertungen anpassen können.

(V4) *Erfahrungsbildung:* Risiken sollen »erfahrbar« sein. Die Technikgestaltung muß deshalb die Erfahrungsbildung im Normalbetrieb und in Störungssituationen erlauben.

Im Unterschied zu den Grundbedrohungen der ITSEC geht die *verletzlichkeitsreduzierende Technikgestaltung* von diesen vier sozialen Zielen aus. Für sie kann unterstellt werden, daß sie auf breite Zustimmung als vernünftige Vorgaben einer Technikgestaltung stoßen. Sie eignen sich daher als Ausgangspunkte für eine Anforderungsanalyse und werden als *normative Vorgaben* bezeichnet.

Die vier normativen Vorgaben sind unter den Gesichtspunkten der sozialverträglichen Technikgestaltung allerdings nicht gleichgewichtig. Die größten Gewinne für die Sozialverträglichkeit sind zu erwarten, wenn es gelingt, Schadenspotentiale niedrig zu halten, weil dadurch z. B. soziale Sicherungszwänge vermieden und die Erfahrungsbildung gefördert werden können. *Verletzlichkeit* bezeichnet daher die Möglichkeit großer Schäden für gesellschaftliche Gruppen, Organisationen oder Individuen.[22] Eine hohe Verletzlichkeit durch Informations- und Kommunikationstechnik besteht für ein soziales System dann, wenn es durch technische Störungen hohe Schäden erleiden kann. Verletzlichkeitsreduzierende Technikgestaltung ist dementsprechend primär auf die Verminderung hoher Schadenspotentiale gerichtet. Die möglichen Abhängigkeiten zwischen den Risiken unterschiedlicher beteiligter Akteure durch den Technikeinsatz muß dabei berücksichtigt werden. Es ist eine Balancierung der Risiken anzustreben, die allen potentiell Betroffenen gerecht wird.

Soziale Anforderungen

Im ersten Konkretisierungsschritt werden aus den generalklauselartigen normativen Vorgaben soziale Anforderungen abgeleitet. Sie beschreiben in der Sprache eines sozialen Modells, welche Aspekte der Vorgaben auch unter dem Eindruck eines geplanten Technikeinsatzes aufrecht erhalten werden sollen. Für den Normbereich Verletzlichkeit können acht soziale Anforderungen identifiziert werden, auf die an dieser Stelle nur kurz eingegangen wird.

Bezogen auf die Leistungsfähigkeit des sozialen Systems sollen durch Störungen in IT-Systemen nur *niedrige Schäden* (A1) auftreten. Soziale Systeme sollen außerdem in Störungssituationen reagieren können (*Beherrschbarkeit von Störungssituationen*, A2), möglichst auch ohne die Hilfe Dritter. Soziale Systeme müssen ein aus ihrer Sicht akzeptables Risiko wählen können, wobei auch die Einflußnahme auf die Schadenshöhe möglich sein muß (*Selbstbestimmbare Risiken*, A3). Die Wahlmöglichkeiten hinsichtlich des Technikeinsatzes, seines Umfangs und der spezifischen Risikoausprägung sind für Anpassungen im Laufe der Zeit offen zu halten.

Soziale Systeme können außerdem darauf setzen, daß sie ihre Risiken selbst kontrollieren, unter anderem um im Störfall schneller handeln zu können, ihre Interessen selbst zu verfolgen und deshalb geringere Schäden zu erleiden, als wenn sie auf Reaktionen eines Dritten angewiesen sind. IT-Systeme sollten deshalb so gestaltet werden, daß sie auch die Möglichkeit zu *autonomer Technikanwendung* (A4) bieten. Wenn kleinere soziale Einheiten individuell auf Störungen reagieren können, kann dies auch aus der Sicht der jeweils größeren sozialen Einheit zur Beherrschbarkeit von Störungssituationen beitragen. Soziale Systeme müssen die Möglichkeit haben, Techniksysteme zu erproben und ihr Verhalten in Störfällen zu untersuchen (*Erprobungsmöglichkeiten*, A5). Schließlich soll die Technik so gestaltet werden, daß Fehler, Angriffsmotive und Angriffsmöglichkeiten vermieden werden (A6, A7 und A8)

Für den Schwerpunkt der verletzlichkeitsreduzierenden Technikgestaltung müssen die Anforderungen A1 und A2 sowie Teile von A3 bis A5 weiter konkretisiert werden. Im nächsten Konkretisierungsschritt sind dazu sozio-technische Kriterien zu bestimmen. Sie sollen beschreiben, wie die sozialen Anforde-

rungen im Zusammenwirken von sozialem System und Technik erfüllt werden können (sozio-technisches Modell). Bevor dies möglich ist, müssen allerdings die technikspezifischen Beiträge zu Schadenspotentialen identifiziert werden.

Exkurs: Technikspezifische Beiträge zum Schadenspotential

Primär sollen Störfälle mit hohen Schadenspotentialen vermieden bzw. beherrscht werden. Für die verletzlichkeitsreduzierende Technikgestaltung bietet es sich daher an, technikspezifische Beiträge von IT-Systemen zu Schadenspotentialen gering zu halten oder zu vermeiden. Potentiell hohe Schäden können zum einen aus einer Störungsursache entstehen, wenn ein *hoher Einzelschaden* möglich ist. Zum anderen sind hohe Schadenspotentiale möglich, wenn eine *Menge von Schäden* gemeinsam bewertet wird, weil sie auf die gleiche oder auf ähnliche Störungsursachen zurückzuführen sind. Für solche Fälle sind mögliche Störungsverläufe zu betrachten. Um Schadenspotentiale in Abhängigkeit vom Störungsverlauf zu charakterisieren, werden die folgenden *Schadenstypen* eingeführt.[23]

Mehrere Schäden, die auf gleichartige Störungsursachen zurückzuführen sind und aus der Sicht eines sozialen Systems gemeinsam zu bewerten sind, können in einem Kumulationsschaden zusammengefaßt werden. Schadenssummen entstehen auch durch Störungsverläufe, insbesondere auch dann, wenn die Störung nicht rechtzeitig erkannt wird oder die Handlungsmöglichkeiten nicht ausreichen, um den Störfall zu beherrschen (*hohe Störungsdynamik*). Die Ausbreitung von Störungen kann unterschiedliche Charakteristika aufweisen. Sie kann linear (Kopplungsschaden) oder als Spezialfall in der Form der automatischen Reproduktion erfolgen (Multiplikationsschaden). Viele Komponenten können auch betroffen sein, wenn sich ein primäres Störereignis über komplexe Abhängigkeiten ausbreitet (Komplexschaden). Durch die Möglichkeit zur Ereignissteuerung kann außerdem eine »außerhalb« der IT-Systeme liegende Störbedingung zur gleichzeitigen Störung vieler ansonsten unabhängiger Komponenten führen. Diese Form von Störungsdynamik ist technikspezifisch für IT-Systeme. Die Schadenssumme eines solchen Störfalls wird als Synchronschaden eingeordnet. Prominentes Beispiel ist das Jahr 2000-Problem.

Das Konzept der Störungsdynamik wird im Konkretisierungsprozeß nach NORA insbesondere in den Kriterien K1 bis K4 aufgegriffen. Die Kriterien werden im nächsten Abschnitt vorgestellt.

Sozio-technische Kriterien verletzlichkeitsreduzierender Technikgestaltung

Mit sozio-technischen Kriterien wird im zweiten Konkretisierungsschritt nach NORA ein »Modell« für das Zusammenwirken von sozialem und technischem System entwickelt. Die Kriterien werden für konkrete Anforderungsanalysen verwendet, um Gestaltungsalternativen zu suchen oder auszuwählen, die den sozialen Anforderungen gerecht werden. Dazu wird beschrieben, welche Eigenschaften für ein sozio-technisches System gelten sollen. Für die verletzlichkeitsreduzierende Technikgestaltung mit dem Schwerpunkt »Schadenspotential« können mit dieser Vorgehensweise zehn Kriterien entwickelt werden (vgl. Abb. 2):[24]

(K1) *Begrenzte Schadenshöhe*: Auch unter den Bedingungen eines Technikeinsatzes sollen für ein soziales System möglichst für alle Schadenstypen Obergrenzen für die Schadenshöhe durchgesetzt werden.

(K2) *Transparenz*: Transparenzmechanismen sollen das Erkennen und Analysieren von Störereignissen und die Planung von Maßnahmen unterstützen. Durch beobachtungsorientierte Sicherungsmaßnahmen sollen soziale Systeme außerdem das sie betreffende Schadenspotential erkennen können. Transparenz kann auch durch einfache Systemstrukturen gefördert werden.

(K3) *Niedrige Störungsdynamik*: Das Kriterium fordert eine Ausgestaltung von Techniksystemen und Einsatzkonzepten, in der sich Störungen nur schwer und nur langsam ausbreiten können. Dazu sind lose Kopplung und lineare Kopplungsstrukturen anzustreben. Außerdem sind Synchronisationsmechanismen (im oben beschriebenen Sinn) zu vermeiden. Zur losen Kopplung tragen auch zeitliche Spielräume oder vorbereitete spezielle und universelle Eingriffsmöglichkeiten für die Operateure bei.

(K4) *Graduelle Reduktion sozialer Funktionen*: Die graduelle Reduktion sozialer Funktionen ist eine besondere Form der losen Kopplung. Das Kriterium empfiehlt, Techniksysteme so zu strukturieren, daß auch beim Auftreten von Störungen wichtige soziale Kernfunktionen noch aufrecht erhalten werden. Dazu können beispielsweise unabhängige Substitutionsmechanismen auf niedrigerem Leistungsniveau zur Verfügung stehen.

(K5) Die *Unterstützung von Schadenskompensation* kann dazu beitragen, das nachlaufend Schäden ausgeglichen werden. Eingeschlossen sind Maßnahmen zur freiwilligen wie zur (rechtlich) durchsetzbaren[25] Kompensation.

(K6) *Entscheidungsfreiheit*: Das Kriterium fordert Entscheidungsmöglichkeiten für soziale Systeme bezüglich aller Aspekte, die risikorelevant sind. Dies bezieht sich z. B. auf Schadensobergrenzen, aber auch auf Störungsdynamiken.

(K7) Das Kriterium *Anpassungsfähigkeit* fordert, daß Techniksysteme in Übereinstimmung mit K6 angepaßt werden können und über die Zeit an veränderte Risikobewertungen anpaßbar bleiben.

(K8) Damit soziale Systeme Techniksysteme im Normalbetrieb selbst steuern und in Störungssituationen selbst handeln können, ist als Option eine *autonome Technikkontrolle* zu fordern. Ob diese Option wahrgenommen wird, unterliegt der Entscheidungsfreiheit (K6).

(K9) *Testunterstützung* soll im Wirkbetrieb und in Störungssituationen erlauben, das Verhalten eines IT-Systems zu untersuchen. Dazu sind zum ersten Testfunktionalitäten bereitzustellen. Zum zweiten ist eine Abgrenzung des Testbetriebs notwendig, damit Tests in produktiven Anwendungen keine hohen Schäden verursachen können.

(K10) Durch *Techniksicherung* sollen die aus den bisher genannten Kriterien abzuleitenden technischen Maßnahmen abgesichert und vor Fehlern und Angriffen geschützt werden. Dazu gehört beispielsweise auch der Schutz von verletzlichkeitsreduzierenden Maßnahmen durch eine geeignete Zugangs- und Zugriffskontrolle, wenn sie Angriffe erlauben können.

Diese zehn sozio-technischen Kriterien erweitern den Gestaltungsraum der IT-Sicherheit um schadenspotentialorientierte, beobachtungsorientierte und handlungsorientierte Sicherungsmaßnahmen. Sie ergänzen die klassischen Ansätze der IT-Sicherheit in der Anforderungsanalyse systematisch um den Schwerpunkt niedriger Schadenspotentiale und berücksichtigen durchgängig eine sozio-technische Sichtweise. Sie sind im nächsten Konkretisierungsschritt auf Gestaltungsobjekte zu beziehen. Für diese werde technische Gestaltungsziele abgeleitet.

Technische Gestaltungsziele

Die sozio-technischen Kriterien zur verletzlichkeitsreduzierenden Technikgestaltung konnten unabhängig von konkreten Techniksystemen und Anwendungskontexten formuliert werden. Im dritten Konkretisierungsschritt werden sie jedoch auf technische Gestaltungsobjekte angewandt.[26] Dazu wird gefragt, welche Eigenschaften diese Gestaltungsobjekte aufweisen müssen, damit die sozio-technischen Kriterien erfüllt werden können. Dazu müssen vier Bezüge hergestellt werden:

- zur *Größe sozialer Systeme*: Da die Möglichkeiten sozialer Systeme, Störungen zu verkraften, von ihrer spezifischen Leistungsfähigkeit abhängt, müssen die Eigenschaften von Gestaltungsobjekten an potentiell betroffenen sozialen Systemen ausgerichtet werden. Dies betrifft zum einen die vertretbare Schadenshöhe und zum anderen die Beobachtungs- und Handlungsoptionen, die für das soziale System zur Verfügung gestellt werden sollen. Häufig wird es dazu ausreichen, Individuen, Organisationen und gesellschaftliche Gruppen als idealtypische soziale Systeme zu unterscheiden.
- zu den *Interessen sozialer Systeme*: Soziale Systeme können in unterschiedlichen Rollen agieren, z. B. als Signierender oder als Empfänger signierter Willenserklärungen. Dementsprechend werden sie an Sicherungsmaßnahmen und damit auch an Technikkomponenten unterschiedliche Erwartungen haben. Das Konzept der rollenspezifischen Gestaltungsobjekte konnte erfolgreich eingesetzt werden, um diesem Aspekt in der Anforderungsanalyse Rechnung zu tragen.[27] Dabei wird durch einen »Übertragungsmechanismus« auch unterstützt, daß sich beispielsweise aus den Interessen des Prüfenden einer digitalen Signatur Anforderungen an die Signaturkomponente des Schlüsselinhabers ergeben.
- zu den potentiellen *Schäden*: Unterschiedlichen Schadensarten, z. B. »monetäre Verluste« oder »Verlust der elektronischen Geschäftsfähigkeit«, wird im allgemeinen mit unterschiedlichen Maßnahmen begegnet werden. Die Konkretisierung der Kriterien ist daher nach den zu erwartenden Schadensarten zu unterscheiden.

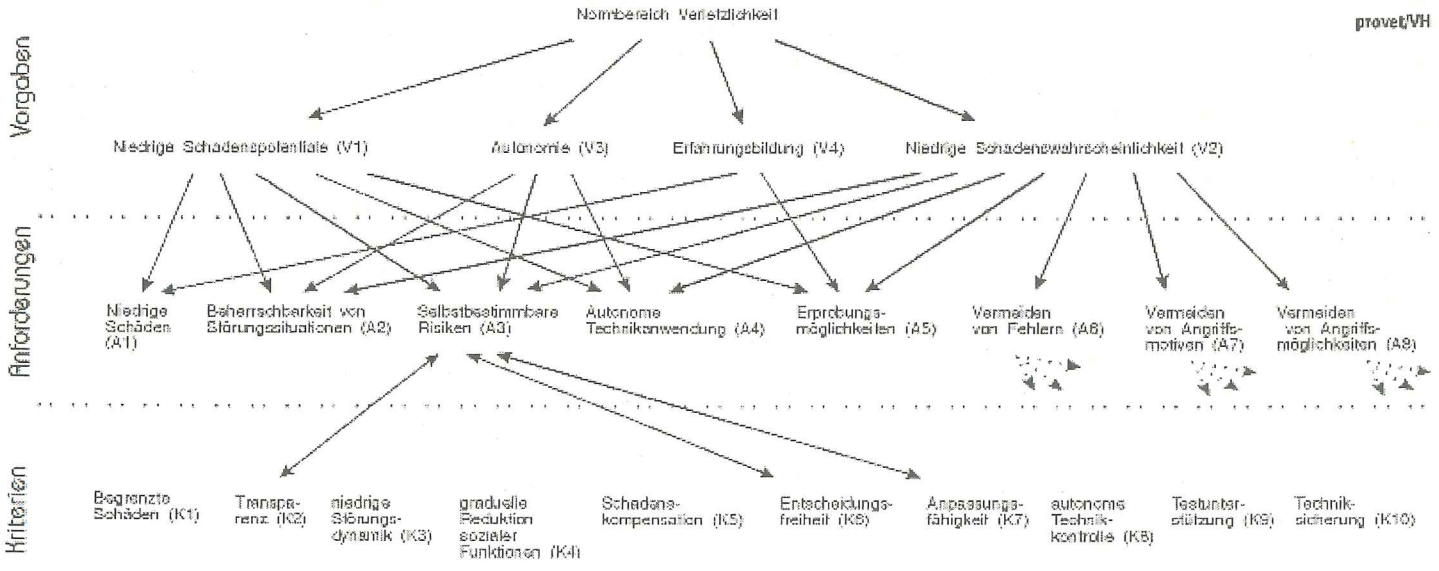


Abb. 2: Vorgaben, Anforderungen und schadenspotentialrelevante Kriterien. Die Relationen zwischen Anforderungen und Kriterien sind beispielhaft für A3 dargestellt. A4 bis A8 werden in den hier vorgestellten Kriterien nur in ihren schadenspotentialrelevanten Anteilen berücksichtigt.

- zu *relevanten Störfällen:* Verletzlichkeitsrelevante Störfälle werden identifiziert, indem aus der Perspektive des jeweiligen sozialen Systems nach Gestaltungsobjekten und Störungsverläufen mit hohem Schadenspotential gesucht wird. Die verschiedenen Störungsdynamiken bieten dabei Anhaltspunkte, an denen die Suche ausgerichtet werden kann, z. B. zur Identifikation zentraler Komponenten für mögliche Komplexschäden oder von Ereignissen, über die eine Synchronstörung entstehen kann. Der Begriff »Gestaltungsobjekt« wird dabei bewußt weit verstanden. Er schließt z. B. Einsatzkonzepte für Techniksysteme oder Strukturen, wie die Zertifizierungsgraphen, ein. Störfall-Szenarien, die ähnliche Eigenschaften aufweisen, können zu Klassen zusammengefaßt werden. Jede Klasse von Störfällen, die vom sozialen System beherrscht werden soll, wird dann als ein *Auslegungsstörfall* betrachtet. Ein Beispiel für einen Auslegungsstörfall ist die Forderung aus der Perspektive der Gesellschaft, daß das Auslaufen eines Zertifizierungsinstanz-Zertifikats nicht zum Verlust der elektronischen Geschäftsfähigkeit vieler Teilnehmer führen darf.

Die zehn Kriterien werden verwendet, um anhand von Auslegungsstörfällen wünschenswerte verletzlichkeitsreduzierende Sicherungsmaßnahmen zu identifizieren. Eine systematische Darstellung der Gestaltungsdiskussion ist wegen des Umfangs an dieser Stelle zwar nicht möglich.[28] Es können jedoch drei Beispiele aus dem Technikfeld Sicherungsinfrastrukturen angedeutet werden.

Beispiele

Nach dem SigG ist eine *Verwendungsbegrenzungen in Zertifikaten* vorgesehen. Im allgemeinen Fall wird sie allerdings nicht ausreichend sein, um Kumulations- oder Multiplikationsschäden durch den Mißbrauch eines Signaturschlüssels für den Schlüsselinhaber zu begrenzen. Zusätzlich wäre es notwendig, durch eine entsprechende Kontrolle auf der Chipkarte oder durch einen Autorisierungsdienst nur eine limitierte Anzahl von Nutzungen pro Zeiteinheit zuzulassen, um dem Kriterium »begrenzte Schäden« (K1) gerecht zu werden.

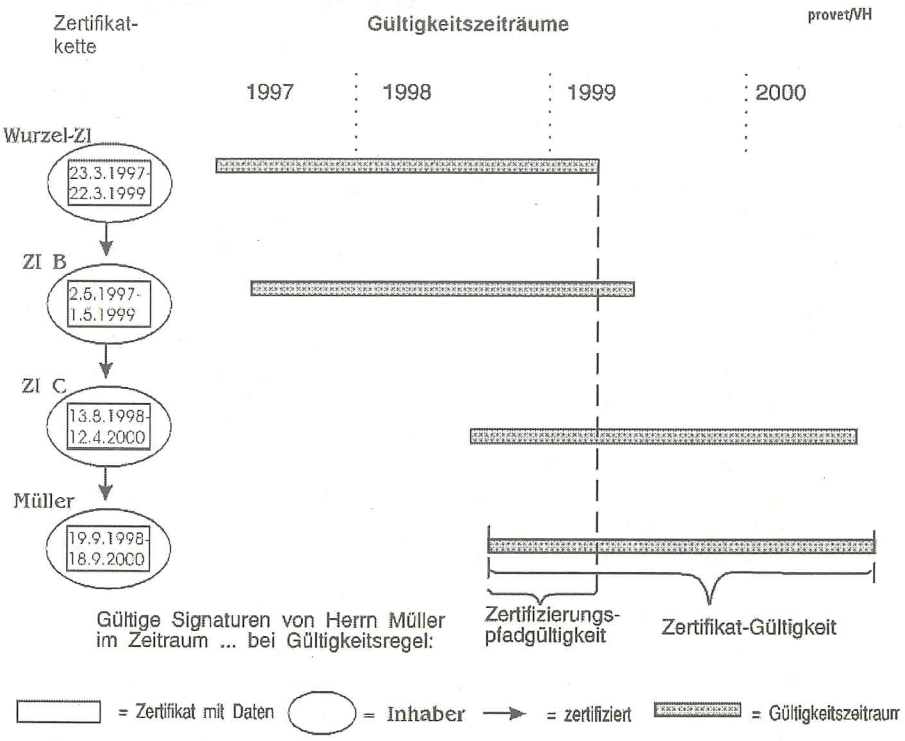


Abb. 3: Gültigkeitszeiträume für Signaturen in Abhängigkeit von der Regel zur Gültigkeitsprüfung. Zertifizierungspfad-Gültigkeit ist nur in der Schnittmenge der Gültigkeitszeiträume gegeben. Bei »Zertifikat-Gültigkeit« gilt dagegen (nur) die Bedingung, daß sich die Gültigkeitszeiträume der Zertifikate in der Zertifikatkette überlappen müssen.

Mißbrauchsfälle bei der Verwendung *von Zertifizierungsschlüsseln* müssen aus der Perspektive der jeweils betroffenen gesellschaftlichen Gruppe beherrscht werden. Bei genauerer Betrachtung zeigt sich, daß mehrere Auslegungsstörfälle unterschieden werden müssen. Zum ersten kann eine Sperrung für *künftige Verwendung* notwendig sein. Davon zu unterscheiden sind einzelne Mißbrauchsfälle, die erst *nach* den Manipulationen bekannt werden. In diesen Fällen kann es notwendig sein, einzelne Zertifikate *rückwirkend zu sperren.* In eine dritte Klasse fallen Störfall-Szenarien, in denen der Mißbrauch nicht abschätzbar ist oder die Ausforschung eines geheimen Schlüssels angenommen werden muß. In diesem Fall kann die *Sperrung einer Teilhierarchie* von Zertifikaten notwendig sein. Wenn die Sicherungsinfrastruktur auf die unterschiedlichen Störfall-Szenarien vorbereitet sein soll, müssen sowohl die Technikkomponenten der Vertrauensinstanzen als auch die Komponenten der Teilnehmer so ausgelegt werden, daß je nach Störfall die geeigneten Maßnahmen ergriffen werden können (K2 bis K4). Nur so können einerseits z. B. monetäre Schäden begrenzt und andererseits die elektronische Geschäftsfähigkeit möglichst gut aufrecht erhalten werden. Bisherige Sperrkonzepte differenzieren die Fälle allerdings nur unzureichend.

Zertifikate werden für einen Gültigkeitszeitraum ausgestellt. Für *Gültigkeitsprüfungen* sind unterschiedliche Akzeptanzregeln möglich (vgl. Abb. 3). Im Falle von Zertifizierungspfad-Gültigkeit wird gefordert, daß zum Signaturzeitpunkt alle Zertifikate einer Zertifikatkette gültig sind. Ohne besondere Vergaberegeln für Zertifikate kann es aus der Perspektive »Gesellschaft« deshalb beim Auslaufen eines Zertifizierungsinstanz-Zertifikats für alle Teilnehmer mit nachgeordneten Zertifikaten und deren Kooperationspartner zu einer Synchronstörung kommen. Muß dagegen jede Signatur nur im Gültigkeitszeitraum des übergeordneten Zertifikats ausgestellt werden (Zertifikat-Gültigkeit), wird die Störungsdynamik erheblich verringert (K3).[29] Aus der Perspektive der Zertifikatinhaber wären Transparenzmechanismen sinnvoll (K2), die sie frühzeitig auf das Gültigkeitsende ihres Zertifikats aufmerksam machen und

ihnen Spielräume für einen Zertifikatwechsel verschaffen.

Technische Gestaltungsvorschläge

Die technischen Gestaltungsziele werden unabhängig von der technischen Implementierung und dem Anwendungskontext formuliert. Diese Übertragung ist Gegenstand des letzten Konkretisierungsschrittes. Dazu wird geprüft, wie die technischen Gestaltungsziele, die für eine real zu implementierende Komponente beachtet werden müssen, mit den verfügbaren Ressourcen, eingesetzten Protokollen, Mitteln der Programmiersprache, geforderten Standards, bestehenden Schnittstellen usw. realisiert werden können. Der vorgesehene Nutzungskontext ist bei Entwurfsentscheidungen zu berücksichtigen. So sind für ein Anwendungssystem für einen ungeübten Privatanwender im Heimbereich andere technische Gestaltungsvorschläge zu erwarten als für eines, das ein professioneller Börsenmakler im Büro einsetzt.

Grenzen und Chancen der verletzlichkeitsreduzierenden Technikgestaltung

Wie mit anderen Ansätzen der IT-Sicherheit kann auch mit der skizzierten Methode selbstverständlich keine »vollständige Sicherheit« erreicht werden. Grenzen der verletzlichkeitsreduzierenden Technikgestaltung ergeben sich unter anderem, weil verletzlichkeitsreduzierende wie andere Sicherungsmaßnahmen neben einem Sicherungsbeitrag auch einen Störungsbeitrag aufweisen. Grenzen ergeben sich auch, wenn Schadenspotentiale durch die Randbedingungen eines Systemkonzepts nicht beeinflußt werden können. Oft können auch die Zielkonflikte innerhalb und zwischen den Kriterien oder zu anderen Anforderungsbereichen nicht völlig aufgelöst, sondern nur balanciert werden.

Mit den sozio-technischen Kriterien werden aber Gestaltungsoptionen erschlossen, die die Schadenspotentiale von Störungen begrenzen oder Beobachtungs- und Handlungsoptionen eröffnen, um sie zu beherrschen. Die verletzlichkeitsreduzierende Technikgestaltung ergänzt damit die herkömmlichen IT-Sicherheitsansätze um eine systematische Berücksichtigung der Dimension des Schadenspotentials. Sie trägt dazu bei, daß der sozialen Bewertung von Risiken und den langfristigen sozialen Folgen hoher Schadenspotentiale besser Rechnung getragen werden kann und die Beherrschung von Störfällen in der Anforderungsanalyse als sozio-technisches Problem berücksichtigt wird. Schließlich trägt die normative Anforderungsanalyse zur verletzlichkeitsreduzierenden Technikgestaltung dazu bei, daß mögliche individuelle Risikopräferenzen und die Interessenkonflikte zwischen verschiedenen Rollen aufgezeigt werden. Sie kann darauf hinweisen, daß für solche Probleme Anpassungs- und Aushandlungsmöglichkeiten in der Technik notwendig sind.

Praxiseignung der normativen Anforderungsanalyse

Mit der normativen Anforderungsanalyse können aus sozialen Zielen für die Technikentwicklung diejenigen für die Technikgestaltung erschlossen werden, für die eine weitgehende Konsentierung angenommen werden kann. Die normativen Vorgaben eines Normbereichs können in einem Kriteriensystem konkretisiert und nachvollziehbar dargestellt werden. Dadurch kann die Beschreibungslücke zwischen normativen Vorgaben und der Spezifikation überwunden werden. Die Erarbeitung eines solchen Kriteriensystems kann allerdings nicht Bestandteil von Anforderungsanalyse-Projekten sein, die den üblichen Rahmenbedingungen unterliegen. Dazu müssen Spezialisten aus dem Normbereich mit Informatikern in interdisziplinärem Austausch die Konkretisierung durchführen. Wurde ein Kriteriensystem jedoch einmal erarbeitet, können die Ergebnisse dieses Prozesses durchaus in Software-Projekten eingesetzt werden. Da die einzelnen Ebenen des Kriteriensystems eine gute Übertragbarkeit aufweisen, sind in einem Technikfeld in der Regel auch nur begrenzte Anpassungen für neue Fragestellungen erforderlich. Allerdings sind in der Regel Vorkenntnisse notwendig, um Kriteriensysteme nach NORA effizient einsetzen zu können. Drei Einsatzszenarien seien hier vorgestellt:

- Fachabteilungen mit entsprechenden Fragestellungen können auf entwickelte Kriteriensysteme zurückgreifen, sie für ihre Arbeit auswerten und gegebenenfalls anpassen.
- Beschäftigen sich Requirements Engineers während ihrer Ausbildung mit Kriteriensystemen der normativen Anforderungsanalyse, dann kennen sie sozio-technische Kriterien als Orientierung für die Anforderungsanalyse oder zur Überprüfung vorgeschlagener Lösungen. Insbesondere verfügen die Requirements Engineers über Sprachmittel, mit denen Kernprobleme der Normbereiche mit anderen Akteuren des Software-Engineering-Prozesses diskutiert werden können, bei Bedarf auch mit Spezialisten aus dem jeweiligen Normbereich.
- Zum Dritten können die Kenntnisse zu den Kriteriensystemen auch über externe Spezialisten, z. B. Consultants, für Software-Projekte eingekauft werden.

Selbstverständlich kann eine Anforderungsanalyse mit Hilfe von sozio-technischen Kriterien nach NORA nicht alle sozialen Anforderungen an Software erfüllen oder alle sozialen Konflikte *lösen*. Das Verfahren trägt vielmehr dazu bei, daß solche Anforderungen oder Konflikte systematisch erkannt und – neben anderen Anforderungen – in den Software-Entwicklungsprozeß eingebracht werden. In den Entwurfsentscheidungen sind aus einem großen Gestaltungsraum solche Lösungen zu suchen, die auch den sozialen Anforderungen Rechnung tragen. So werden beispielsweise soziale Konflikte nicht technisch vorentschieden, sondern können z. B. mit Aushandlungsmechanismen offen gehalten werden.

Kriteriensysteme der normativen Anforderungsanalyse können nachlaufend zur Bewertung von technischen Lösungen oder zur Wahl zwischen alternativen Techniksystemen genutzt werden. Ihr größtes Potential entfalten sie jedoch für die vorlaufende Technikgestaltung. Sie erlauben es Technikentwicklern, Fragestellungen der sozialen Einbindung von Technik bereits während der Planungs- oder Entwicklungsphase von Techniksystemen zu berücksichtigen. Dies verbessert die Chance zur Anwendbarkeit, weil nicht erst für eine fertige Spezifikation Änderungsbedarf festgestellt wird, sondern die sozialen Anforderungen prozeßbegleitend berücksichtigt werden können.

Literatur

Amann, E. / Atzmüller, H. (1992): IT-Sicherheit – Was ist das?, DuD 6/1992, 286 ff.

BSI – Bundesamt für Sicherheit in der Informationstechnik (1997): IT-Grundschutzhandbuch 1997 – Maßnahmenempfehlungen für den mittleren Schutzbedarf, Köln, 1997.

BSI – Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (1999): Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV – SigI Abschnitt A6 Gültigkeitsmodell, BSI, Bonn 1999.

Grimm, R. (1994): Sicherheit für offene Kommunikation – Verbindliche Telekooperation, Mannheim, 1994.

Guggenberger, B. (1987): Das Menschenrecht auf Irrtum, München, Wien, 1987.

Hammer, V. (1999a): Die 2. Dimension der IT-Sicherheit – Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen, Braunschweig/ Wiesbaden, 1999.

Hammer, V. (1999b): Verletzlichkeitsreduzierende Technikgestaltung für Beispiele aus Sicherungsinfrastrukturen, in: Horster, P. (Hrsg.): Sicherheitsinfrastrukturen – Grundlagen, Realisierungen, rechtliche Aspekte, Anwendungen, Braunschweig/ Wiesbaden, 1999, 163 ff.

Hammer, V. / Pordesch, U. / Roßnagel, A. (1993): Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, Heidelberg, New York, 1993.

Hammer, V. / Pordesch, U. / Roßnagel, A. / Schneider, M.J. (1994): Vorlaufende Gestaltung von Telekooperationstechnik am Beispiel von Verzeichnisdiensten, Personal Digital Assistants und Erreichbarkeits-Management in der Dienstleistungsgesellschaft, GMD-Studie 235, Sankt Augustin, 1994.

Hammer, V. / Sesink, W. (2000): Normative Anforderungsanalyse im Normbereich Bildung für Lernumgebungen, in Vorbereitung.

ITSEC (1993): Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik – Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, in: Internationale Sicherheitskriterien – Kriterien zur Bewertung der Vertrauenswürdigkeit von IT-Systemen sowie von Entwicklungs- und Prüfumgebungen, München, 1993, 427 ff.

Jungermann, H. / Slovic, P. (1993): Die Psychologie der Kognition und Evaluation von Risiko, in: Bechmann, G. (Hrsg.): Risiko und Gesellschaft, Opladen, 1993, 167 ff.

Kumbruck, C. (1999): Angemessenheit für situierte Kooperation, Münster, 1999.

Kumbruck, C. / Hammer, V. (1995): Psychologische Technikwirkungsforschung und -gestaltung im Bereich Telekooperationstechnologie, provet-Projektbericht Nr. 15, Darmstadt, September 1995.

Leveson, N. (1995): Safeware – System Safety and Computers, Bonn, 1995.

Pordesch, U. (2000): Der fehlende Nachweis der Präsentation signierter Daten, DuD 2/2000, 89 ff.

Pordesch, U. / Hammer, V. / Roßnagel, A. (1991): Prüfung des rechtsgemäßen Betriebs von ISDN-Anlagen, Braunschweig 1991.

provet / GMD (1994): Die Simulationsstudie Rechtspflege – Eine neue Methode zur Technikgestaltung für Telekooperation, Berlin, 1994.

Rannenberg, K. / Pfitzmann, A. / Müller, G. (1997): Sicherheit, insbesondere mehrseitige IT-Sicherheit, in: Müller, G. / Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Bonn, 1997, 21 ff.

Roßnagel, A. (1995): Die Verletzlichkeit der Informationsgesellschaft und rechtlicher Gestaltungsbedarf, in: Kreowski, H.-J. / Risse, T. / Spillner, A. / Streibl, R. E. / Vosseberg, K. (Hrsg.): Realität und Utopien der Informatik, Münster, 1995, 56 ff.

Roßnagel, A. / Schröder, U. (1999, Hrsg.): Multimedia in immissionsschutzrechtlichen Genehmigungsverfahren, Köln, 1999.

Roßnagel, A. / Wedde, P. / Hammer, V. / Pordesch, U. (1990a): Die Verletzlichkeit der 'Informationsgesellschaft', Opladen, 1990.

Roßnagel, A. / Wedde, P. / Hammer, V. / Pordesch, U. (1990b): Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, Opladen, 1990.

Rudinger, G. / Espey, J. / Holte, H. / Neuf, H. (1996): Der menschliche Umgang mit Unsicherheit, Ungewißheit und (technischen) Risiken aus psychologischer Sicht, in: BSI – Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Kulturelle Beherrschbarkeit digitaler Signaturen – Interdisziplinärer Diskurs zu querschnittlichen Fragen der IT-Sicherheit, Ingelheim, 1996, 128 – 154.

Starr, Ch. (1969): Sozialer Nutzen versus technisches Risiko; Übersetzung von Rader, M, Original: Science, 19/1969, 1232 ff.; übersetzt in: Bechmann, G. (Hrsg.): Risiko und Gesellschaft, Opladen, 1993, 3 ff.

Wehner, T. (1993): Zum Umgang mit Fehlern, BSI-Forum in KES 5/1993, 49f.

Weizsäcker, C. v. / Weizsäcker, E. U. v. (1984): Fehlerfreundlichkeit, in: Kornwachs, K. (Hrsg.): Offenheit – Zeitlichkeit – Komplexität. Zur Theorie der Offenen Systeme, Frankfurt a.M., 1984, 167 ff.

---

1 Der Aufsatz gibt eine Übersicht über Ergebnisse aus Hammer 1999a. Er ist eine ergänzte und überarbeitete Fassung von Hammer 1999b.

2 Vgl. Hammer/Pordesch/Roßnagel 1993. Ausführlicher zur Entstehungsgeschichte siehe auch Hammer 1999a, Kap. 9 mwN.

3 Pordesch/Hammer/Roßnagel 1991.

4 Hammer/Pordesch/Roßnagel/Schneider 1994, 28 ff.

5 Hammer/Pordesch/Roßnagel/Schneider 1994, 101 ff.

6 Z. B. Pordesch/Roßnagel, DuD 1994, 82 ff., Roßnagel / Schröder 1999 und Pordesch, DuD 2000, 89 ff.

7 Vgl. Kumbruck 1999 mwN.

8 Hammer 1999a, Kap. 10 ff.

9 Hammer / Sesink 2000.

10 Zur Vorgehensweise siehe Hammer 1999a, Kap. 9 mwN.

11 Zum weiteren siehe die Entwicklung des Kriteriensystems mit den ausführlichen Konkretisierungsschritten in Hammer 1999a, Kap. 10 ff.

12 Z. B. ITSEC 1993, 427 ff.

13 Vgl. dazu und zum folgenden die Analyse in Hammer 1999a, Kap. 4 bis 6.

14 So Z. B. in BSI 1997, Kap. 1-5, oder in Amann/Atzmüller, DuD 1992, 287.

15 Z. B. Jungermann / Slovic 1993, 167 ff.; Rudinger / Espey / Holte / Neuf 1996, 128 ff.

16 Bereits Starr 1969, 12 stellt eine »Differenz, um mehreren Größenordnungen, zwischen der gesellschaftlichen Bereitschaft, 'freiwilliges' oder 'unfreiwilliges' Risiko zu akzeptieren« fest.

17 Vgl. zu diesem Absatz und den folgenden Aspekten z. B. Roßnagel / Wedde / Hammer / Pordesch 1990a und Roßnagel / Wedde / Hammer / Pordesch 1990b, 171 ff.; Roßnagel 1995, 56 ff.

18 Vgl. z. B. Guggenberger 1987; Wehner, BSI-Forum 1993, 49f., oder Weizsäcker / Weizsäcker 1984, 167 ff.

19 Leveson 1995, 91-126, bezeichnet damit Situationen, in denen Operateure die Aufgabe, ein technisches System zu steuern, nicht erfüllen können, weil dies durch die Situation und das Technikystem verhindert wird. Ein Grund können unzureichende oder verfälschte Informationen über Störungsursachen sein.

20 Vgl. die Nachweise in Wehner, BSI-Forum 1993, 146 ff.

21 Siehe zum folgenden Hammer 1999a, Kap. 7 und die Begründungen in Kap. 4-6 mwN.

22 Roßnagel/Wedde/Hammer/Pordesch 1990a, 7; provet/GMD 1994, 20f.

23 Vgl. Hammer 1999a, Kap. 8.

24 Zur Konkretisierung der Kriterien siehe ausführlich Hammer 1999a, Kap. 10.4.

25 Vgl. dazu auch den Ansatz des Gleichgewichtsmodells bei Grimm 1994.

26 Vgl. dazu Hammer 1999a, Kap. 11, und die Beispiele in Kap. 12-14. Da sich die Kriterien auf sozio-technische Systeme beziehen, können mit ihnen auch Gestaltungsziele für andere Gestaltungsobjekte, beispielsweise Rechtsregeln oder organisatorische Maßnahmen abgeleitet werden. In der Praxis werden sogar im allgemeinen Systemlösungen zu suchen sein, die sich aus einer Kombination der verschiedenen Gestaltungsziele zusammensetzen. Im Sinne einer Technikgestaltung sollte jedoch zunächst versucht werden, technische Gestaltungsobjekte gemäß der Kriterien auszuformen. Kompensationsmaßnahmen für technische Defizite durch Recht, Organisation oder soziale Anpassung sind nur Mittel der zweiten Wahl.

27 Dadurch wird mit NORA das Ziel der mehrseitigen Sicherheit (vgl. Rannenberg / Pfitzmann / Müller 1997, 21 ff) in der Anforderungsanalyse berücksichtigt.

28 Zu diesen und weiteren Beispielen ausführlich Hammer 1999a, Kap. 11-14 mwN. Auf die Ebene der technischen Gestaltungsvorschläge nach NORA geht dieser Aufsatz nicht ein.

29 Die Regeln für »Zertifikat-Gültigkeit« werden in BSI 1999 angewandt.

Marit Köhntopp

Verletzlichkeit und Vertrauen

Vertrauen ist gut, Kontrolle ist besser. – Lenin

Verletzbare Gesellschaft

Immer stärker wird uns bewusst, dass wir in einer verletzlichen Risikogesellschaft leben. Die Verletzlichkeit der Gesellschaft wird beispielsweise im Bereich der Informationstechnologie deutlich. Hier ist dasselbe Phänomen zu beobachten wie zu Beginn der industriellen Revolution, als sich zwar immer mehr der Nutzen des Technikeinsatzes abzeichnete, aber noch gar nicht an Aspekte der Arbeitssicherheit oder des Umweltschutzes gedacht wurde. Am Anfang einer Entwicklung gibt es stets genügend Probleme, um überhaupt die Funktionalität ausreichend sicherzustellen, bevor dann quasi als Kürprogramm die »Randthemen« angegangen werden können. So manches fällt da der Geschwindigkeit des Fortschritts zum Opfer: »Unter hoher Wachstumsgeschwindigkeit hat die Informatik kein professionelles Selbstverständnis entwickelt, das per se zuverlässig ist und bedachte Konstruktionen zum beruflichen Normalfall werden lässt.« [Coy_92]

Im Unterschied zur industriellen Revolution sind die Nebenwirkungen des jetzigen Umbruchs, gekennzeichnet durch eine zunehmende Durchdringung aller Lebensbereiche mit vernetzten Computern, weniger offensichtlich. Durch eine zunehmende Komplexität der technischen Welt sind große Datenverarbeitungssysteme längst nicht mehr durchschaubar, auch nicht für Experten. Gerade die steigende Abhängigkeit von stets korrekt arbeitenden und stets verfügbaren IT-Systemen bewirkt, dass die Effekte, die durch lediglich einen Fehler im ganzen System oder den Ausfall nur einer Komponente hervorgerufen werden, immens sein können. Oft sind sie nicht eng räumlich oder zeitlich beschränkt, wie dies beispielsweise die regelmäßig neu entstehenden und in Umlauf gebrachten E-Mail-Viren zeigen – der I-Love-You-Wurm war da noch vergleichsweise nett. Aus solchen Fehlfunktionen oder Angriffen können handfeste materielle Schäden, aber auch tatsächliche Bedrohungen für Leib und Leben folgen, z.B. wenn der Bereich der medizinischen Versorgung betroffen ist.

Solange alles gut geht oder man den Schaden nicht merkt, zerbrechen sich die meisten nicht den Kopf darüber, wie Fallback-Lösungen aussehen können oder wie man bereits beim Design der Systeme als Absicherung »sowohl Gürtel als auch Hosenträger« vorsieht. Dadurch, dass ein Schaden nicht sofort offensichtlich ist oder auch nicht in erkennbarer Beziehung zu dem fehlerhaften System steht, wird ein angemessenes Reagieren noch schwieriger. Es bleibt nur die Aussage: »We have never had an undetected break-in ...« [ChBe_94]. Gerade bei Aspekten der Vertraulichkeit ist dies in besonderem Maße relevant, denn dass Unbefugte an Informationen herangekommen sind, die sie irgendwann einmal vielleicht in einem ganz anderen Kontext verwenden, ist schwer zu beweisen. Ein solcher Schaden ließe sich jedoch nicht einfach wieder aus der Welt räumen.

Wird doch eine Bedrohung offenbar, muss für sehr viel Geld nachgelegt werden. Selbst dann fehlen meist die Garantien, dass tatsächlich alles im grünen Bereich bleibt. Dies zeigte sich beispielsweise bei der Jahr-2000-Problematik, als zum Jahreswechsel auch noch um Mitternacht völlig unklar war, ob alles reibungslos ablaufen würde, obwohl riesige Geldsummen und ganze Trupps von Jahr-2000-Beauftragten zur Lösung des Problems aufgefahren worden waren. Die Computer-Experten wussten es einfach nicht.

Wertvolles Vertrauen

Vertrauen spielt nicht nur im persönlichen Leben, sondern auch als Herzstück für das Funktionieren der Gesellschaft und der Wirtschaft eine Rolle. Dies gilt um so mehr, als in der Informationsgesellschaft der persönliche Kontakt zum Abwickeln von Geschäften immer weniger von Bedeutung ist, sondern Transaktionen vollständig über das Netz abgewickelt werden können. Eine zwischenmenschliche Beziehung, die Basis für das Vertrauen sein könnte, fehlt hier völlig. Von dem Vertrauen hängt aber viel ab: Ohne ein Vertrauen in Personen und in Technik sowie in die damit verbundenen sozialen Systeme könnten moderne Gesellschaften nicht überleben [BBFK_99].

Um Vertrauen aufzubauen, gibt es keine Patentrezepte. Es ist aber recht offensichtlich, wie sich Vertrauen zerstören lässt: wenn öffentlich gemacht wird, dass ein Vertrauen nicht gerechtfertigt ist, oder wenn das Vertrauen enttäuscht wurde. Die Presse hat hierbei eine große Macht, denn in der Regel geht es in der Vertrauensfrage weniger um einen objektiven Gefährdungstatbestand, sondern Gerüchte können bereits ausreichen, um Misstrauen zu erzeugen. In der heutigen Welt hat dies meist unmittelbare finanzielle Auswirkungen; z.B. sind solche Enttäuschungen der Menschen oft mit sinkenden Aktienkursen der entsprechenden Firma verbunden, wie dies der Fall war, als die Firma DoubleClick ankündigte, ihre Internet-Marketingdaten mit einer Datenbank zusammenzuführen, in denen Informationen über Millionen von US-Haushalten gespeichert waren. Die Kunden fühlten sich hinters Licht geführt und brachten ihren Unmut darüber deutlich zum Ausdruck.

Inwieweit die Menschen auf dem Weg in die Informationsgesellschaft mitgehen, hängt davon ab, wie groß ihr Vertrauen in die IT-Systeme ist [Camp_00]. Bei fehlender Akzeptanz wird die Technik boykottiert, oder – ist dies nicht möglich –sie kommt nur widerwillig und nur soweit unbedingt nötig zum Einsatz. Dies zeigt sich gerade im E-Commerce, der nicht so recht vom Fleck kommt. Ein Hauptgrund liegt laut Umfragen darin, dass die Kunden Bedenken haben, was ihre Datensicherheit und ihren Datenschutz im E-Commerce angeht, und deswegen sehr zurückhaltend agieren. Speziell der Datenschutzbereich hängt in besonderem Maße mit Vertrauen zusammen: »Datenschutz ist [...] in seiner Gesamtheit symbolisiertes Vertrauen der Informationsgesellschaft in ihre technischen Kommunikationsmittel durch eine Koppelung des Vertrauens in das jeweils genutzte technische System mit dem Vertrauen in das Rechtssystem. Allerdings können fortgesetzte Meldungen über die Nichteinhaltung dieses Vertrauen gefährden.« [Burk_91]

Verletzlichkeit zerstört Vertrauen

Diese unsichere Situation, der sich jeder Bürger ausgesetzt sieht, ist nicht besonders vertrauenerweckend. Es ist noch nicht einmal mehr möglich, das Vertrauen auf die Experten zu »delegieren«, denn diese geben zu, dass sie selbst die Systeme nicht mehr vollständig durchschauen, und legen für die korrekte Funktionsweise nicht die Hand ins Feuer. Viele Menschen verschließen die Augen vor der Situation: aus Hilflosigkeit oder weil sie gewohnt sind, dass der Staat es schon richten wird. Der Staat ist aber genauso überfordert von der Situation und kann das Problem der Verletzlichkeit nicht alleine lösen. Andere Leute versuchen, sich selbst – zumindest scheinbar – kontrollierbare Umgebungen zu schaffen. Im Jahr-2000-Beispiel gab es in den USA Aufrufe, sich mit Notrationen für eine längere Zeit einzudecken und gegen die erwarteten Plünderungsversuche derjeniger, die nicht vorgesorgt haben, Waffen bereitzuhalten. Da fragt man sich, ob nicht die verbreitete Hysterie zum Jahreswechsel mindestens ebenso gefährlich war wie das Jahr-2000-Problem selbst. Die Radikalkur zur Lösung des Verletzlichkeitsproblems mit Parole wie««Zurück in die (Vor-Computer-)Steinzeit« wäre nicht ernsthaft durchsetzbar und ist keine Lösung, denn dies würde das Aussteigen aus der heutigen Gesellschaft bedeuten.

Verletzlichkeit erfordert Vertrauen

Gerade weil es keine vollständige Sicherheit gibt, ist Vertrauen zum Funktionieren der Gesellschaft notwendig. Denn Vertrauen tritt da ein, wo die totale Kontrolle und Beherrschung eines Systems eben nicht gegeben ist. Wer zu wenig über die Funktionsweise eines Systems weiß, muss vertrauen. Blindes Vertrauen ist jedoch gefährlich: Es kann schnell umschlagen und erhöht sogar die Verletzlichkeit, denn durch einen weniger risikobewußten Umgang verbreitert sich die Angriffsfläche. Daher muss ein Vertrauen, auf das unsere Gesellschaft bauen kann, auf stabilen Füßen stehen. Und das geht nicht bei der heutigen potenziell hohen und sogar noch steigenden Verletzlichkeit der Systeme. Ebenso darf nicht weiterhin nur an Symptomen kuriert werden, sondern die Ursachen müssen erkannt und angegangen werden. Im Datenschutzbereich ist dies bereits zu merken, denn mit der Entwicklung »Datenschutz durch Technik« und der Beteiligung von Datenschutzinstitutionen an der Technikgestaltung auf ihren verschiedenen Ebenen findet man mittlerweile eine strukturellere Herangehensweise, die im Vorfeld schon viel bewirken kann und deutlich effektvoller ist als Versuche, in späteren Entwicklungsphasen nachträglich einzuwirken [KöRu_99]. Auch in anderen Bereichen muss viel mehr getan werden, um die strukturellen Zusammenhänge zu erkennen und dann zu angemessenen Handlungsvorschlägen zu kommen. Das dafür nötige interdisziplinäre, vernetzte Denken ist nicht einfach und muss erst gelernt werden.

Mehr Vertrauen; wie?

Vertrauensbildung ist ein komplexer gesellschaftlicher und persönlicher Prozess. Eng damit verknüpft ist der Grad der Informiertheit, denn nur mit ausreichender Information können die Chancen und Risiken neuer Techniken bewertet werden, die die Grundlage für die weitere gesellschaftliche Entwicklung darstellen. Hier gilt es, Medienkompetenz schon von Kindesbeinen an zu vermitteln. Dennoch wird dies aufgrund der hohen Komplexität der Systeme nicht ausreichen; es ist davon auszugehen, dass weiterhin für die meisten Nutzer die Informationstechnik undurchschaubar ist [EsRN_99]. Dies liegt auch daran, dass diese Technik nicht so einfach »begreifbar« ist wie beispielsweise das mechanische Ineinandergreifen von Zahnrädern. Aus diesem Grund sind vertrauenswürdige Experten, bei denen die Systeme auf den Prüfstand kommen, ganz wichtig für das gesellschaftliche Vertrauen. Ihre Vertrauenswürdigkeit muss allerdings gerechtfertigt sein, z.B. durch eine Unabhängigkeit von wirtschaftlichen Interessen, durch größtmögliche Transparenz ihres Vorgehens und durch eine Vielfalt der Vertrauensstellen und Experten mit Wahlmöglichkeiten für Bürger. Die Datenschutzbeauftragten als unabhängige Instanzen oder unabhängige Wissenschaftler, aber auch z.B. eine »Stiftung »Datenschutztest« analog zur »Stiftung »Warentest« oder Wissenschaftler, kämen hier als vertrauenswürdige Experten in Frage.

Damit aber überhaupt Aussagen über Technik und ihre Auswirkungen getroffen werden können, müssten die technischen Systeme und die Verquickungen verschiedener Komponenten transparent sein. Black Boxes führen hier nicht weiter. Ein modularer Aufbau, definierte Schnittstellen und eine ausreichende Dokumentation sind selbstverständlich.

Ausblick

Tatsächlich sind die Möglichkeiten für weniger Verletzlichkeit und mehr Vertrauen zurzeit nicht ungünstig: In den letzten Jahren wurde das Niveau dessen, was zum Standardumfang der Systeme an Sicherheitsfunktionalität gehört, deutlich gehoben, beispielsweise die integrierten RAID-Systeme im Windows-Server-Betriebssystem oder die eingebaute Möglichkeit der Verschlüsselung in Internet-Browsern. Hier lässt zwar die Umsetzung noch in Teilen zu wünschen übrig, doch die Durchdringung bei den Nutzern nimmt zu. Gleichzeitig besteht hier auch das Problem, dass vieles über proprietäre Systeme, die nicht offengelegt sind, und Monokulturen, bei denen erfolgreiche Angriffe gleich sehr viel mehr Auswirkungen haben, realisiert ist.

Vermutlich werden wir in nächster Zeit noch des öfteren Denial-of-Trust-Attacks, also Angriffe, die das Vertrauen der Nutzer erschüttern, erleben. Einige haben dies erkannt und arbeiten daran, sowohl die Verletzlichkeit zu reduzieren als auch vertrauenswürdige Stellen als Service-Einheiten für die Nutzer zu schaffen, bei denen nicht nur Vertrauen draufsteht, sondern auch drin ist.

Literatur

[BBFK_99] Hans-Joachim Braczyk, Jochen Barthel, Gerhard Fuchs, Kornelia Konrad: Trust and Socio-Technical Systems; in: Günter Müller, Kai Rannenberg (Hg.): Multilateral Security in Communications – Technology, Infrastructure, Economy; Addison-Wesley-Longman, München 1999; 425-438

[Burk_91] Herbert Burkert: Systemvertrauen: Ein Versuch über einige Zusammenhänge zwischen Karte und Datenschutz; à la Card Euro-Journal; Heft 1, 1991; 52-66; http://www.gmd.de/People/Herbert.Burkert/CardTrust.html

[Camp_00] L. Jean Camp: Trust and Risk in Internet Commerce; MIT Press, 2000; frühere Version unter http://www.ksg.harvard.edu/people/jcamp/trustRisk/book.html

[ChBe_94] William R. Cheswick, Stephen M. Bellovin: Firewalls and Internet Security; Addison-Wesley 1994

[Coy_92] Wolfgang Coy: Informatik – Eine Disziplin im Umbruch?, in: Wolfgang Coy u.a. (Hg.): Sichtweisen der Informatik; Vieweg; Braunschweig 1992; 1-9.

[EsRN_99] Jürgen Espey, Georg Rudinger, Hartmut Neuf: Excessive Demands on Users of Technology; in: Günter Müller, Kai Rannenberg (Hg.): Multilateral Security in Communications – Technology, Infrastructure, Economy; Addison-Wesley-Longman, München 1999; 439-449

[KöRu_99] Marit Köhntopp, Ingo Ruhmann: Trust through Participation of Trusted Parties in Technology Design; in: Günter Müller, Kai Rannenberg (Hg.): Multilateral Security in Communications – Technology, Infrastructure, Economy; Addison-Wesley-Longman, München 1999; 499-514

FIfF e.V.

Pressemitteilung

Kiel, 29. August 2000

Neuer Standard für Online-Privacy in Deutschland vorgestellt

Anlässlich der Vorstellung des aufkommenden neuen P3P-Standards im Rahmen der Sommerakademie in Kiel erklären die Datenschutzbeauftragten von Berlin, Brandenburg, Hamburg, Nordrhein-Westfalen, Schleswig-Holstein und Zürich:

Stellen Sie sich vor, beim Einkaufen im Internet geht in Ihrem Browser automatisch ein Fenster auf: »Der Anbieter XYZ benötigt von Ihnen den Namen und die Lieferadresse, um Ihnen die Ware zustellen zu können. Die Daten werden nur zur Abwicklung dieser Transaktion verwendet und keinen Dritten übermittelt. Bitte geben Sie die Daten in das Formular ein.« Weil Sie damit einverstanden sind, bestätigen Sie und weisen per Mausklick Ihren Computer an, die erforderlichen Daten automatisch in das Formular einzugeben.

Auch über andere Dinge wie Cookies oder die Möglichkeit einer persönlichen Website-Gestaltung nach Ihren Wünschen könnten Sie bequemer entscheiden. Bei bestimmten Meldungen von Websites, die Ihre persönlichen Informationen anfordern, sind Sie aber vielleicht gar nicht einverstanden und geben daher auch keine Daten heraus. Statt dessen beschweren Sie sich per E-Mail beim Anbieter oder fragen bei einer Datenschutzstelle nach, ob das Verhalten der Website in Ordnung ist.

So weit sind wir von einem solchen Szenario gar nicht entfernt. Mit »P3P Platform for Privacy Preferences« kommt ein neuer weltweiter Standard für Online-Privacy, der erstmalig in Deutschland im Rahmen der Sommerakademie in Kiel vorgestellt wird. Mit P3P können Websites auf einfache Weise ihre Privacy Policy nach einem einheitlichen Schema ausdrücken, sodass sie von dem Nutzerrechner ausgewertet werden kann. Die Nutzerin

Pressemitteilung

Kiel, 29. August 2000

oder der Nutzer entscheidet dann, ob sie oder er er die Website unter den gegebenen Bedingungen besuchen möchte oder nicht. Außerdem soll es Software für P3P geben, die sich merkt, welche Informationen man unter welchen Bedingungen herausgegeben hat. Dies ist ein wesentlicher Schritt in Richtung informationelle Selbstbestimmung, denn wer hat heutzutage schon den Überblick darüber, wo er welche Daten gelassen hat?

P3P als universeller, technischer Standard erlaubt es, weltweit im ganzen Internet Datenschutz-Policies für die Nutzer transparent zu machen, sofern die Anbieter P3P auch verwenden. Die Nutzer haben damit eine größere Kontrolle darüber, was mit ihren persönlichen Daten geschieht. P3P kann sich den verschiedenen lokalen Bedingungen anpassen und damit einen Wettbewerb der Anbieter um den besten Datenschutz ermöglichen.

Der internationale Standardisierungsprozess von P3P 1.0, der vom World Wide Web Consortium (W3C) betrieben wird, steht kurz vor dem Abschluss. An der Standardisierung beteiligen sich neben Firmen und Organisationen auch Datenschutzbeauftragte, z.B. aus Kanada und der EU. In Kürze werden die ersten Software-Tools für P3P allgemein verfügbar sein. Rigo Wenning vom W3C erklärte: »P3P definiert eine Basis für die weitere Entwicklung des Datenschutzes. Das Meeting der Working Group in Kiel zeigt, dass europäische Werte durch die Beteiligung der Datenschützer Eingang in die Spezifizierung finden und das W3C der Mitarbeit der Datenschutzbeauftragten einen hohen Wert beimisst. P3P ist auch eine globale Herausforderung für den europäischen Datenschutz.«

Von den europäischen Datenschutzbeauftragten kommen immer mehr zu dem Schluss: Die P3P-Technik ist nützlich für den Datenschutz im Internet, allerdings für sich allein nicht ausreichend, denn P3P stellt nur einen technischen Basisstandard zum Schutz der Privatsphäre zur Verfügung. Unverzichtbar bleiben auch in Zukunft eine ergänzende, wirksame Datenschutzkontrolle und präzise Rechtsnormen zum Schutz der Internetnutzerinnen und -nutzer. Mit P3P wird es möglich, viele Regelungen der vorbildlichen europäischen Datenschutzgesetze in »Bits und Bytes« umzusetzen. Schwieriger ist es in diesem Punkt für den Datenschutz in den USA, in denen die Bürgerinnen und Bürger beim Surfen ohne den Rückhalt von Gesetzen und Datenschutzbeauftragten auskommen müssen.

In Deutschland stellt sich die Aufgabe, P3P so schnell wie möglich zu implementieren und auf seiner Basis ein vollständiges Datenschutzkonzept zu entwickeln, damit das Teledienstedatenschutzgesetz adäquat umgesetzt wird. P3P in der Version 1.0 ist ein erster Schritt in die richtige Richtung. Mit P3P 1.0 ist die Entwicklung in diesem Bereich aber noch nicht zu Ende, sondern es gilt, im weiteren Prozess zusätzliche Features einzubringen.

Auf Dauer könnte sich der Einsatz von P3P und weiteren Datenschutz-Tools als Wettbewerbsvorteil für die deutsche Internetbranche erweisen, denn das Teledienstedatenschutzgesetz verfügt über einen auch im europäischen Vergleich hohen Datenschutzstandard. Die Kundinnen und Kunden werden, wenn man die Verbraucherumfragen in vielen Ländern berücksichtigt, Webseiten bevorzugen, auf denen ihnen ein Maximum an Datenschutz technisch garantiert wird.

P3P ist ein wichtiger Baustein einer neuen Datenschutzkonzeption, die verstärkt auf Transparenz und marktwirtschaftliche Elemente setzt. P3P gibt den Datenschutzstellen neue Möglichkeiten, mit der Industrie zu kooperieren und den effektiven Datenschutz in Europa zum Wettbewerbsfaktor werden zu lassen. In Zukunft sollen mehr und mehr die Kundinnen und Kunden die Möglichkeit haben, durch ihr Verhalten eine spürbare Nachfrage nach Datenschutz zu erzeugen. Dadurch soll den Unternehmen klar werden, dass der europäische Datenschutz ein Standortvorteil ist und dass datenschutzwidrige Angebote auf Dauer keine Chance auf dem Markt haben.

P3P-Homepage:
http://www.w3.org/P3P/

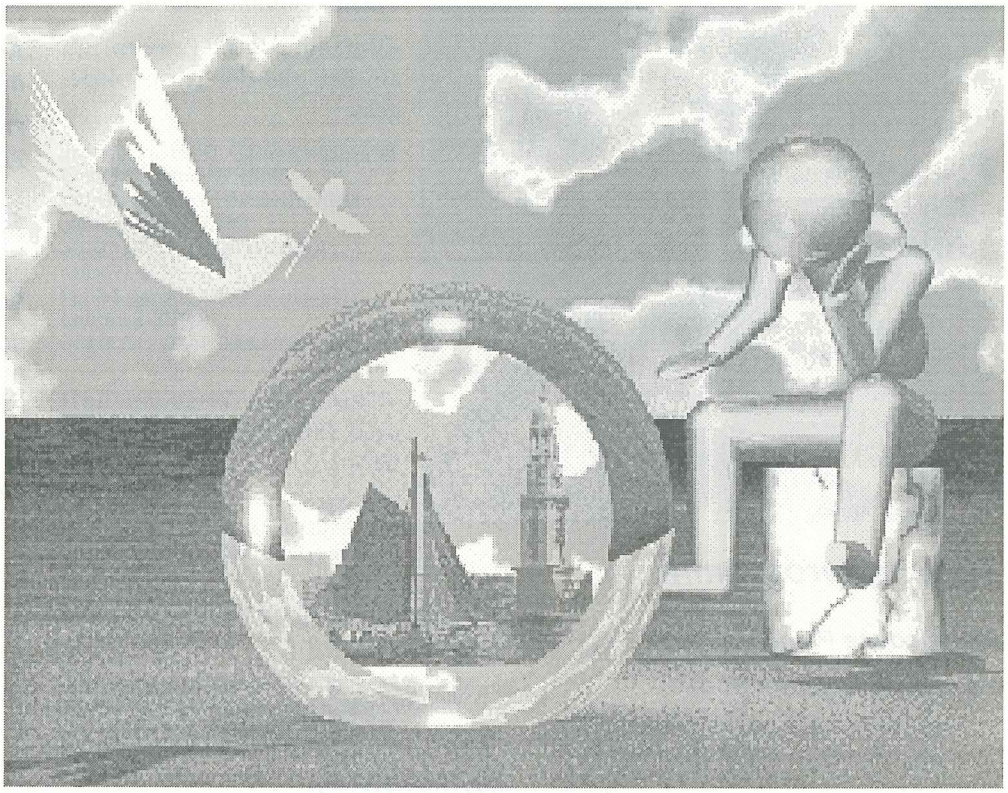
Weitere Informationen sind beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein erhältlich.

Unabhängiges Landeszentrum fuer Datenschutz Schleswig-Holstein, Duesternbrooker Weg 82, D-24105 Kiel
E-Mail: mail@datenschutzzentrum.de
Tel: 0431-98812-00 Fax: -23
Homepage: http://www.datenschutzzentrum.de

16. FIfF– Jahrestagung

Prognosemodelle: Szenarien für die Zukunft
Informatik, Naturwissenschaften und Friedensforschung im Dialog
Hamburg, 29. September bis 2. Oktober 2000

Veranstaltet von:
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
Fachbereich Informatik der Universität Hamburg
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH)



Die diesjährige Tagung wendet sich an engagierte Wissenschaftlerinnen und Wissenschaftler aus der Informatik, den Naturwissenschaften und der Friedensforschung, die sich in interdisziplinärer Zusammenarbeit mit Modellbildung, Simulation und Prognosen für zentrale Fragen aus Umwelt und Friedensforschung auseinandersetzen.

In eingeladenen Übersichtsvorträgen, Podiumsdiskussionen und Arbeitsgruppen wird thematisiert werden, wie der Stand der Forschung zu Prognosemodellen in den einzelnen Disziplinen ist und wie mit den typischen Problemen der Modellbildung, Validierung und Übertragung der Ergebnisse in die Anwendungsdomänen umgegangen wird. Insbesondere sind Expertinnen und Experten eingeladen worden, die im Rahmen der Politikberatung zwischen Fachexperten und Entscheidungsträgern vermitteln.

Programmkomitee

Vorsitz

Prof. Dr. Leonie Dreschler-Fischer, Universität Hamburg, Fachbereich Informatik;
Prof. Dr. Dr. Dieter S. Lutz, IFSH

Weitere Mitglieder

Dr. Stephan Albrecht
Prof. Dr. Jan Backhaus
Werner Hülsmann
Dr. Götz Neuneck
Prof. Dr. Bernd Page
Prof. Dr. Hartwig Spitzer

Kontaktadresse

Prof. Dr. Leonie Dreschler-Fischer
Universität Hamburg
Fachbereich Informatik
FIfF-Jahrestagung 2000
Vogt-Kölln-Str. 30
22527 Hamburg
Telefon:+49 40 428 83-2402
Telefax: +49 40 428 83-2206
email:
FIfF2000@informatik.uni-hamburg.de
http://kogs-www.informatik.uni-hamburg.de/~dreschle/fiff2000/home.html

Tagungskonto

Heike Tewes
Norisbank
BLZ: 760 260 00
Kto-Nr.: 4058 309 015

Teilnahmegebühren:

Für StudentInnen: DM 36,-
für Berufstätige: DM 140,-

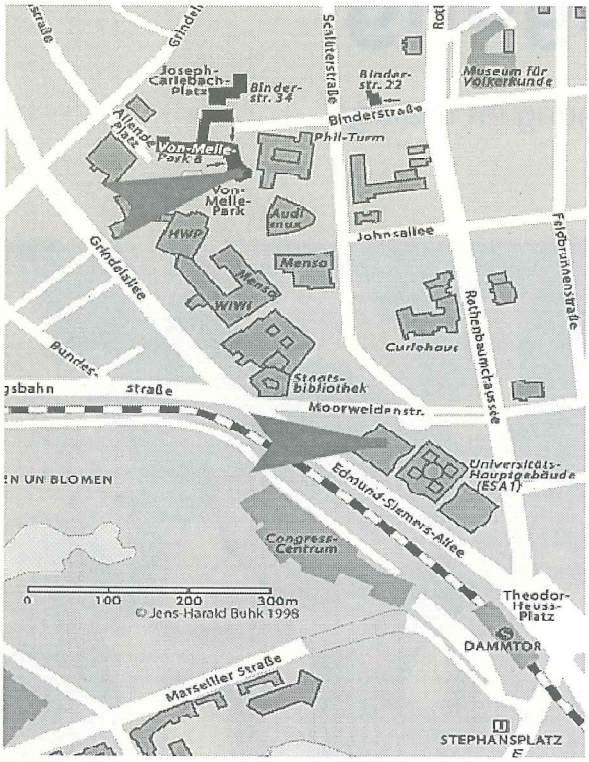
Tagungsort

Die Tagung findet auf dem Campus der Universität Hamburg statt, Übersichtsvorträge und Podiumsdiskussionen im Hörsaal des Fachbereichs Erziehungswissenschaft im Von-Melle-Park 8, die Arbeitsgruppen und die Mitgliederversammlung im Flügel West des Hauptgebäudes in der Edmund-Siemers-Allee 1.

Die Tagungsstätte liegt verkehrsgünstig in der Nähe des Intercity-Bahnhofes Hamburg-Dammtor.

Bei der **Zimmersuche** hilft Ihnen die
Tourismus-Zentrale Hamburg GmbH
Steinstraße 7
20095 Hamburg
Internet:
http://www.hamburg-tourism.de
email: info@hamburg-tourism.de
Telefax: +49 40 300 51 220
Telefon:+49 40 300 51 – 0

Lageplan



Tagungsprogramm

Eingeladene Plenarvorträge

»Wasser als Konfliktursache«

Prof. Dr. Jan Backhaus, Universität Hamburg, Institut für Meereskunde

»Sozioökonomische Prognosemodelle: Stand der Forschung und Perspektiven«

Dr. Marian Leimbach, Potsdam-Institut für Klimafolgenforschung

»Modelle kooperativer Sicherheit«

Dr. Hans-Joachim Gießmann, IFSH

»Modellbildung und Simulation – Grundlage für Entscheidungen im Umweltbereich«

Prof. Dr. Rolf Grützner, Universität Rostock, Fachbereich Informatik

»Nachhaltigkeit in der Informationsgesellschaft«

Prof. Dr. Lorenz M. Hilty, Hochschule für Wirtschaft, Olten (Schweiz)

»Modellierung und Prognose klimatischer Phänomene«

Dr. Mojib Latif, Max-Planck-Institut für Meteorologie, Hamburg

»Prognosemodelle in der Friedensforschung«

Dr. Götz Neuneck, IFSH

»Stand der Prognoseverfahren«

Dr. Christian Reick, Universität Hamburg,Fachbereich Informatik

Podiumsdiskussionen

»Versagen von Prävention am Beispiel des Kosovokrieges«

Brigadegeneral a.D. Dr. Heinz Loquai; Willy Wimmer, MdB und Stellvertretender Vorsitzender der OSZE-Versammlung; Johannes Dieterich, Journalist, »Die Woche«
Moderation: Dr. Wolfgang Zellner (OSZE-Zentrum)
Samstag, 30.09.2000, 16.00 – 17.30 Uhr

»Gefährden Wissenschaft und Technik die Demokratie?«

Moderation:
Prof. Dr. Dr. Dieter S. Lutz, IFSH
Montag, 2.10.2000, 10.00 – 12.00 Uhr

»Prognosemodelle: Szenarien für die Zukunft"

Moderation: Prof. Dr. Leonie Dreschler-Fischer, Universität Hamburg, Fachbereich Informatik
Montag, 2.10.2000, 13.00 – 15.00 Uhr

Workshops

Sonntag, den 01.10.2000

AG 1 »Cyberterrorismus und Information Warfare«

Ute Bernhardt, FIfF; Dr. Götz Neuneck, IFSH; Ingo Ruhmann, FIfF

AG 2 »Umweltinformatik«

Prof. Dr. Lorenz Hilty, Hochschule für Wirtschaft, Olten (Schweiz); Prof. Dr. Bernd Page, Universität Hamburg, Fachbereich Informatik; Dr. Christian Reick, Universität Hamburg, Fachbereich Informatik

AG 3 »Fernerkundungsverfahren zur Verifikation von Abrüstungs- und Umweltvereinbarungen«

Prof. Dr. Leonie Dreschler-Fischer, Universität Hamburg, Fachbereich Informatik

AG 4 »Frauenstudien«

Prof. Dr. Britta Schinzel, Universität Freiburg, Institut für Informatik und Gesellschaft

AG 5 »Informatik im Informationszeitalter«

Prof. Dr. Arno Rolf, Universität Hamburg, Fachbereich Informatik

AG 6 »Sicherheit und Datenschutz im eCommerce«

Dipl.-Math. Ulrich Moser, SYSTOR AG, Zürich

Rahmenprogramm

Empfang

im Rathaus durch die Zweite Bürgermeisterin und Wissenschaftssenatorin Frau Krista Sager
Freitag, den 29.9.2000, 17.00 – 18.00 Uhr

Conference-Dinner

auf dem Historischen Dreimaster »Rickmer-Rickmers« mit einem Vortrag von Prof. Dr. Klaus Brunnstein, Universität Hamburg, mit dem Titel »Viren, Würmer und andere Viechereien im Internet: Über die Schattenseiten der Schönen Neuen Informationsgesellschaft«

Samstag, den 30.9.2000, 20 - 23 Uhr

FIfF-Mitgliederversammlung

Sonntag, den 1.10.2000, 16 - 18 Uhr
Ort: Hörsaal im Flügel West des Hauptgebäudes, Edmund-Siemers-Allee 1

Poster-Ausstellung zu den Workshops

Sonntag, den 1.10.2000 Beginn der Tagung

Freitag, 29.09.2000, 13.00 Uhr

Ende der Tagung

Montag, 2.10.2000, 15.00 Uhr

Adressen

Aachen

Prof.Dr.Dietrich Meyer-Ebrecht
Lehrstuhl für Meßtechnik
RWTH Aachen
52056 Aachen
Tel.: (0241) 80 78 60
Fax: (0241) 88 88 200
Mail@LfM.RWTH-Aachen.De

Berlin

TU Berlin
Irina Piens
Schmidtstraße 3
10179 Berlin
piens@prz.tu-berlin.de

FU Berlin
Lukas Faulstich
Mehringdamm 119
10965 Berlin
Tel.: (030) 69 50 92 24

Bonn

Ingo Ruhmann
Rittershausstrasse 11
53113 Bonn
ingo@ruhmann.ki.shuttle.de

Braunschweig

TU Braunschweig
Fachschaft Informatik
AStA-Fach
Katharinenstraße 1
38106 Braunschweig

Bielefeld

c/o Angewandte Informatik
Technische Fakultät
Universität Bielefeld
Postfach 100 131
33502 Bielefeld
fiff-bi@TechFak.Uni-Bielefeld.DE

Bremen

Prof. Dr. Hans-Jörg Kreowski
Uni Bremen
FB Informatik/Mathematik
Postfach 330 440
28334 Bremen
Tel.: (0421) 218-2956
fiff@informatik.uni-bremen.de

Darmstadt

Jens Woinowski
Rhoenring 141
64289 Darmstadt
Tel.: (06151) 16 61 82 (d)
(06151) 71 81 50 (p)
woinowsk@iti.informatik.tu-darmstadt.de

Erlangen/Fürth/Nürnberg

Klaus Thielking-Riechert
Sommerstraße 10
90762 Fürth
k.thielking@link-n.cl.sub.de

Freiburg

Uwe Jendricke
Bernhardstrasse 1B
79098 Freiburg
Tel. & Fax: 0761/25665
jendricke@telematik.iig.uni-freiburg.de

Frankfurt

Ingo Fischer
Dahlmannstraße 31
60385 Frankfurt am Main

Hamburg

Simone Pribbenow
Hein-Köllisch-Platz 5
20359 Hamburg
Tel.: (040) 54715-366
pribbeno@informatik.uni-hamburg.de

Hannover

Bernhard Pfitzner
Rosenbergstraße 14a
30163 Hannover

Heilbronn

Michael Müller
FH Heilbronn, FB
Max-Planck-Straße 39
74081 Heilbronn
Tel.: (07131) 50 43 64
michael.mueller@fh-heilbronn.de

Jena

Prof. Dr. Eberhard Zehendner
Institut für Informatik
Friedrich-Schiller-Universitaet
07740 Jena
Tel: (03641) 946385
Fax: (03641) 946372
zehendner@acm.org

Kaiserslautern

Frank Leidermann
Institut für Technol. und Arbeit
Universität Kaiserslautern
Gottlieb-Daimler-Str.
67663 Kaiserslautern
Tel. 0631/205-3742
fleider@sozwi.uni-kl.de

Karlsruhe

Thomas Freytag
Institut AIFB
Universität Karlsruhe
76128 Karlsruhe
Tel.: (0721) 6084063 (d)
(0721) 815416 (p)
tfr@aifb.uni-karlsruhe.de

Kiel

Hans-Otto Kühl
Alte Kieler Landstraße 118
24768 Rendsburg
Tel.: (04331) 201-2187

Koblenz

Dr. Michael Möhring
Uni Koblenz-Landau
FB Informatik
Rheinau 3–4
56075 Koblenz
Tel.: (0261) 9119477
Fax: (0261) 37524
moeh@infko.uni-koblenz.de

Köln

Manfred Keul
Landsbergstraße 16
50678 Köln
Tel.: (0221) 317911
100031.12@compuserv.com

Konstanz

Volker Schuchhardt
Jungerhalde 78
78464 Konstanz
Tel: (07531) 874098 (d)
(07531) 34921 (p)
volker.schuchhardt@cgk.siemens.de

Lahn-Dill

Fiff-Regionalgruppe Lahn-Dill
c/o Markus Thielmann
Fritz-Philippi-Straße 7
35767 Breitscheid
Tel.: (02777) 912 520
mail@thielmann-group.de

München

Bernd Rendenbach
Leerbichlallee 19
82031 Grünwald
Tel.: (089) 6410547

Münster

Werner Ahrens
Franz-Daspestr. 36
48231 Warendorf

Oldenburg

Universität Oldenburg
Fachschaft Informatik
Ammerländer Heerstraße
26129 Oldenburg
Fachschaft.Informatik@informatik.uni-oldenburg.de

Paderborn

Harald Selke
Heinz Nixdorf Institut
U-GH Paderborn
Fürstenallee 11
33102 Paderborn
Tel.: (05251) 606518
hase@uni-paderborn.de

Stuttgart

Kurt Jaeger
Schozacher Straße 40
70437 Stuttgart
Tel.: (0711) 8701309
(0711) 90074-23
Fax: (0711) 7289041
pi@lf.net

Tübingen

Jochen Krämer
Sand 13
72076 Tübingen
Tel.: (07071) 29-5957
fiff@informatik.uni-tuebingen.de

Ulm

Universität Ulm
Fachschaft Informatik
Bernhard C. Witt
Oberer Eselsberg
89081 Ulm
wittbe@pcpool1.informatik.uni-ulm.de

FIfF

Geschäftsstelle

FIfF e.V.
Medemstade 64
21775 Ihlienworth

Tel.: (04755) 911 154
Fax: (04755) 911 026

E-Mail:fiff@fiff.de

Dienstags 10 bis 16 Uhr,
Donnerstags 10 bis 16 Uhr

Volksbank Stade-Cuxhaven
Kontoverbindung: 3641383600
BLZ 241 910 15

Überregionale Arbeitskreise des FIfF

AK »RUIN« (Rüstung und Informatik)

Ingo Ruhmann
Rittershausstraße 11
53113 Bonn
ingo.ruhmann@acm.org

AK »FIfF in Europa«

Dagmar Boedicker
Daiserstraße 45
81371 München
Tel.: (089) 7256547

FIfF im Netz

Das ganze FIfF

http://www.fiff.de

Mailing-Liste

Beiträge an:
fiff-l@fiff.de
An- und Abbestellungen an:
fiff-l-request@fiff.de

Regionalgruppen

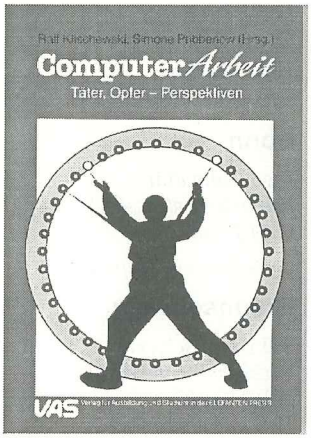
Bremen:
http://fiff.informatik.uni-bremen.de
Konstanz::
http://www.puk.de/fiff-kn
München:
http://hyperg.uni-paderborn.de/fiff/regional/muenchen

F.I.f.F.

Ute Bernhardt, Ingo Ruhmann (Hrsg.): Ein sauberer Tod: Informatik und Krieg.

Informations- und Kommunikationstechnik – seit ihren Anfängen politisch geformt · Computer auf dem Schlachtfeld · Dual-Use: zivil geforscht – militärisch genutzt? · »Wehrtechnik und Landesverteidigung« – Zur Forschung in der Bundesrepublik · Weiter so oder umsteuern? · u.v.a.

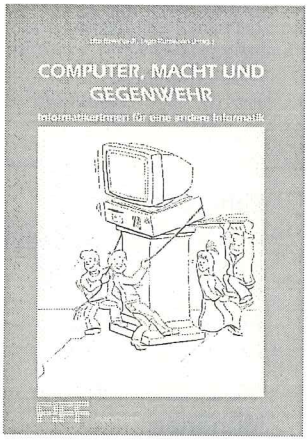
320 Seiten, Marburg 1991, 20,– DM



Ralf Klischewski, Simone Pribbenow (Hrsg.): ComputerArbeit. Täter, Opfer – Perspektiven

Das demokratische Potential der Neuen Fabrik · Maschinelle Intelligenz – Industrielle Arbeit · Arbeitnehmer und Betriebsräte zur Informatik im Betrieb.

190 Seiten, Berlin 1989, 19,80 DM



Ute Bernhardt, Ingo Ruhmann (Hrsg.): Computer, Macht und Gegenwehr – InformatikerInnen für eine andere Informatik

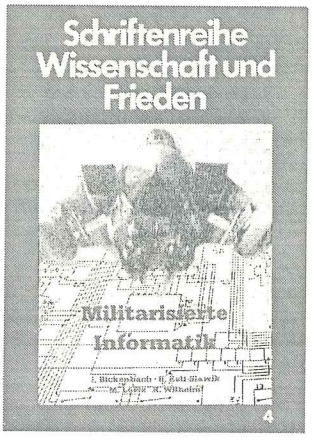
Protected Mode · Computersicherheit: militärisch oder zivil · Computer und Umwelt · Technologiepolitik und Technikfolgenforschung · Partizipative Entwicklung von Systemen ·
EU: Grundrechte als Handelshemmnisse? · u.v.a.

216 Seiten, Bonn 1991, 12,80 DM

Jutta Schaaf (Hrsg.): Die Würde des Menschen ist unverNETZbar.

Netzknoten Frankfurt · Automatisierung des Zahlungsverkehrs · Rüstungshaushalt und Informationstechnik · Verfassungsverträglichkeit als Kriterium der Technikbewertung · Ethik und Technik · Theorie der Informatik · u.v.a.

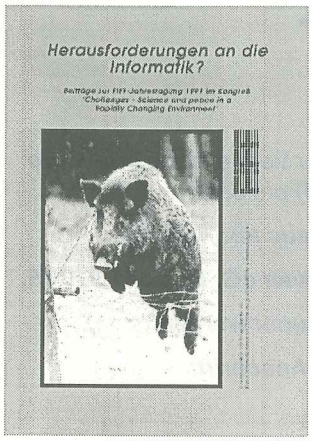
300 Seiten, Bonn 1990, 12,80 DM



J. Bickenbach et. al. (Hrsg.): Militarisierte Informatik

Erschienen in der Schriftenreihe Wissenschaft und Frieden, Nr. 4, 1985. Dieses Buch war vergriffen, doch sind einige Restexemplare aufgetaucht, die jetzt über das FIfF-Büro zum Preis von 10,– DM erhältlich sind.

Bibliothek



Rudolf Kitzing, Ursula Linder-Kostka, Fritz Obermaier (Hrsg.): Schöne neue Computerwelt – Zur gesellschaftlichen Verantwortung der Informatiker

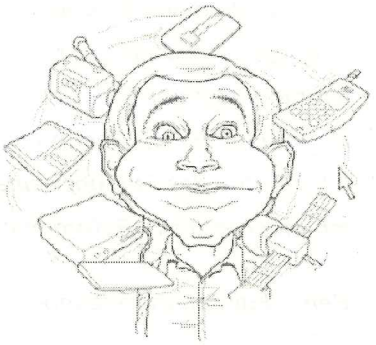
Beherrschbarkeit von Systemen, ihre Verletzlichkeit und die Verantwortung von Informatikern · Neue Wege in der Informatik · Psychosoziale Folgen des Computereinsatzes

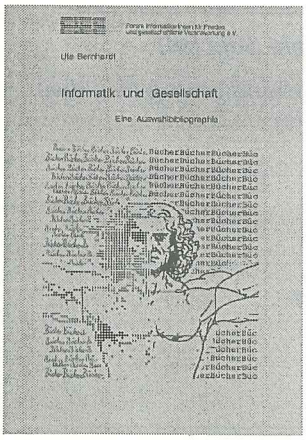
256 Seiten, Berlin 1988, 19,80 DM

Heiko Dörr (Hrsg.): Herausforderungen an die Informatik? – Science in a Rapidly Changing Environment

Wissenschaft und Ethik · Computergestützte und Elektronische Kriegsführung · Curricula und Forschungs- & Entwicklungs-Ansätze in der Informatik – den Anforderungen des 21. Jahrhunderts gerecht werden · Computertechnologie – ein angemessenes Mittel gegen die Armut der 3. Welt? · (Kredit-)Kartenzahlung im Licht von Daten- und Verbraucherschutz · Vernetzung von Friedensgruppen · Texte in englisch und deutsch

126 Seiten, Bonn 1992, 12,80 DM





Peter Bittner, Jens Woinowski (Hrsg.): Mensch – Informatisierung – Gesellschaft

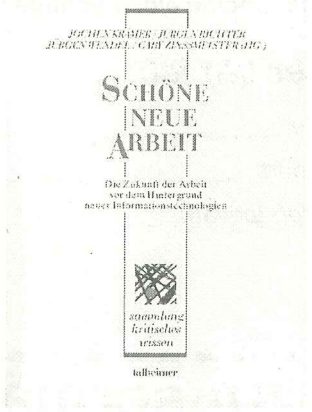
Kritische Informatik, Band 1, Beiträge zur 14. Jahrestagung des FIfF 1998 in Darmstadt unter dem Motto: „Mensch sein in einer informatisierten Gesellschaft", 188 Seiten,

Münster: Lit-Verlag, 1999, Preis: 39,90 DM

Ute Bernhardt: Informatik und Gesellschaft. Eine Auswahlbibliographie

Ein thematisch gegliederter Einstieg in die Literatur zu Informatik und Gesellschaft

26 Seiten, Bonn 1990, 3,– DM



Jochen Krämer et. al. (Hrsg.): »Schöne Neue Arbeit«

Die Zukunft der Arbeit vor dem Hintergrund neuer Informationstechnologien. Der Tagungsband zur 12. Jahrestagung des FIfF in Tübingen 1996

Talheimer, 1997, 44,– DM

Hans-Jörg Kreowski et al.: Realität und Utopien der Informatik

Aus dem Vorwort: »Realität und Utopien der Informatik werden im vorliegenden Sammelband aus unterschiedlichen Sichten dargestellt, um die aktuelle Diskussion im Spannungsverhältnis von Informatik und Gesellschaft zu unterstützen und voranzubringen. Zusammengestellt sind ausgewählte Beiträge der 10. Jahrestagung des „Forums Informatikerinnen und Informatiker für Frieden und gesellschaftliche Verantwortung" (FIFF), die vom 7. bis 9. Oktober 1994 in Bremen unter dem Motto „1984 plus 10 – Realität und Utopien der Informatik" stattfand.«

Münster: agenda Verlag, 1995, 28,- DM

Alle Bücher sind erhältlich über: FIfF-Geschäftsstelle, Medemstade 64, 21775 Ihlienworth

Vielzweck-Schnipsel

Kopieren, ausfüllen und einsenden an: FIFF e.V. Medemstade 64 21775 Ihlienworth

FIfF

Das möchte ich:

- ❒ **Ich möchte ❒ aktives / ❒ förderndes Mitglied des FIfF werden** *(Mindestjahresbeitrag ist für Verdienende* **60,– Euro (117,35 DM)** *für Studierende und Menschen in vergleichbarer Situation* **15,– Euro (29,34 DM)** *pro Jahr.*
- ❒ **Ich möchte die FIfF-Kommunikation zum Preis von 20,– Euro (39,15 DM) jährlich frei Haus abonnieren.**
- ❒ **Ich überweise den Beitrag auf das Konto 36 413 836 00 bei der Volksbank Stade-Cuxhaven eG, BLZ 241 910 15.**
- ❒ **Der Mitglieds- bzw. Abobeitrag soll per Lastschriftverfahren von meinem Konto abgebucht werden** *(s. u.).*
- ❒ **Ich möchte meine neue/korrigierte Anschrift mitteilen** *(siehe unten).* **Meine alte/falsche Anschrift:**

  Straße: _____ *Wohnort:* _____
- ❒ **Ich möchte dem FIfF etwas spenden:**
- ❒ *Verrechnungsscheck über* _____ *EUR liegt bei* ❒ *Spendenquittung am Ende des Kalenderjahres erbeten*
- ❒ **Ich möchte mehr über das FIfF wissen, bitte schickt mir:** _____
- ❒ **Ich möchte gegen Rechnung, zuzüglich Portokosten, bestellen:** _____
- ❒ **Ich möchte das FIfF über einen Artikel/ein Buch informieren: ❒ Zitat** *(siehe unten)* **❒ Kopie** *(liegt bei)*
- ❒ **Ich möchte zur FIfF-Kommunikation beitragen mit:** ❒ **einem Manuskript zur Veröffentlichung** *(liegt bei)* ❒ **einer Anregung** *(siehe unten)*

  Bemerkungen/Ergänzungen: _____

  _____

  _____
- ❒ **Ich möchte einen richtigen Brief schreiben. Der Vielzweck-Schnipsel ist nichts für mich.**

Die/der bin ich:

Name: _____ *Straße:* _____

Wohnort: _____ *ggf. Mitgliedsnummer:* _____

Telefon (privat): _____ *(Arbeit):* _____ *E-Mail:* _____

Einzugsermächtigung

Hiermit ermächtige ich das FIfF e.V. widerruflich, meinen Mitgliedsbeitrag durch Lastschrift einzuziehen. Wenn das Konto keine Deckung aufweist, besteht keine Verpflichtung des Geldinstituts, die Lastschrift auszuführen.

Name: _____ *Jahresbeitrag:* _____ *EUR, erstmals* _____

Konto-Nr.: _____ *BLZ:* _____ *Geldinstitut:* _____

Straße: _____ *Wohnort:* _____

Datum: _____ *Unterschrift:* _____

(Wir werden Ihre Daten nach §28 BDSG nur für eigene Zwecke verarbeiten und keinem Dritten zugänglich machen.)

Was will das FIfF?

Im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. haben sich InformatikerInnen zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen ihres Fachgebiets verantwortlich fühlen und entsprechende Arbeit leisten wollen:

- *Kritik üben, denn wir haben das Know-how dazu*
- *uns für eine Abrüstung der Informatik engagieren*
- *uns am Diskurs über Technik und Wissenschaft beteiligen*
- *die Öffentlichkeit warnen, wenn wir Entwicklungen in unserem Fachgebiet für schädlich halten*
- *möglichen Gefahren eigene Vorstellungen entgegensetzen*
- *die Informations- und Kommunikationstechnik nicht gegen, sondern für den Menschen gestalten*
- *uns für eine zivile und gerechte Welt einsetzen; eine Welt, in der die Grundrechte aller Menschen gewahrt werden, eine Welt, die menschenwürdig ist*
- *last not least nicht alles machen, was machbar ist*

Geplante Themenschwerpunkte

für die FIfF-Kommunikation

4/2000 »Arbeit und Neue Medien«

zuständig: *Dagmar Boedicker und Ute Bernhardt*

1/2001 »Bildung und Computer«

zuständig: *Dirk Siefkes, Britta Schinzel und Johannes Busse*

2/2001 »Arbeitnehmerdatenschutz«

zuständig: *Werner Hülsmann und Dagmar Boedicker*

Die FIfF-Kommunikation bittet um Beiträge!

Die FIFF-Kommunikation lebt von der aktiven Mitarbeit ihrer LeserInnen! Interessante Artikel sowie Fotos und Zeichnungen zur Illustration (mit Quellengaben) sind immer herzlich willkommen. Die Bearbeitung wird erleichtert, wenn Beiträge elektronisch und zusätzlich auf Papier der Redaktion zugehen. Die Redaktion behält sich Kürzungen und Titeländerungen vor.

Impressum

Die FIfF-Kommunikation ist das Mitteilungsblatt des »Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.« (FIfF). Die Beiträge sollen die Diskussion unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige AutorInnen-Meinung wieder. Nachdruck genehmigung wird nach Rücksprache mit der Redaktion in der Regel gerne erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Heftpreis: 5 EUR. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 20 EUR/Jahr (inkl. Versand) abonnieren.

Erscheinungsweise: einmal vierteljährlich

Erscheinungsort: Medemstade

Auflage: 2000

Herausgeber: Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)

Verlagsadresse: FIfF-Geschäftsstelle, Medemstade 64, 21775 Ihlienworth, Tel. (04755) 911 154

ISSN: 0938–3476

Druck: Druckpartner Hemmoor

Layout: Frank Meiners

Titelfoto: Corbis Collection

Redaktionsadresse: FIfF-Kommunikation, Medemstade 64, 21775 Ihlienworth, Tel. (04755) 911 154, Fax (04755) 911 026 E-Mail: fiffko@uni-paderborn.de

FIfF-Überall: In dieser Rubrik der FIfF-Kommunikation ist jederzeit Platz für Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an: hubert@cs.tu-berlin.de

Lesen, Schluß-PFIFF: Beiträge für diese Rubriken bitte per Post an Claus Stark (Heilbronn) oder per E-Mail an: stark@secorvo.de

Redaktionsschluß für die Ausgabe 4/2000: 15. 10. 2000

Redaktions-Team FIfF-Kommunikation 3/2000:
Ute Bernhardt, Markus Hoff-Holtmanns (verantwortlich), Frank Meiners

Hinweis: Postvertriebsstücke wie die FIfF-Kommunikation werden von der Post auch auf Antrag nicht nachgesandt; daher bitten wir alle Mitglieder und Abonnenten, dem FIfF-Büro jede ***Adreßänderung*** rechtzeitig bekanntzugeben!

»THE WORLD WAS FULL OF BAD SECURITY SYSTEMS DESIGNED BY PEOPLE WHO READ APPLIED CRYPTOGRAPHY«

oder: Über den Kontext der Kryptographie

Vorwort aus Secrets and Lies von Bruce Schneier, IT-Security-Experte

I have written this book partly to correct a mistake.

Seven years ago I wrote another book: Applied Cryptography. In it I described a mathematical utopia: algorithms that would keep your deepest secrets safe for millennia, protocols that could perform the most fantastical electronic interactions – unregulated gambling, undetectable authentication, anonymous cash – safely and securely. In my vision cryptography was the great technological equalizer; anyone with a cheap (and getting cheaper every year) computer could have the same security as the largest government. In the second edition of the same book, written two years later, I went so far as to write: »It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics.«

It's just not true. Cryptography can't do any of that.

It's not that cryptography has gotten weaker since 1994, or that the things I described in that book are no longer true; it's that cryptography doesn't exist in a vacuum.

Cryptography is a branch of mathematics. And like all mathematics, it involves numbers, equations, and logic. Security, palpable security that you or I might find useful in our lives, involves people: things people know, relationships between people, people and how they relate to machines. Digital security involves computers: complex, unstable, buggy computers.

Mathematics is perfect; reality is subjective. Mathematics is defined; computers are ornery. Mathematics is logical; people are erratic, capricious, and barely comprehensible.

The error of Applied Cryptography is that I didn't talk at all about the context. I talked about cryptography as if it were The Answer™. I was pretty naïve.

The result wasn't pretty. Readers believed that cryptography was a kind of magic security dust that they could sprinkle over their software and make it secure. That they could invoke magic spells like »128-bit key« and »public-key infrastructure«. A colleague once told me that the world was full of bad security systems designed by people who read Applied Cryptography.

Since writing the book, I have made a living as a cryptography consultant: designing and analyzing security systems. To my initial surprise, I found that the weak points had nothing to do with the mathematics. They were in the hardware, the software, the networks, and the people. Beautiful pieces of mathematics were made irrelevant through bad programming, a lousy operating system, or someone's bad password choice. I learned to look beyond the cryptography, at the entire system, to find weaknesses. I started repeating a couple of sentiments you'll find throughout this book: »Security is a chain; it's only as secure as the weakest link.« »Security is a process, not a product.«

Any real-world system is a complicated series of interconnections. Security must permeate the system: its components and connections. And in this book I argue that modern systems have so many components and connections – some of them not even known by the systems' designers, implementers, or users – that insecurities always remain. No system is perfect; no technology is The Answer™.

This is obvious to anyone involved in real-world security. In the real world, security involves processes. It involves preventative technologies, but also detection and reaction processes, and an entire forensics system to hunt down and prosecute the guilty. Security is not a product; it itself is a process. And if we're ever going to make our digital systems secure, we're going to have to start building processes.

A few years ago I heard a quotation, and I am going to modify it here: If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

This book is about those security problems, the limitations of technology, and the solutions.

Vorwort aus Schneier, B. (2000): Secrets and Lies – Digital Securities in a Networked World, Wiley&Sons mit freundlicher Abruckgenehmigung.

Mehr Informationen zum Autor und zum Buch im Internet unter: http://www.counterpane.com