E.f.F.Kommunikation
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. 14. Jahrgang 1997 • Einzelpreis: 6 DM

Z 7625 F

3/97
September 1997

SICHERUNGSINFRASTRUKTUREN

ISSN 0938-3476

Inhalt

Editorial

Schwerpunkt »Sicherungsinfrastrukturen«

FIFF e.V.

Rubriken

Vertrauen ist gut, Kontrolle ist besser ?

Das Thema „Sicherungsinfrastrukturen" (SIS) ist durch die kürzliche Verabschiedung des Signaturgesetzes (SigG) und der Signaturverordnung (SigV) sehr massiv in den Blickpunkt des allgemeinen Interesses gerückt worden! Dieses Gesetz stellt die ersten Weichen für bundesdeutsche Sicherungsinfrastrukturen – damit ziehen Zertifikate, elektronische Signaturen und TrustCenter endgültig in unseren Alltag ein. Aber wozu benötigen wir diese Sicherungsmaßnahmen? Ist es nicht ein „Kuckucksei", das uns da ins Nest gelegt wird? Werden da nicht Trust Center – die vertrauenswürdigen Dritten – zum idealen „Center of Control" ausgebaut frei nach dem Motto „Vertrauen ist gut, ..."? Bedeutet dieses von außen verordnete „Ver"-trauen nicht eher „Miß"-trauen – soll durch die geplanten technischen und organisatorischen Strukturen die Kontrolle über alle Kommunikationsbeziehungen endgültig zementiert werden? Der Geier auf dem Bild visualisiert diese Vorstellung sehr eindringlich – Viele Institutionen (Das muß nicht immer der Staat sein!) streben die Schlüsselgewalt in der Informationsgesellschaft an.

Soviel Pessimismus ist aber zum Glück nicht angebracht! Wir wollen etwas Licht in dieses Dickicht bringen und so die gesellschaftliche Diskussion um dieses aktuelle Thema anregen. Die sozialverträgliche Gestaltung dieser neuen Infrastrukturen ist möglich! Wir müssen uns nur aktiv in die Diskussion und die Gestaltungsprozesse einmischen – das FIFF ist hier gefordert!

Dieses Heft möchte den Rahmen um das Thema „Sicherungsinfrastrukturen" sehr weit fassen, um dieses neue Phänomen auch für Nicht-Informatiker verständlich zu machen. Wir wollen uns diesem Thema aus philosophischer, soziologischer, praktischer, grundsätzlicher, juristischer – ja, und auch technischer Sicht nähern und so verschiedene Zugänge anbieten. Der Aufbau von Sicherungsinfrastrukturen kann als gewaltige gesellschaftliche Aufgabe angesehen werden (viele sprechen von einem neuen Infrastruktur-„Saurier"), an der sich viele Menschen, viele Disziplinen konstruktiv beteiligen müssen.

Wir haben die in diesem Heft gesammelten Beiträge in fünf Themenkreise gefaßt, die einen roten Faden durch das Heft legen – so sollte jeder seinen adäquaten Einstiegspunkt in das Thema finden.

Im ersten Themenkreis dieses Heftes geht es um die **Einführung in die Konzepte der „Sicherung und Sicherheit in der Informationsgesellschaft"**. Fox gibt einen allgemeinen Überblick darüber, was sich hinter dem abstrakten Begriff „Sicherungsinfrastruktur" überhaupt verbirgt und stellt einzelne Komponenten vor. Kelm erläutert dann konkret den Aufbau eines zentralen Elementes einer SIS, nämlich eine „Policy Certification Authority" (PCA), im Detail.

Im zweiten Themenkreis werden **philosophische und soziologische Aspekte der Sicherungsinfrastrukturen** diskutiert: Bittner und Woinowski nähern sich den Begriffen „Vertrauen" und „Mißtrauen", um sie zur technischen Sicherung in Beziehung zu setzen. Banse und Friedrich begreifen die Digitale Signatur nicht ausschließlich technisch und arbeiten ihre kulturellen Aspekte heraus. Hillebrand und Büllingen stellen ihre Ergebnisse einer Umfrage unter Klein- und Mittelbetrieben dar, wie diese es mit der IT-Sicherheit halten – können SIS helfen, hier die schlechte Lage zu verbessern?

Schefe schließlich beschäftigt sich in seinem Aufsatz allgemeiner mit (Un-)Sicherheiten im Software-Engineering.

Im dritten Themenkreis beschäftigen sich die AutorInnen mit der **Praxis der Sicherungsinfrastrukturen:** Wohlmacher und Pharow stellen am Beispiel ihres Projektes zur Health Professional Card in Magdeburg den Aufbau berufsspezifischer Sicherungsstrukturen (hier: im Gesundheitswesen) dar – die Übertragung in andere Berufszweige sollte nicht schwerfallen. Rannenberg und Müller diskutieren das Konzept der mehrseitigen Sicherheit des Freiburger Kollegs „Sicherheit in der Kommunikationstechnik". Aus der Sicht eines Systemadministrators stellt Rohrer seine Anforderungen an Sicherungsinfrastruktur in Form eines Rundgangs durch sein Rechenzentrum sehr plastisch dar. Stark diskutiert die Rolle der Evaluation bei der Entwicklung von Sicherungstechnologien – wieviel Vertrauen verdient Sicherheit überhaupt? Hühnlein schließlich führt vor, daß SIS im Endeffekt auch programmiert werden muß – er vergleicht verschiedene Ansätze der praktischen Umsetzung.

Der vierte Themenkreis ist der **Politik** gewidmet: Winkel betrachtet die deutsche Kryptokontroverse im Detail und arbeitet zu drei prinzipiellen Optionen (Kryptoverbot, Kryptofreigabe, Treuhandmodell für Schlüssel) Szenarien heraus. Hedberg skizziert dann HPs Konzept des „International Cryptography Framework", das viele große Unternehmen wie Microsoft und Gemplus unterstützen – und diskutiert die kontroverse gesellschaftliche Diskussion dazu in den USA.

Der fünfte Themenkreis ist der **Ausbildung in IT-Sicherheit** gewidmet: Fischer-Hübner analysiert die europäische Hochschullandschaft aus dem Security-Blickwinkel und stellt einige Curricula konkret vor.

In der **Leseecke** findet sich (wie immer!) wichtige, interessante und auch amüsante Literatur zum Titelthema, einige **Tagungshinweise** ergänzen das Serviceangebot. Im **SchlußpFIFF** schließlich stellt ein „Madam & Eve"-Cartoon das Problem ungesicherter Datenhighways sehr drastisch dar – in Südafrika scheint man nicht mal mehr auf dem Datenhighway vor Highjacker sicher zu sein!

Wir hoffen, daß wir mit diesem Heft die gesellschaftliche Diskussion um die sozialorientierte Gestaltung von Sicherungsinfrastrukturen anregen konnten – und freuen uns nun sehr auf Ihren Leserbrief!

Kathrin Schier, Universität Hamburg,
Fachbereich Informatik
Claus Stark, TÜViT GmbH Essen,
Bereich Informationssicherheit

...Recht auf informationelle Selbstbestimmung sichern...

...die Öffentlichkeit informieren...

...gemeinsam handeln...

Die Rolle kritischer ExpertInnen in der Informationsgesellschaft

...Technik sozial gestalten...

...freien Zugang sichern...

14. - 16. November 1997
13. FIFF-Jahrestagung
Paderborn

FIfF

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Carmen Buschmeyer
Sekretariat: Informatik und Gesellschaft
Universität Gesamthochschule Paderborn
Fürstenallee 11
33102 Paderborn
Telefon: 05251/60-6412
Fax: 05251/60-6414
mailto:c5@uni-paderborn.de
http://hyperg.uni-paderborn.de/fiff_jt_97

Tagungsbüro:

Carmen Buschmeyer
Sekretariat Informatik und Gesellschaft
Universität-GH Paderborn
Fürstenallee 11
33102 Paderborn

Tel.: ++49 +52 51 60-64 12
Fax: ++49 +52 51 60-64 14
E-Mail: carmen@uni-paderborn.de

Tagungskonto:

Dieter Engbring
Volksbank Paderborn
BLZ: 472 601 21
Konto-Nr.: 880 8988 900

Weitere Informationen zur Tagung gibt es im WWW unter der Adresse:
http://hyperg.uni-paderborn.de/FIFF_JT_97

13. FIFF-Jahrestagung

Die Rolle kritischer ExpertInnen in der Informationsgesellschaft

14.-16. November 1997 in Paderborn

Programm:

Freitag 14.11.	
bis 18.00 Uhr	Ankunft und Anmeldung
18.00 Uhr	Eröffnung
18.30 Uhr	Podiumsdiskussion: „Kritische ExpertInnen – Zwischen Establishment und Bedeutungslosigkeit?“
20.30 Uhr	Abend im Gownsmen´s Pub

Samstag 15.11.	
9.00 Uhr	Arbeitsgruppen 1 – 10
14.00 Uhr	Arbeitsgruppen 1 – 10
17.30 Uhr	Mitglieder-Versammlung des FIFF

Sonntag 16.11.	
9.00 Uhr	kurze Vorstellung der AG-Ergebnisse
10.30 Uhr	Abschlußvortrag

Die Themen der Arbeitsgruppen

1 Arbeit in der Informationsgesellschaft – zwischen Degradation und Emanzipation

Moderation: Bettina Törpel
Berlin, 030/6135548, e-Mail: beetee@cs.tu-berlin.de
Prof. Dr. Rudi Schmiede
Darmstadt, 06151/16-2809, e-Mail: rs@ifs.th-darmstadt.de

Informatisierung und Wandel von Arbeitsteilung und gesellschaftlichen/kulturellen Strukturen.

Die gesellschaftliche Arbeit befindet sich im Umbruch: eine wachsende Anzahl von Arbeitenden verrichtet Informationsarbeit; in fast allen Bereichen verändern sich mit dem Übergang zur „Informationsgesellschaft“ die Arbeitsmittel und Arbeitsinhalte, und somit verändert sich letztlich der Charakter der Arbeit selbst. Insbesondere die gesellschaftliche Arbeitsteilung unterliegt gravierenden Veränderungen. Es besteht ein Bedarf an theoretisch fundierten Konzepten, um diesen Umbruch der Arbeit zu erfassen. In der Arbeitsgruppe wollen wir uns über Analyseansätze verständigen, mit denen sich der quantitative Umbruch von Arbeit und Gesellschaft erfassen läßt. Von zentralem Interesse ist das Verhältnis von Arbeit, Kultur und gesellschaftlichen Strukturen.

2 Vernetzte Computermenschen: Der Deutschen Tragödie zweiter Teil?

Moderation: Gerlinde Heinze, N.N.
Kontakt: Buchenstr. 45, 42283 Wuppertal

Der von Iwan P. Pawlow und John B. Watson gegründete Behaviourismus führt menschliches Verhalten und Lernen allein auf vorangegangene Konditionierungsprozesse zurück. Behaviouristischer Pädagogik liegt ein Menschenbild zugrunde, das Menschen als adaptionsfähige Computersysteme begreift. Die Pädagogik verdankt dieser Strömung auch positive Impulse, andererseits lassen behaviouristische Techniken sich sehr mißbrauchen: Wer Menschen ernsthaft für schlechtere Expertensysteme hält, kann leicht versucht sein, Menschen ganz wie Computer geplant zu programmieren. So entstehen Computermenschen, gute Funktionierer, die sich für nahezu jeden Zweck instrumentalisieren lassen. Treten Computermenschen in soziale Interaktion miteinander, so wirken sie wechselseitig als Multiplikatoren und programmieren sich zugleich nach einem vorgegebenen Regelwerk weiter – ganz wie vernetzte adaptionsfähige Systeme. Das kann geradewegs wieder in die Barbarei führen …

Wir InformatikerInnen verfügen über das Instrumentarium zur Analyse programmierter Abläufe. In der Arbeitsgruppe geht es um den Transfer dieses Instrumentariums auf Humanwissenschaften und um unseren Beitrag dazu, der barbarischen Produktion von Computermenschen humanistische Zielsetzungen entgegenzusetzen.

3 Die Explikation technologieformender Werte und Bedeutungszuschreibungen – ein Arbeitsbereich für kritische ExpertInnen?

Moderation: Dipl. Inf. Heike Stach, Dipl. Inf. Peter Eulenhöfer
Kontakt: IFP Sozialgeschichte der Informatik, TU Berlin, Sekr. FR 6-2, Franklinstr. 28/29, 10587 Berlin

Informationstechnologien werden nicht nur durch ökonomische und politische Interessen sowie durch Konstruktionsstile geformt. Auch kulturelle Deutungsmuster und Werte orientieren – zumeist unbewußt – in hohem Maße die Entwicklung und Nutzung von Techik. Im Interdisziplinären Forschungsprojekt „Sozialgeschichte der Informatik" an der TU Berlin wurde an relevanten Beispielen aus der Hardware-, Software- und Disziplingeschichte der Informatik der Einfluß solcher „Orientierungsmuster" herausgearbeitet.

In der Arbeitsgruppe soll diskutiert werden, inwieweit es sinnvoll und praktikabel ist, bereits bei der Gestaltung von Informationstechnik solche technologieformenden Werte und Bedeutungszuschreibungen zu explizieren und bewußt in den Gestaltungsprozeß einzubeziehen. Eröffnet sich dadurch ein neues Arbeitsfeld für kritische ExpertInnen?

4 NEW WORK: Das Ende der Arbeit und ihre Zukunft

Moderation: Ditz Schroer
Dozent für Informatik, Betriebsrat Siemens Nixdorf Informationssysteme AG Otto-Hahn-Ring 6, 81730 München
Konrad Jablonskie
Dipl.-Inf.; Betriebsrat Siemens Nixdorf Informationssysteme AG, Heinz-Nixdorf-Ring 1, 33106 Paderborn

Glücklich, wer noch einen festen Arbeitsplatz hat! Aber auch für die „abhängig Beschäftigten" ändert sich so manches: Wie arbeitet es sich in virtuellen Unternehmen, wie fühlen sich die neuen Formen von Team- und Gruppenarbeit an? Berichte aus dem modernen Arbeitsalltag mit seinen Konflikten und Freiräumen.

Struktur virtueller Unternehmen · Projektarbeit, Gruppenarbeit, Telearbeit · Skill-Datenbank · MitarbeiterInnenbewertung · Erfolgsabhängige Bezahlung · Arbeitsrechtliche Folgen · Betriebsräte als Netzräte

5 Informatisierung im Sozial- und Gesundheitsbereich

Moderation: Prof. Dr.-Ing. Dietrich Meyer-Ebrecht
Lehrstuhl für Messtechnik, RWTH Aachen, 0241/807860

Infolge des erhöhten Rationalisierungsdruckes im Sozial- und Gesundheitsbereich werden in Krankenhäusern und Sozialeinrichtungen verstärkt Informationstechnologien für die Kostenkontrolle und Qualitätssicherung eingesetzt. Zwar sind in diesem Zusammenhang Probleme des Datenschutzes und Angst vor dem gläsernen Patienten Themen der öffentlichen Diskussion. Jedoch findet man

Diesen Abschnitt bitte ausgefüllt
(Rückseite nicht vergessen)
und ausreichend frankiert
(z. B. im Fensterbriefumschlag)
an die angegebene Adresse senden!

Name, Adresse:

Universität-GH Paderborn
Sekretariat Informatik und Gesellschaft
Carmen Buschmeyer
Fürstenallee 11

33102 Paderborn

Tel. dienstl.:

Tel. privat:

kaum Kritisches über den Widerspruch zwischen informationstechnischer Optimierung von Geschäftsprozessen, die eine Formalisierung und Standardisierung implizieren, und dem Anspruch auf individuelle, ganzheitliche und patientenzentrierte Behandlung und Pflege. Ökonomie und Computer als rationale Konstruktionen verdrängen (ersticken) damit die von den Helfern zu erbringende Gefühls- und Beziehungsarbeit, die die Effektivität der instrumentellen Arbeit erst möglich machen.

Diskussionsthema ist die Frage, ob sich hier neue Lösungsansätze und Methodenkonzepte für eine Technisierung finden lassen, die diesem in der Informatikwelt nur selten widersprochenen Rationalisierungstrend eine Grenze setzen. Als Lösungsalternative wird die Methode der „Kommunikativen Systementwicklung", die anhand von zwei exemplarischen interdisziplinären Entwicklungsprojekten vorgestellt wird, diskutiert.

6 „Internet Politics" – Zur politischen Gestaltung der Informationsgesellschaft.

Moderation: Ingo Ruhmann
c/o Büro Kiper MdB, Bundeshaus HT 404, 53113 Bonn
Ute Bernhardt
FIfF-Geschäftsstelle, Reuterstr. 44, 53113 Bonn, Tel: 0228/ 219548 email: fiff@fiff.gun.de

Solange das Internet nur ein politisch unbedeutender Tummelplatz einer technischen Subkultur war, konnte sich darin ein komplexes System der Selbstregulierung entwickeln. Der Internet-Boom machte daraus für manche ein Wunschbild für Demokratie und Kultur.

Das mit der Kommerzialisierung und Politisierung des Internets einhergehende forcierte Zusammenwachsen bisher getrennter Rechts-, Politik- und Kulturräume macht überdeutlich, wie wenig diese Räume zusammenpassen. Überall wird im Internet Gefährliches, Verbotenes und Extremes geortet. Zum Schutz bestehender Werte und Normen greifen Politiker zunehmend ins Internet ein, um ein „anständiges" und sauberes Internet nach ihren Maßstäben zu schaffen. Der Communications Decency Act in den USA, das Informations- und Kommunikations-Dienstegesetz in der Bundesrepublik und ähnliche Vorhaben in anderen Staaten haben zum Ziel, das Internet unter Kontrolle zu bekommen.

Was ist der Hintergrund dieser Politik, was können Organisationen wie das FIfF tun, um Beschränkungen von Freiheitsrechten entgegenzuwirken? Wo hapert es in der Politik, zu kompetenten Entscheidungen über das Internet zu kommen, wo sind Ansatzpunkte politischen Handelns? Und vor allem: Was sollten die Ziele einer politischen Einflußnahme sein?

7 SOFTWEHRTECHNIK – Mit Sicherheit ein gutes Gefühl

Moderation und Kontakt: Peter Ansorge, Ralf E. Streibl
Universität Bremen FB 3 – Informatik, Postfach 330 440, 28334 Bremen, Tel. 0421/218-4044 o. -4922, email: ansorge@informatik.uni-bremen.de, res@informatik.uni-bremen.de

In der Arbeitsgruppe sollen aktuelle Probleme und Diskussionen im Themenbereich „Rüstung und Informatik" behandelt werden, insbesondere: · aktuelle Tendenzen in der Wehrtechnik · Software-Musterung: Tauglich oder nicht? · Möglichkeiten und Risiken der Rüstungskonversion im Informatikbereich · Dual-Use · Information Warfare · Militarisierung der Informationsgesellschaft · Rüstung und Informatik: zur Rolle kritischer ExpertInnen

Anmeldung zur Jahrestagung '97 in Paderborn

Hiermit melde ich mich verbindlich zur 13. FIfF-Jahrestagung „Zur Rolle kritischer ExpertInnen in der Informationsgesellschaft" an. Der Tagungsbeitrag beträgt:

	bei Zahlungseingang vor dem 10. Okt. 97	nach dem 10. Okt. 97
für Verdienende	80,- DM	100,- DM
für Studierende/Nichtverdienende	40,- DM	50,- DM

Den Beitrag in Höhe von _____ DM habe ich am _____ 1997 auf das Konto Dieter Engbring (Nr. 880 8988 900 bei der Volksbank Paderborn eG, BLZ 472 601 21) überwiesen.

Ich wünsche die Vermittlung einer (einfachen) privaten Unterkunft für ◯ 14./15. Nov. ◯ 15./16. Nov.

Ich bitte um die Vermittlung von Pension/Hotel (◯ Einzelzimmer) für ◯ 14./15. Nov. ◯ 15./16. Nov.

Die Arbeitsgruppe Nr. _____ interessiert mich besonders.

_____
Datum, Unterschrift

8 Kritische Informatik und (Allgemein-)Bildung

Moderation: Dieter Engbring, Rolf Oberliesen
Kontakt: Dieter Engbring, 05251/606410

Gegenwärtige gesellschaftliche Problemfelder zum Beispiel der Verteilung von Arbeit, der Lösung der Fragen von Krieg und Frieden, Globalisierung, Mediatisierung, Informationelle Selbstbestimmung sind entscheidend bestimmt durch informations- und kommunikationstechnologische Entwicklungen und Verwendungen. Kritische InformatikerInnen identifizieren diese Problemfelder als prinzipiell gestaltungsoffen.

Die Zukunft gesellschaftlicher Entwicklung wird entscheidend von der Gestaltung der Problemlösungen abhängen. Dies ist auch eine Frage von Bildung, einer „neuorientierten" allgemeinen Bildung, verstanden als eine Bildung für alle, die auf Mitgestaltungsfähigkeit abhebt und in der jene gesellschaftlichen Problemfelder Gegenstand der Auseinandersetzung und des Kompetenzerwerbs darstellen.

Kritische InformatikerInnen müssen versuchen, sich in diese Prozesse demokratischer Verständigung selbstgestaltend einzubringen, beziehungsweise ihre Mitgestaltungsrechte hinsichtlich der zukünftigen gesellschaftlichen Entwicklung einzufordern.

In der Arbeitsgruppe sollen verschiedene gesellschaftlicher Problemstellungen in Hinblick auf ihre Relevanz für eine allgemeine Bildung diskutiert werden.

9 Die „Informationsgesellschaft": Politisches Programm – Globalisierte Geschäftssphäre – Schön- und Schwarzfärberei

Moderation: Christel Keller
Uni Tübingen, Inf.-Fak.

Die „Informationsgesellschaft" hat sich als Sammelbegriff für alles eingebürgert, was mit dem Einsatz von Informations- und Kommunikationstechnik (IKT) in verschiedensten gesellschaftlichen Bereichen irgendwie zu tun hat. Aber wie genau? Das Schlagwort steht sowohl für positive Erwartungen wie negative Befürchtungen. Und stimmt es überhaupt, daß die IKT die Gesellschaft neu prägen?

1.These: Mit dem der Soziologie entlehnten Schlagwort von der „Informationsgesellschaft" wird eine Verwechslung von gesellschaftlichem Zweck und technischem Mittel transportiert.

2.These: In der „Informationsgesellschaft" – wie vordem in der „Industriegesellschaft" – faßt sich nicht nur ein fragwürdiger Soziologismus zusammen; daß dieser sich so erfolgreich in der Öffentlichkeit wie auch in der Informatik hält, dürfte sich seiner Verwendung durch die Politik verdanken: Mittlerweile firmieren weltweit politische Programme für Entwicklung und Anwendung innovativer IKT, staatliche Maßnahmen auf dem Gebiet des IKT-Einsatzes und Neuordnungen der Infrastruktur von Informations- und Kommunikationswesen und des Unterhaltungssektors unter den Topoi „Globale Informationsgesellschaft", EU-Programm 1994, „Fortgeschrittene Informationsgesellschaft", Japanisches Programm 1993/94, bzw. „Informationszeitalter", US-amerikanische Programme 1992/93. Diese Programme und ihre aktuellen Fortschreibungen sollen in der AG behandelt werden, denn sie geben Auskunft über die staatlichen Ziele, die unter dem Schlagwort „Informationsgesellschaft" verfolgt werden und die tatsächlich so einiges in der Gesellschaft verändern. Zentrales Thema hierbei ist das politische Motiv, der privatwirtschaftlichen Nutzung von IKT absolute Priorität einzuräumen.

3.These: Die „unausweichliche Entwicklung" wird einerseits geprägt durch die Konkurrenz zwischen den USA, Europa und Japan darum, welche Nation von der wirtschaftlichen Nutzung der IKT profitiert. Die Ziele sind zwar in allen Nationen gleichlautend; doch das steht nicht für eine arbeitsteilige, internationale IKT-Politik, sondern für einander ausschließende Nutzungsinteressen. Darüber dürfte sich auch erklären, wieso ganze Teile des Globus im weltumspannenden Netz gar nicht drin sind. Zweitens scheinen die großen Konkurrenten aber voneinander abhängig zu sein, so daß sie ihre Maßnahmen wechselseitig als Sachzwang empfinden, dem sie ausgesetzt sind.

(Die AG knüpft an den Abschlußvortrag von Hans-Jörg Kreowski auf der letztjährigen Jahrestagung an. Die Dokumente hängen alle im WWW, die URLs werden bei Bedarf rechtzeitig vorher mitgeteilt.)

10 Electronic Data System (EDS) – der größte Geheimdienst der Welt?

Moderation: padeluun
Kontakt über FoeBuD Bielefeld, http://www.foebud.org

Denn sie wissen, was wir tun.

„Datenschutz: Eine Handvoll Firmen verwalten die wichtigsten Informationen der Welt. Fast niemand kennt sie, aber sie kennt Millionen. Sie hat mehr sensible Daten über viele Bürger als das Finanzamt. Sie ist im Bilde über deren Lebensstil, über ihre Lieblingsfarbe und manchmal auch über die Vorlieben beim Sex. Sie weiss, wohin sie jedes Jahr in den Urlaub fliegen, welches Auto sie fahren und wie hoch ihr Dispo ist bei der Bank um die Ecke. Die Firma Electronic Data Systems Corporation (EDS) aus Plano, Texas, ist besser informiert als jede andere private Institution auf diesem Planeten. Kein Staat der Welt hat so viele Informationen über seine Bürger gespeichert. Und keine Rasterfahndung wäre in der Lage, ein derart genaues Persönlichkeitsprofil zu erstellen.(...)"

padeluun/Frank Rieger
Auszug aus: SPIEGEL special 3/96

Diese Arbeitsgruppe wird sich mit dem Thema EDS befassen.

Schwerpunkt:
»Sicherungsinfrastrukturen«

Die Autorinnen und Autoren:

Gerhard Banse ist Professor am Lehrstuhl *Allgemeine Technikwissenschaft* der Brandenburgischen Technischen Universität Cottbus und arbeitet an der *Europäischen Akademie zur Erforschung von Folgen wissenschaftlicher Entwicklungen* in Bad Neuenahr-Ahrweiler.

Peter Bittner ist wissenschaftlicher Mitarbeiter am *Zentrum für Interdisziplinäre Technikforschung* an der TH Darmstadt und Mitglied im FIfF-Vorstand.

Franz Büllingen ist Diplom-Soziologe und leitet die Forschungsgruppe *Technikfolgenabschätzung* des Wissenschaftlichen Instituts für Kommunikationsdienste (WIK).

Simone Fischer-Hübner ist wissenschaftliche Assistentin am Fachbereich Informatik der Universität Hamburg.

Dirk Fox ist wissenschaftlicher Mitarbeiter an der Universität Siegen im Gebiet *Sicherheit in Netzen und kryptographische Verfahren* sowie Mitherausgeber der Zeitschrift „Datenschutz und Datensicherheit (DuD)".

Käthe Friedrich ist promovierte Miarbeiterin am Lehrstuhl *Technikphilosophie* der Brandenburgischen Technischen Universität Cottbus.

Sara Reese Hedberg ist freiberufliche Journalistin in Issaquah, Washington. Sie interessiert sich für aktuelle Trends in der Informatik.

Annette Hillebrand ist Diplom-Sozialwirtin und wissenschaftliche Mitarbeiterin in der Forschungsgruppe *Technikfolgenabschätzung* des Wissenschaftlichen Instituts für Kommunikationsdienste (WIK).

Detlef Hühnlein ist Berater für IT-Sicherheit bei der SECUNET GmbH und wissenschaftlicher Mitarbeiter an der TH-Darmstadt.

Günther Müller ist Professor am *Institut für Informatik und Gesellschaft* der Universität Freiburg, dort leitet er die Abteilung Telematik. Außerdem ist er Leiter des Kollegs „Sicherheit in der Kommunikationstechnik".

Peter Pharow arbeitet seit 1996 als wissenschaftlicher Mitarbeiter an der Otto-von-Guericke-Universität Magdeburg am *Institut für Biometrie und Medizinische Informatik.*

Kai Rannenberg ist promovierter Mitarbeiter des *Instituts für Informatik und Gesellschaft* an der Universität Freiburg. Er ist Koordinator des Kollegs „Sicherheit in der Kommunikationstechnik".

Ralf Rohrer arbeitet bei "THOMSON multimedia" europaweit und ist verantwortlich für die Projektierung und Integration in den Bereichen Internet und UNIX Mail, Internet Security und Network Services.

Peter Schefe ist Professor für Informatik an der Universität Hamburg.

Jutta Stolp ist verantwortlich für Presse- und Öffentlichkeitsarbeit bei der Utimaco Safeware AG.

Olaf Winkel ist Privatdozent am Institut für Politikwissenschaft der Westfälischen Wilhelmsuniversität Münster.

Petra Wohlmacher ist als Universitätsassistentin an der Universität Klagenfurt im Institut für Informatik am *Lehrstuhl für Systemsicherheit* tätig.

Jens Woinowski ist wissenschaftlicher Mitarbeiter am FB Informatik der TH Darmstadt.

Verantwortlich für diesen Schwerpunkt sind:

Kathrin Schier ist wissenschaftliche Mitarbeiterin am Fachbereich Informatik der Universität Hamburg und arbeitet an ihrer Promotion zum Thema *Sicherheit im elektronischen Zahlungsverkehr.*

Claus Stark ist Medizininformatiker und arbeitet als Evaluator bei der *TÜV Informationstechnik GmbH* in Essen im Bereich Informationssicherheit.

Dirk Fox

Sicherungsinfrastrukturen

Fortschritt ist der Übergang von Situationen,
deren Nachteile man schon kennt,
zu Situationen,
deren Nachteile man noch nicht kennt.

Arnold Gehlen

Einführung

Mit der wachsenden Bedeutung von Rechnernetzen, der Verbreitung von Internet-Diensten wie *electronic mail* und dem Ausbau der „Datenautobahn" zu einem weltweiten *electronic market place* rücken Sicherheitsdienste und -mechanismen zum Schutz der übertragenen Daten z. B. vor unberechtigtem Zugriff oder Veränderung immer mehr ins Zentrum des Interesses.

Für eine allgemeine Durchsetzung und Verbreitung von Sicherheitsmechanismen sind jedoch neben einer Klarheit in der Frage der Kryptoregulierung (Freiheit, Verbot oder Einschränkung der Verwendung kryptographischer Verfahren) Standardisierung, Vereinheitlichung, einfache Handhabbarkeit und hohe Verfügbarkeit erforderlich. Der Siegeszug des Internet hat gezeigt, daß „smarte", d. h. einfache, preiswerte und für viele Betriebssysteme verfügbare Lösungen wie die Internet-Protokollfamilie (TCP/IP etc.) gegenüber komplexen und teuren, wenn auch sicherlich ausgefeilteren Lösungen wie den ISO-Protokollen eine wesentlich höhere Durchsetzungswahrscheinlichkeit besitzen.

Bei der Standardisierung der Internet-Protokolle und darauf aufsetzender Kommunikationsdienste wurde allerdings auf die Integration von Sicherheitsmechanismen nahezu vollständig verzichtet. Diese Nachlässigkeit rächt sich nun: Nachträglich müssen Protokolle und Dienste mit solchen Mechanismen ausgestattet werden, um für einen Einsatz z. B. für *„electronic commerce"*-Anwendungen geeignet zu sein. So befinden sich derzeit zahlreiche Protokollvarianten und -ergänzungen wie *Secure Socket Layer* (SSL), *Simple Key Management for Internet Protocols* (SKIP) oder *IP Security* (IPSec) in der Internet-Standardisierung (Fox 1997).

Allerdings genügt es keineswegs, Protokolle und Programme um kryptographische Verfahren zu bereichern, um die Kommunikation im Netz zu schützen. Denn wenn man eine gesicherte Kommunikation auch zwischen Teilnehmern ermöglichen will, die sich zuvor nie gesehen oder getroffen haben – eine wesentliche Eigenschaft *offener* Netze wie dem Internet – dann benötigt man darüber hinaus Vertrauensinstanzen, die wichtige Basisfunktionen wie z. B. die Erzeugung und Verteilung von Schlüsseln im Netz erfüllen. Ähnlich wie man die Gesamtheit aller Kommunikationsprotokolle, -dienste und Übertragungseinrichtungen beispielsweise des Internet als „Kommunikationsinfrastruktur" bezeichnet, wird daher in diesem Zusammenhang auch von „Sicherungsinfrastruktur" gesprochen (Hammer 1995).

Sicherungsinfrastrukturen

Eine Sicherungsinfrastruktur besteht im Kern aus technischen Komponenten, der Summe von (vereinheitlichten) Diensten und erforderlichenfalls rechtlichen Festlegungen. Als Infrastruktur zeichnet sie sich vor allem durch die folgenden Eigenschaften aus:

- Offenheit (Benutzer können Dienste für unterschiedliche Anwendungen frei wählen),
- Langlebigkeit (standardisierte Verfahren gewährleisten Investitionsschutz),
- Stabilität (Instandhaltung und redundante Auslegung verringern Ausfallzeiten) und
- Erweiterbarkeit (modulare Gestaltung und definierte Schnittstellen erlauben Ausbau).

Für spezielle Anwendungen wie beispielsweise Zahlungssysteme (Kreditkarten, EC-Karten, *electronic cash*, Geldkarte etc.) existieren bereits heute Vorformen einer Sicherungsinfrastruktur. Allerdings handelt es sich hier um geschlossene Systeme, da die einzelnen Dienste wie z. B. die Ausstellung von personalisierten Magnetstreifenkarten ausschließlich für eine bestimmte Anwendung erfolgt und freie Erweiterungen ebenfalls nicht möglich sind.

Ein zentraler Dienst einer Sicherungsinfrastruktur ist die Erzeugung von Schlüsseln, sowohl für die Sicherstellung von Vertraulichkeit (Schutz vor unbefugter Kenntnisnahme, z. B. durch Verschlüsselung von Daten) als auch für weitergehende Sicherheitsdienste wie Integrität (Schutz vor unbemerkter Veränderung, z. B. durch digitale Signaturen) oder Authentizität (überprüfbare Sicherstellung der Urheberschaft von Daten oder Kommunikationsabläufen). Wesentlich sind weiter die Verteilung dieser Schlüssel, für *„public key"*-Verfahren auch die authentische Bekanntmachung der öffentlichen Schlüssel, und erforderlichenfalls deren Rückruf, z. B. durch Sperrlisten.

Für diese Basisdienste werden „vertrauenswürdige Instanzen" benötigt, auch *trusted third parties* (TTP) genannt, die zusammen mit den Regeln und technischen Komponenten das Rückgrat der Sicherungsinfrastruktur bilden. Diese Instanzen sind einerseits zentrale Einrichtungen, denen von einer größeren Zahl von Benutzern besonderes Vertrauen entgegengebracht wird, und andererseits spezielle Hard- und Softwarekomponenten, wie z. B. geeignete Chipkarten im Besitz des einzelnen Benutzers,

die sensible Daten wie beispielsweise seine geheimen Schlüssel enthalten und denen dieser hinsichtlich der Nicht-Ausspähbarkeit besonders vertraut.

Das Vertrauen, das der Dienstnutzer den einzelnen Instanzen entgegenbringen muß, hängt dabei vom jeweiligen Dienst ab. So erfordern Komponenten oder vertrauenswürdige Dritte, die langlebige geheime Schlüssel (*master keys*) erzeugen, naturgemäß ein besonders großes Vertrauen. Hingegen kann das Vertrauen in öffentliche Schlüssel-Verzeichnisse wesentlich geringer sein: Integrität und Authentizität, d. h. Unverfälschtheit und Zugehörigkeit dieser Schlüssel zu einer Person, kann ein Benutzer selbst anhand der jeweiligen Schlüssel-Zertifikate überprüfen.

Um eine Infrastruktur zu bilden, müssen Dienste und Instanzen jedoch nicht nur das Vertrauen der Benutzer besitzen, sondern auch noch den oben genannten Kriterien genügen:

- **Offenheit** erfordert die freie Wählbarkeit der Dienste und Vertrauensinstanzen. Es müssen daher sowohl Anwendungen für unterschiedliche Betriebssysteme verfügbar als auch ein einheitlicher Zugriff auf diese Dienste möglich sein. Die Dienste selbst müssen so allgemein gestaltet sein, daß sie sich für unterschiedliche Anwendungen einsetzen lassen (z. B. Schlüssel für digitale Signatursysteme sowohl zum Signieren einer EMail als auch zum elektronischen Vertragsabschluß).
- **Langlebigkeit** setzt voraus, daß den angebotenen Diensten gut durchdachte und möglichst standardisierte Verfahren und Mechanismen zugrundeliegen, die ein Ersetzen durch korrigierte oder geänderte Versionen vermeiden. Dies erfordert z. B. einerseits die Verwendung öffentlich bekannter und geeigneter, d. h. vor allem als sicher einzustufender Kryptoalgorithmen, andererseits die Existenz einer politisch konsentierten und möglichst liberalen Krypto-Policy.[1]
- **Stabilität** kann durch die Etablierung konkurrierender Vertrauensinstanzen erreicht werden. Bei Ausfall einer Instanz können deren Dienste von einer anderen Instanz übernommen werden. Auch die Beschränkung auf möglichst wenige, vereinheitlichte Verfahren und Mechanismen erhöht die Stabilität der Infrastruktur durch die Austauschbarkeit einzelner Komponenten.
- **Erweiterbarkeit** läßt sich durch einen weitgehenden Verzicht auf Beschränkungen und die Verwendung von Verfahren erreichen, die dynamische Ergänzungen wie z. B. neue Schlüsselerzeugungs-Instanzen zulassen.

Aktuelle Entwicklungen

Will man eine allgemein akzeptierte Sicherungsinfrastruktur etablieren, sollte möglichst ein unkontrolliertes „Wuchern" vermieden werden. Das kann einerseits indirekt durch die Förderung gewünschter Entwicklungen oder andererseits durch direkte rechtliche Steuerung geschehen.

Den ersten Weg beschreiten EU und US-Regierung, indem sie Projekte fördern, die sich die Entwicklung einer technischen Zertifizierungs-Infrastruktur zum Ziel gesetzt haben (Chokhani 1994). Eine solche Infrastruktur ist überfällig, denn schon heute stehen sich unterschiedliche und damit nicht verträgliche Standards gegenüber – sowohl für kryptographische Verfahren und Mechanismen als auch für Datenstrukturen wie bspw. Zertifikate (z. B. X.509, CV, PKCS, PGP,...). Einige Projekte zielen daher darauf, die unterschiedlichen Ansätze zu vereinen (Chadwick et al. 1997). Seit einer Weile arbeitet die ISO an der Standardisierung von „*trusted third party* (TTP)"-Diensten (ISO 1997), und kürzlich wurde von DIN ein Projekt zur Spezifikation von TTP-Diensten für die Anwendungen digitaler Signaturen initiiert. Zugleich werden unabhängig davon durch den Aufbau von Infrastrukturen andernorts Fakten geschaffen – z. B. durch den Aufbau von Trust Centern für PGP-Schlüssel.[2]

Den zweiten Weg hat nun die Bundesregierung mit dem Signaturgesetz (SigG) beschritten, das am 4. Juli 1997 vom Bundesrat als Teil des Informations- und Kommunikationsdienstegesetzes (IuKD-G) verabschiedet wurde und zum 1. August 1997 in Kraft getreten ist (Engel-Flechsig 1997). Dieses Gesetz legt die Gestaltung einer Sicherungsinfrastruktur für digitale Signaturen fest, mit der auf mittlere Sicht erreicht werden soll, daß digitale Signaturen dasselbe Vertrauen und die selbe Rechtskraft gewinnen, die heute eigenhändige Unterschriften genießen. Damit ist Deutschland der erste europäische Staat, der nach dem Beispiel des US-Bundesstaates Utah die Bedeutung digitaler Signaturen für neue, elektronische Dienste erkannt hat und deren Entwicklung und Durchsetzung regulierend gestaltet. Deutschland spielt daher in diesem Bereich eine wichtige Vorreiterrolle, wenigstens in Europa.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) arbeitet derzeit unter Einbeziehung von Industrie und Experten fieberhaft an einem Maßnahmenkatalog, der Empfehlungen für die Umsetzung der Regelungen der zum Signaturgesetz gehörigen Signaturverordnung (SigV) enthält. Dabei zeigt sich, welche Schwierigkeiten sich im Detail bei der Ausgestaltung einer solchen Infrastruktur ergeben.

Der Erfolg des Signaturgesetzes wird einerseits davon abhängen, ob die Industrie in absehbarer Zeit genügend anwendergerechte und sinnvolle Anwendungen z. B. für *electronic commerce* anbieten wird, die die Dienste dieser Sicherungsinfrastruktur nutzen. Viel wichtiger aber wird sein, ob genügend viele Menschen der entstehenden Infrastruktur ausreichend Vertrauen entgegenbringen werden.

Gesellschaftliche Auswirkungen

Zweifellos wird der Aufbau einer Sicherungsinfrastruktur die Erweiterung heutiger Kommunikationsdienste um

1. So würde beispielsweise ein Verbot starker Kryptoalgorithmen einen häufigen Verfahrenswechsel zur Folge haben, da schwache Kryptoalgorithmen sehr bald nicht einmal mehr vor Angreifern mit vergleichsweise geringem Potential schützen können (Blaze 1997).

2. Trust Center für PGP-Schlüssel werden z. B. betrieben vom DFN-Cert (http://www.cert.dfn.de/dfnpca/) und dem MAZ in Hamburg (http://www.trustcenter.de).

Sicherheitsmechanismen ermöglichen und vorantreiben. Damit werden einerseits längst überfällige Defizite in Sicherheit und Verläßlichkeit der schon heute auch in kritischen Anwendungen genutzten Kommunikationsinfrastruktur verringert.

Andererseits werden zugleich eine Vielzahl neuer Dienste durch diese Sicherungsinfrastruktur erst möglich, wie digitale Zahlungssysteme (Knorr, Schläger 1997) und *„electronic commerce"*-Anwendungen (Grimm 1997), sogar elektronische Wahl-Systeme. Sollten diese zukünftig herkömmliche Formen des Zahlens (z. B. Bargeld), Kaufens (Besuch eines echten Warenhauses) und Wählens (Wahlurne) ersetzen, wird dies zweifellos erhebliche Auswirkungen auf unser tägliches Leben und unser Verhältnis zur Technik haben. So werden zum einen die „Datenspuren", die wir als Kunde und Bürger hinterlassen, sich zu nahezu lückenlosen Bewegungs- und Verhaltensprofilen verdichten lassen – schon heute wird das Daten-Netz dank bargeldloser Zahlungsmittel, dem Einzug der Datenverarbeitung in der Medizin und der Verbreitung neuer Kommunikationstechniken wie Mobilfunkgeräten, die ständig unseren Standort durchgeben, immer engmaschiger.

Zum anderen wird unsere Abhängigkeit vom fehlerfreien Funktionieren dieser Techniken steigen und damit auch die Verletzlichkeit unserer Gesellschaft (Roßnagel 1991). Die Undurchschaubarkeit technischer Vorgänge wird zunehmen, denn Geräte und Abläufe werden zunehmend komplexer. Beides könnte sich zu einem allgemeinen Gefühl des „Ausgeliefertseins" gegenüber der Technik verdichten. Und schließlich ist es eine offene Frage, ob diese neuen Techniken und Dienste nicht Teile der Gesellschaft von ihrer Nutzung ausschließen, sei es aus finanziellen, sei es aus anderen Gründen.

Zweifellos lassen sich sämtliche dieser negativen Auswirkungen durch geeignete Gestaltung der Technik vermeiden, z. B. durch das Prinzip der Datensparsamkeit, die Verwendung anonymer Protokolle, sowie eine hohe Verfügbarkeit durch Redundanz und die Koexistenz der neuen Techniken neben herkömmlichen, vertrauten, meist nicht-elektronischen Diensten. Noch ist es eine offene Frage, ob sich diese Art der Technikgestaltung durchsetzen kann; in vielen Bereichen sieht es derzeit nicht danach aus. Aber selbst dann bleibt es eine zentrale Herausforderung nicht nur für Techniker, die heute vielleicht nicht einmal absehbaren Risiken und negativen Folgen neuer Techniken und Dienste abzuwenden.

Glossar

CV	*Card Verifiable Certificate*: Schlüssel-Zertifikatsformat nach ISO/IEC 7816-8 (Standard-Entwurf), das sich für den Einsatz auf Chipkarten eignet (Wohlmacher 1997).
IPSec	*IP Security*: Sicherheitsmechanismen für das *Internet Protocol* (IP), spezifiziert in aktuellen *Request for Comments* (RFC) (Fox 1997).
ISO	*International Organization for Standardization*: Internationale Vereinigung der nationalen Standardisierungsgremien (in Deutschland: DIN).
ITU	*International Telecommunication Unit*: Internationales Telekommunikations-Standardisierungsgremium; früher CCITT.
PEM	*Privacy Enhanced Mail*: Internet-Standard-Familie zur Erweiterung des EMail-Protokolls um Verschlüsselung und digitale Signaturen (Horster, Portz 1994).
PGP	*Pretty Good Privacy*: Sehr verbreitete *Public-Domain*-Implementierung verschiedener Kryptoverfahren. Dazu existieren inzwischen viele Erweiterungen für EMail-Systeme, die ein bedienungsfreundliches Verschlüsseln und digitales Signieren von Mail-Nachrichten erlauben (Stallings 1995).
PKCS	*Public Key Cryptography Standards*: Spezifikation asymmetrischer Kryptoverfahren, Schlüssel-Zertifikats- und Nachrichtenformate der Firma RSA Inc.
SKIP	*Simple Key Management for Internet Protocols*: Vorschlag für einen Internet-Standard zum Schlüsselmanagement, angelehnt an das Diffie/Hellman-Protokoll (Fox 1997).
SSL	*Secure Socket Layer*: Internet-Standard (Entwurf, aktuelle Version 3) zum Schutz der Internet-Dienste WWW, EMail und News unter Verwendung asymmetrischer Kryptoverfahren.
X.509	Erste Standardisierung eines Formates für Schlüssel-Zertifikate, CCITT (heute ITU) 1988. Enthält auch ein Authentisierungsprotokoll mit asymmetrischen Kryptoverfahren und wurde Ende 1993 in Neufassung verabschiedet. Liegt inzwischen der ISO in erweiterterter Version 3 zur Standardisierung vor.

Literatur

Blaze, Matt: *Kryptopolitik und Informations-Wirtschaft*. Datenschutz und Datensicherheit (DuD), 4/97, S. 209-213.

Chokhani, Santosh: *Toward a National Public Key Infrastructure*. IEEE Communications Magazine, 9/94, S. 70-74.

Chadwick, David W.; Young, Andrew J.; Cicovic, Nada Kapidzic: *Merging and Extending the PGP and PEM Trust Models – The ICE-TEL Trust Model*. IEEE Network, May/June 1997, S. 16-24.

Engel-Flechsig, Stefan: *Teledienstedatenschutz*. Datenschutz und Datensicherheit (DuD), 1/97, S. 8-16; sowie: *IuKDG vom Bundestag verabschiedet*. Datenschutz und Datensicherheit (DuD), 8/97, S. 474-476.

Fox, Dirk: *Sicherheit: Schutzmechanismen fürs Internet*. iX – Magazin für professionelle Informationstechnik, 5/97, S. 148-153.

Grimm, Rüdiger: *Electronic Commerce*. Gateway, Datenschutz und Datensicherheit (DuD), 7/97, S. 420.

Hammer, Volker (Hrsg.): *Sicherheitsinfrastrukturen. Gestaltungsvorschläge für Technik, Organisation und Recht*. Springer Verlag, Heidelberg 1995.

Horster, Patrick; Portz, Michael: *Privacy Enhanced Mail: Ein Standard zur Sicherung des elektronischen Nachrichtenverkehrs im Internet*. Datenschutz und Datensicherung (DuD), 8/94, S. 434-442.

International Organization for Standardization (ISO): *Guidelines for the use and management of Trusted Third Parties (TTP)*. ISO/IEC CD 14516, 1997.

Knorr, Michael; Schläger, Uwe: *Datenschutz bei elektronischem Geld*. Datenschutz und Datensicherheit (DuD), 7/97, S. 396-402.

Roßnagel, Alexander: *Verletzlichkeit und Komplexität einer informatisierten Gesellschaft*. Datenschutz und Datensicherung (DuD), 9/91, S. 442-446.

Stallings, William: *Protect Your Privacy. A Guide for PGP Users*. Prentice Hall PTR, Englewood Cliffs, 1995.

Wohlmacher, Petra: *CV-Zertifikat*. Gateway, Datenschutz und Datensicherheit (DuD), 5/97, S. 291.

Jutta Stolp, UTIMACO AG

SigG

Warum brauchen wir ein Signaturgesetz ?

Mit dem am 1. August 1997 inkraftgetretenen Signaturgesetz ist ein wichtiger Schritt in Richtung der Beweisfähigkeit digitaler Dokumente und deren Gleichbehandlung mit der im Rechtsverkehr vorgeschriebenen Schriftform erfolgt. Die Fragen der rechtlichen Gleichstellung werden mit diesem Gesetz zwar nicht explizit geregelt. Mit der Formulierung von Anforderungen an eine hohe Gesamtsicherheit des Verfahrens ist allerdings eine wichtige Voraussetzung für die faktische Sicherheit digitaler Signaturen geschaffen worden. Eine gesetzliche Gleichstellung wird auf dieser Basis nur eine Frage der Zeit sein.

Trotz wachsender Nutzung von kommunikationstechnischen Möglichkeiten wie E-Mail, Electronic Commerce oder Electronic Banking ist das Problem der Verbindlichkeit digitaler Willensäußerungen (Bestellungen, Zahlungsanweisungen etc.) noch weitgehend ungelöst. Solange es nicht zu Unstimmigkeiten kommt, wird dieser Zustand fraglos hingenommen. Wird das digitale Geschäft allerdings von einer Partei angefochten, ist die Beweislage schwierig. Elektronische Dokumente können mit jedem Editor auf einfache Weise verändert werden. Ein elektronischer Überweisungsauftrag über 1000 DM läßt sich durch eine unbemerkt angehängte Null auf 10.000 DM verzehnfachen. Wie läßt sich darüber hinaus eindeutig der Urheber bzw. Absender einer digitalen Nachricht bestimmen?

Digitale Dokumente müssen fälschungssicher sein, um einen verbindlichen Charakter zu erhalten. Die Fälschungssicherheit umfaßt sowohl den Inhalt des Dokumentes (Integrität) als auch die Urheberschaft (Authentisierung des Urhebers/Absenders). Manipulationen am Informationsgehalt müssen sich eindeutig feststellen lassen. Darüber hinaus muß es möglich sein, den Urheber eindeutig zu bestimmen, so daß niemand unter falschem Namen ein Dokument erstellen bzw. versenden kann und andererseits ein Urheber das Erstellen und Versenden eines Dokumentes nicht abstreiten kann (non repudiation).

Herkömmliche Dokumente garantieren dies beispielsweise durch ein besonderes Papier, vorgedruckte Formulare und nicht zuletzt durch die handschriftliche Unterschrift. Bei der elektronischen Erstellung und Versendung von Dokumenten entfallen diese Echtheitsmerkmale, denn das Resultat liegt in digitaler Form vor – also als reine Bit-Folge nach dem Muster des jeweiligen Datenformats einer Anwendungssoftware.

Sicherheit durch Kryptographie

Um die Fälschungssicherheit digitaler Dokumente zu gewährleisten sind verschiedene kryptographische Verfahren entwickelt worden, deren gemeinsamer Nenner die Verwendung digitaler Signaturen auf der Basis von Public-Key-Systemen ist. Eine digitale Signatur hat in diesem Fall nichts mit einer digitalisierten handschriftlichen Unterschrift zu tun, wie sie beispielsweise beim Einscannen und Kopieren entsteht. Sie wird bei kryptographischen Verfahren vielmehr durch mathematische Verfahren (Algorithmen) zur Ver- und Entschlüsselung von Daten erzeugt. Public-Key-Systeme haben die besondere Eigenschaft, daß die Ver- und korrekte Entschlüsselung von Daten auf der Basis eines eindeutigen Schlüsselpaares (private key/public key) erfolgen. Zur Verschlüsselung wird der private key verwendet. Die korrekte Entschlüsselung der Daten ist nur mit dem dazugehörigen public key möglich. Das Verfahren muß sicherstellen, daß der private key eindeutig einer bestimmten Person gehört, dort sicher verwahrt wird und aus dem public key nicht ableitbar ist.

Jeder Teilnemer dieses kryptographischen Systems verfügt demnach über ein persönliches Schlüsselpaar. Soll ein Dokument digital signiert werden, wird mittels eines mathematischen Verfahrens (Hash-Funktion) zunächst ein digitaler Fingerabdruck des Dokuments erzeugt. Der Wert dieser Hash-Funktion ist für jedes Dokument eindeutig. Jede Änderung des Dokumentes führt zu einem neuen Hashwert. Im nächsten Schritt wird dieser Hashwert mit dem private key des Teilnehmers signiert (verschlüsselt) und anschließend zusammen mit dem Original-Dokument gespeichert oder elektronisch übermittelt. Die Prüfung erfolgt in umgekehrter Reihenfolge: Der signierte Hashwert wird mit dem öffentlichen Schlüssel des Teilnehmers entschlüsselt (dieser kann z. B. einem öffentlichen Verzeichnis entnommen oder an das Dokument angehängt werden) und mit dem Hashwert des Original-Dokumentes verglichen. Stimmen die Resultate überein, ist sowohl die Korrektheit des Dokumenteninhalts als auch die Urheberschaft eindeutig erwiesen.

Problem: Zertifizierung von Schlüsselpaaren

Eine wichtige Bedingung für die Sicherheit der digitalen Signatur ist eine eindeutige Zuordbarkeit des public keys zu einer Person. Anderenfalls könnte sich jeder Teilnehmer eine beliebige Anzahl von public keys und damit eine Vielzahl von digitalen Identitäten zulegen bzw. unter dem Namen einer anderen Person digital signieren. Um dies zu verhindern, ist eine Bescheinigung (Zertifikat) durch Dritte erforderlich, die die Zugehörigkeit eines Schlüsselpaares zu einer Person bestätigt. Ein solches Zertifikat kann ebenfalls digital erstellt werden. In der einfachsten Form würde ein solches Zertifikat aus der von einer neutralen Stelle digital signierten Kombination des öffentlichen Schlüssels und des Namens einer Person bestehen. Es kann aber auch weitere Erkennungszeichen umfassen sowie die Gültigkeitsdauer des Zertifikats festlegen. Weitere Zertifizierungshierarchien sind denkbar, um eine Prüfung der Echtheit von Zertifikaten zu gewährleisten.

Problem: Darstellung von Dokumenten, Korrektheit des Verfahrens

Weiterhin muß sichergestellt sein, daß bei der Erzeugung digitaler Signaturen eine korrekte Darstellung der zu signierenden Daten erfolgt. Wer etwas digital signiert, muß sicher sein können, daß die Daten, die am Bildschirm angezeigt werden, mit dem Inhalt der unterzeichneten Datei übereinstimmen. Ist die Datei beispielsweise mit einem Virus infiziert, der bei einem späteren Aufruf der Datei den Inhalt verändert, wird die Signatur ungültig. Eine Gefahr sind auch sogenannte Trojaner (Programme, die eine andere Funktion vortäuschen als sie tatsächlich ausführen), die beispielsweise unbemerkt eine Signatur nicht-gewählter Dateien veranlassen können. Deutlich wird hierbei, daß nicht nur das eigentliche Signaturverfahren sicher sein muß, sondern auch die zusätzlich genutzten technischen Komponenten wie Hardware, Betriebssystem und Anwendungssoftware.

Anforderungen des SigG und der SigV an die digitale Signatur

Das Signaturgesetz (SigG) enthält allgemeine Rahmenbedingungen und läßt Raum für unterschiedliche innovative technische Lösungen. Es fordert explizit die Verwendung eines Public-Key-Verfahrens für die Erzeugung und Prüfung digitaler Signaturen. Spezielle Algorithmen zur Schlüsselgenerierung, zur Hash-Funktion und zum Signaturmechanismus werden nicht vorgeschrieben. Das Gesetz fordert eine hohe Fälschungssicherheit digitaler Signaturen und verlangt dazu u.a. eine Prüfung der technischen Komponenten, die das Verfahren realisieren. Diese Prüfung hat nach dem jeweils aktuellen Stand der Technik zu erfolgen. Ob ein Verfahren die Anforderungen des Gesetzes erfüllt, soll durch von der zuständigen Bundesbehörde (Regulierungsbehörde nach § 66 des Telekommunikationsgesetzes) anerkannte Evaluierungs- und Zertifizierungsstellen (z. B. BSI) bestätigt werden. Interessant ist hierbei, daß die dem BSI auferlegte Zurückhaltung bei der Bewertung von Algorithmen (aus Gründen der Geheimhaltung des dortigen Know-How) nicht für Algorithmen für die digitale Signatur gilt.

Detaillierte Anforderungen an das Verfahren sowie die Sicherheitshöhe nach ITSEC für bestimmte Einsatzbereiche werden in einer Signaturverordnung (SigV) ausgeführt. Zu einer Grundforderungen dieser SigV zählt beispielsweise der notwendige Einsatz von Hardware (z.B. Chipkarte, PCMCIA-Karte) zur sicheren Speicherung des private keys nach dem Prinzip Besitz und Wissen. Des weiteren wird dort die Gültigkeitsdauer von Zertifikaten auf maximal 14 Jahre eingeschränkt. Die Signaturverordnung wurde vom zuständigen Bundesministerium erlassen und kann ohne weitere Beschlußfassung auf Bundesebene fortgeschrieben werden. Höhere Anforderungen an die technischen Komponenten und einzelne Parameter (z. B. höhere Schlüssellänge) können somit zügig umgesetzt werden. Die Entwicklung von geeigneten Verfahren ist der Wirtschaft im freien Wettbewerb überlassen.

Des weiteren regeln das Signaturgesetz und die Signaturverordnung eine Reihe von Fragen der Sicherheitsinfrastruktur, die zur Gewährleistung der Gesamtsicherheit der Verfahren erforderlich ist. Im einzelnen geht es um die Fragen:

- Wer generiert die Schlüsselpaare?
- Wer zertifiziert Schlüsselpaare und personalisiert z. B. Chipkarten?
- Welche Anforderungen müssen Zertifizierungsstellen erfüllen?
- Wie ist die Zertifizierungshierachie aufgebaut?

Nach dem derzeitigen Stand können Schlüsselpaare sowohl vom Anwender als auch von einer lizenzierten Zertifizierungsstelle generiert werden. Werden Schlüsselpaare von einer Zertifizierungsstelle generiert, dürfen die private keys dort nicht gespeichert werden. Generieren Anwender (zum Beispiel eine Bank oder ein Kaufhaus) Schlüsselpaare, muß der Einsatz eines anerkannten Verfahrens nachgewiesen werden. Zum Betrieb einer kommerziellen Zertifizierungsstelle (Trust Center) ist eine Lizenz der zuständigen Behörde nach § 66 Telekommunikationsgesetz erforderlich. Es werden hohe Sicherheitsanforderungen an den Betreiber gestellt, die u. a. ein vollständiges Sicherheitskonzept vorschreiben. Die Zertifizierungsstelle stellt Zertifikate für Schlüsselpaare aus und führt ein Verzeichnis über erteilte bzw. gesperrte Zertifikate. Als sogenannte „Wurzelinstanz" stellt die zuständige Behörde Zertifikate für die Signaturschlüssel der Zertifizierungsstellen aus, die zum Signieren von Anwender-Zertifikaten eingesetzt werden. Ein Verzeichnis der für Zertifizierungsinstanzen geltenden Zertifikate muß öffentlich zugänglich sein.

Internationale Anerkennung digitaler Signaturen

Nach dem SigG sind digitale Signaturen gleichgestellt, die mit einem öffentlichen Signaturschlüssel überprüft werden können, für das ein Zertifikat aus einem anderen Mitgliedsstaat der Europäischen Union oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum vorliegt. Darüber hinaus muß das Verfahren vergleichbare Sicherheit bieten. Weltweit dürfte es zu einer überstaatlichen oder zwischenstaatlichen Anerkennung kommen, wobei das SigG dafür die nationale Grundlage bildet.

Fazit

Mit dem Signaturgesetz und der Signaturverordnung ist eine wichtiger Schritt in Richtung der Anpassung gesetzlicher Regelungen an die Praxis des modernen Wirtschaftsverkehrs erfolgt. Darüber hinaus wird durch Festlegung von Anforderungen an zulässige Verfahren einem Wildwuchs unterschiedlicher Verfahren vorgebeugt, der im Zuge der Internationalisierung von Märkten eher hinderlich wäre. Die Entwicklung geeigneter Verfahren ist der Wirtschaft im freien Wettbewerb aufgetragen worden. Jetzt sind die Hersteller aufgefordert, für den nationalen und internationalen Markt entsprechende Lösungen bereitzustellen, die für Unternehmen und Behörden bundesweit aber auch in Europa sicherlich bald eine wichtige Bedeutung haben werden.

Nachdruck aus: Logon Sonderausgabe, Informationsdienst der Utimaco Safware AG, mit freundlicher Genehmigung.

Peter Bittner und Jens Woinowski

Vertrauen ist der Anfang von allem

Über Vertrauen, Sicherungsinfrastrukturen und Gestaltung

Vertrauen ist eine Brücke zwischen zwei Menschen,
die dadurch entsteht, daß beide losgehen.

Jochen Mariss, Bielefeld

Einleitung

Wir erleben derzeit einen Schub von Technisierung, der zu einem großen Teil von der Informations- und Kommunikationstechnik getragen wird. In diesem Artikel wollen wir die Bedeutung des Vertrauensbegriffes für solche technische Systeme untersuchen. Hierzu gehört auch eine Fundierung der verwendeten Begriffe. Wir werden Vertrauen im Zusammenhang mit Sicherungsinfrastrukturen (auf deren technische Details wir hier jedoch nicht eingehen werden) und der Gestaltungsproblematik diskutieren. Die Kernthese dieses Artikels ist, daß der Vertrauensbegriff im Zusammenhang mit technischen Systemen häufig fälschlicherweise anstelle des korrekteren Begriffes Verläßlichkeit verwendet wird.

„Vertrauen reduziert soziale Komplexität, wenn Entscheidungen trotz Unsicherheit über das Verhalten anderer Menschen [...] getroffen werden müssen." (Hammer 1995) Grundsätzlich kann Vertrauen in sozialen Systemen verschiedenster Größe von Bedeutung sein. Es bleibt aber im Kern immer eine subjektive Leistung einzelner Menschen.Vertrauen zwischen betroffenen Handlungssubjekten muß dabei zuerst einmal aufgebaut bzw. erworben werden – auch wenn hier eine Grundkomponente, die Fähigkeit zu vertrauen, als Urvertrauen gegeben sein muß. In seinem Wirken kann es entweder sich als berechtigt erweisen (funktionieren), oder es kann zu Störungen kommen, welche letzten Endes entweder überwunden werden oder das Vertrauen vergehen lassen. Eine wesentliche Rolle spielen dabei auch hierarchische oder abstrakte Vertrauenskonstellationen (z.B. Rechtssicherheit).

„Vertrauen" in Technik vs. Personenvertrauen

In seinem Artikel „Vertrauen in Technik" (Wagner 1992) fragt Gerald Wagner nach dem *„Ermöglichungsgrund"* für das *soziale Funktionieren technischer Artefakte* und findet die Antwort im Begriff des Vertrauens. Er sieht die moderne Gesellschaft als eine „Vertrauensgemeinschaft in Technik" an. Insbesondere schlägt er vor, *„Vertrauen als das symbolische Meta-Kommunikationsmedium der technisierten Lebenswelt* aufzufassen". Im Rahmen seiner Analyse stellt er (unter Hinzuziehung von Max Weber und Niklas Luhmann) verschiedene Begriffe von Personen- und Systemvertrauen vor. Diese beinhalten auch Vertrauen in die „prinzipielle[n] Rationalität der Gesellschaftsordnung." Da sowohl die Deutung von Vertrauen als Medium der Kommunikation, als auch der (Luhmannsche) Systembegriff als soziale Begriffe zu verstehen sind, halten wir es für gerechtfertigt, grundsätzlich nur für Personenvertrauen auch tatsächlich das Wort „Vertrauen" zu verwenden.

Damit nehmen wir an, daß Vertrauen sich grundsätzlich immer auf Formen persönlicher Beziehungen stützen muß. Das kann allerdings auch heißen, daß diese direkten Beziehungen nur die unterste Stufe einer komplexen Hierarchie sind – was sich z. B. im Gedanken der Sicherungsinfrastrukturen widerspiegelt. Mit anderen Worten besteht die „Vertrauens"würdigkeit gerade von großen technischen Systemen nicht darin, wie das System selbst ist, sondern wie es den Betroffenen durch andere – im allgemeinen selbst Betroffene – dargestellt wird. Damit wird die „Vertrauens"würdigkeit technischer Systeme auf zwei Säulen zurückgeführt: Personenvertrauen und Verläßlichkeit der Technik. Beides sind Punkte, die im Rahmen der Systemgestaltung, von der Einführung bis zum Gebrauch, eine wesentliche Rolle spielen.

Über Vertrauen und Verläßlichkeit

Nach dieser Vorarbeit sollte der Unterschied nachvollziehbar sein, den wir zwischen Verläßlichkeit und Vertrauenswürdigkeit sehen. Wir nutzen dabei auch die umgangssprachliche Unterscheidung zwischen „sich auf jemanden (oder etwas) verlassen" und „jemandem vertrauen". Der Begriff der Verläßlichkeit technischer Systeme ist bereits ausreichend gesichert. So stellt etwa M. Marhöfer fest: „Will man Verläßlichkeit genauer fassen, unterscheidet man verschiedene Teilaspekte, wie z.B. Funktionsfähigkeit, Sicherheit im Sinne von Safety und Sicherheit im Sinn von Security." Erweitert wird das durch Hans Brüggemann und Waltraud Gerhardt-Häckl, nach denen Verläßlichkeit ein „Bündel von Systemeigenschaften" über die „klassischen Sicherheitsanforderungen" hinaus anzusehen ist. Dazu gehören auch „Durchschaubarkeit", „Rückverfolgbarkeit" und „Verantwortbarkeit der Nutzung" (Brüggemann/Gerhardt-Häckl 1995). Allerdings tun sie einen nächsten Schritt, den wir so nicht nachvollziehen wollen: „Verläßlichkeitskriterien sind ein Schlüssel für das Vertrauen, das Benutzer und Betreiber in technische Systeme setzen." Im Sinne unserer Unterscheidung müßte das heißen, sie sind auf der technischen Ebene ein Maßstab dafür, wie sehr sich Benutzerinnen und Betreiberinnen auf das System verlassen können. Auf der sozialen Ebene sind sie ein Moment (neben anderen), das das Vertrauen in Entwickler und das gegenseitige Vertrauen von Betreibern und Benutzern rechtfertigt.

Vertrauen: Entstehen – Wirken – Vergehen

Für ein besseres Verständnis soll in den zwei folgenden Abschnitten der Begriff des Vertrauens in seinem Entstehen, seinem Wirken, seinen möglichen Störungen und seinem Vergehen intensiver aus einem eher „theoretischen" Blickwinkel angegangen werden. Wir halten diese Betrachtungen für unumgänglich, da es sich bei Vertrauen um ein sehr komplexes Phänomen handelt. Insbesondere ermöglicht diese umfangreichere Analyse hinterher, in den Abschnitten über Sicherungsinfrastrukturen und Gestaltung eine knappere, elegantere Darstellung.

Über die „Produktion" des Erfahrungs- und Zukunftsgutes Vertrauen

Vor allem die *persönlich* zurechenbaren Handlungen sind es, die Vertrauen hervorrufen; damit sind solche Handlungen gemeint, „die nicht zum Kanon der 'Systemerwartungen' gehören" (Offermanns 1990) bzw. mit Luhmann gesprochen unter die „ausdrucksschwache Normausführung" (Luhmann 1989) fallen. Einen günstigen Nährboden für Vertrauensbeziehungen findet man in denjenigen sozialen Zusammenhängen, die durch eine relative Dauer der Beziehung, wechselnde Abhängigkeiten und ein Moment der Unvorhersehbarkeit ausgezeichnet sind. Für Vertrauen herrscht das Gesetz des Wiedersehens, man muß sich immer wieder in die Augen blicken können. Vertrauen ist in die Zukunft gerichtet. Es bedarf zwar der in der Vergangenheit (am besten selber) gemachten Erfahrungen als Absicherung – insofern ist es Erfahrungsgut – es ist aber „keine Folgerung aus der Vergangenheit, sondern es überzieht die Informationen, die es aus der Vergangenheit besitzt und riskiert eine Bestimmung der Zukunft." (Luhmann 1989, S. 20)

Vertrauensbeziehungen haben graduellen Charakter. In der Regel wird nicht bedingungslos vertraut, sondern in Grenzen und nach Maßgabe vernünftiger Ewartungen. Dabei gefährdet oder zerstört nicht jede Information das Vertrauen. Die Vertrauensperson genießt einen gewissen Kredit, innerhalb dessen ungünstige Erfahrungen zurechtinterpretiert oder absorbiert werden können (vgl. Luhmann 1989). Vertraut man jemandem in bestimmten Grenzen, so verknüpft man damit bestimmte Ansprüche, deren Erfüllung auch die Erfüllung des auf die Person bezogenen Anspruchsniveaus bedeutet. In Beziehungen kann das Anspruchsniveau dynamisch angepaßt werden (vgl. Sauermann/Selten 1962).

Über Vertrauensbrüche, Sanktionen und Mißtrauen

Geht man davon aus, daß die Interaktionen in einer Gruppe freiwillig zustandekommen und die Fluktuation innerhalb der Gruppe nicht sehr hoch ist, dann läßt sich zwar durch einen Vertrauensbruch ein kurzfristiger Gewinn erzielen, es geht aber Vertrauenswürdigkeit verloren. Mit daraus folgenden „Interaktionsverlusten" kommt es oft auch zu einem Wohlstandsverlust und die Rückgewinnung des Vertrauens ist ein sehr langwieriger Prozeß (vgl. Offermanns 1990). Auf der Ebene des Systemvertrauens verkompliziert sich die Lage. Durch sogenannte Trittbrettfahrer, die die Systemstruktur für ihre Zwecke – aber ohne Leistungserbringung – nutzen, kann es dazu kommen, daß ehemals Vertrauende nicht mehr mit dem System in Kontakt treten. Den anderen Systemteilnehmern werden diese Trittbrettfahrer nicht immer bekannt. Deren Erkennen erfordert systeminterne Kontrollmechanismen; „das Vertrauen in die Funktionsfähigkeit des Systems schließt das Vertrauen in die Funktionsfähigkeit der immanenten Kontrollen ein" (Luhmann 1989, S. 65). Für entdeckte Trittbrettfahrer droht der Ausschluß aus der informellen Gruppe; dies hat in der Regel auch Konsequenzen für das persönliche Vertrauen.

Wie schon erwähnt, dient Vertrauen der Entlastung von sozialer Komplexität. „Wer [...] Vertrauen mißbrauchen will, muß seinerseits diese Komplexität übernehmen. Er muß so komplexe Verhaltensanforderungen auf sich laden, muß eine sehr weitreichende Beherrschung der relevanten Informationen und eine lückenlose Kontrolle der dem Vertrauenden zugänglichen Nachrichten sicherstellen, so daß er selbst Gefahr läuft, unter dem Druck der Komplexität zusammenzubrechen [...] Das Vertrauen zu rechtfertigen, ist in allen Dauerbeziehungen als Verhaltensregel einfacher, wenngleich diese Regel den Vertrauenden natürlich nicht gegen einzelne, überlegt plazierte, gut gesicherte Ausnahmen schützt" (Luhmann 1989, S. 70f.). In der Regel werden wir es also mit solchen gezielten Vertrauensbrüchen zu tun haben.

Der Einsatz von Sanktionen im Falle eines Vertrauensbruches bedingt üblicherweise deren Androhung und die Überzeugung des Gegenübers von der Verfügbarkeit der Sanktionsmittel. Mit der Selbstverpflichtung, die Drohung gegebenenfalls wahr zu machen, macht sich der Drohende berechenbar. Mit der Existenz von Sanktionsmöglichkeiten geht aber auch immer ein Stück „Vertrauen" verloren, man kann sich nicht mehr sicher sein, ob Gegenleistungen aufgrund des Vertrauens erfolgen oder aus Angst vor Sanktionen (vgl. Offermanns 1990). Ausgesprochene Drohungen kehren eine faktische oder fiktive Ungleichheit hervor, die jede Fiktion von Gemeinschaft und Egalität zerstört und kooperative Aspekte des Verhältnisses zurückdrängt (vgl. Paris/Sofsky 1987).

Die Weigerung, Vertrauen zu schenken, stellt für den Nicht-Vertrauenden die ursprüngliche Komplexität der Geschehensmöglichkeiten wieder her. Das Übermaß an Komplexität überfordert und macht ihn handlungsunfähig. „Wer nicht vertraut, muß daher, um überhaupt eine praktisch sinnvolle Situation definieren zu können, auf funktional äquivalente Strategien der Reduktion von Komplexität zurückgreifen. Er muß seine Erwartungen ins Negative zuspitzen, muß in bestimmten Hinsichten mißtrauisch werden" (Luhmann 1989, S. 78). In einer solchen Situation des Mißtrauens wird jedem Alles zugetraut. Für jede Handlungsweise des Anderen ist zu prüfen, ob sie einem selber schadet und in wessen Interesse der Betreffende agiert (vgl. Offermanns 1990).

Zu Sicherungsinfrastrukturen

Wir haben nun Vertrauen als eine grundlegend subjektive Leistung des Menschen zur Reduktion sozialer Komplexität bestimmt, und seine Funktionsweise analysiert. Wir wollen nun den Schritt in die Welt der offenen Netze wagen und beobachten, wie Telekommunikation in ihnen stattfindet, wie es sich dabei um die Begriffe Vertrauen und Verläßlichkeit verhält und welche Bedeutung Sicherungsinfrastrukturen aus diesem Blickwinkel zukommt.

Für Teilnehmer an der Telekommunikation in offenen Netzen entsteht eine besondere Form der Unsicherheit. Durch den Verlust vieler sozialer Kontrollmöglichkeiten sind sie gezwungen, medienspezifische Risiken einzugehen. Über den Einsatz von Verschlüsselungsverfahren kann ein Teilnehmer für die Vertraulichkeit und Integrität von Nachrichten sorgen, aber es besteht zunächst keine Kontrolle darüber, ob man in die vom Gegenüber angegebene Identität und die von ihm veranlaßten Transaktionen vertrauen kann. Wie läßt sich nun diese „Vertrauenslücke" (Hammer 1995) überwinden, sofern dies überhaupt geht? Für die Verkleinerung der Vertrauenslücke werden Vertrauensinstanzen – sogenannte vertrauenswürdige Dritte, Trust Center, Trusted Third Parties – als organisatorische Einheiten mit institutionellem

Charakter vorgeschlagen, die die Identität von Teilnehmern oder Leistungen garantieren sollen. Den gegenwärtigen Trends zufolge (z.B.: X.500, PEM, ...) werden Leistungen im Verbund von Vertrauensinstanzen erbracht, diese bilden dann die Sicherungsinfrastruktur.

Auf die Zusicherungen von Vertrauensinstanzen, die sowohl öffentlichen als auch privaten Charakter haben können, wird man sich aber nur verlassen, wenn man der jeweiligen organisatorischen, sozio-technischen Einheit vertraut. Durch ein Bündel technischer, organisatorischer und rechtlicher Maßnahmen müssen sich die Vertrauensinstanzen als vertrauenswürdig erweisen. Hammer stellt heraus, daß seitens der Teilnehmer Vertrauen durch (gute) Erfahrungen entsteht, aber auch durch rechtliche Rahmenbedingungen, wie etwa Zulassungs- und Aufsichtsverfahren, dies verschiebt das Problem aber nur, weil man nun denjenigen, die die Kontroll- und Prüfverfahren durchführen, vertrauen muß.

In ihrer Dissertation geht Birgit Klein auch auf den Aspekt des Vertrauens bei Authentifikationsdiensten ein (Klein 1993). Innerhalb von Sicherungsinfrastrukturen nehmen diese Authentifikationsdienste eine zentrale Stellung ein. Sie wendet dabei den Vertrauensbegriff auf die Beziehungen zwischen Rechnerinstanzen eines Netzwerkes an. „Das Vertrauen in eine Instanz beschreibt in der Informationstechnik das Überzeugtsein von den Fähigkeiten und der Zuverlässigkeit einer Instanz. Es stellt das Zutrauen dar, das einer Instanz entgegengebracht wird, daß sie einerseits gewillt und andererseits kompetent ist, ihre Aufgaben korrekt und zuverlässig zu bewältigen" (Klein 1993, S. 37). Diese Instanzen werden dann, und soweit können wir das auch nachvollziehen, im Hinblick auf die Erfüllung ihrer Aufgaben sehr differenziert betrachtet. Für den Aufbau vertraulicher und authentischer Kommunikation geht sie von der Existenz „vertrauenswürdiger" Server aus. Diese werden gegenüber der Institution, die sie betreibt, in den Vordergrund gerückt. Sie benennt sieben Aspekte von Vertrauen, die in Betracht kommen können, wenn Instanzen vertraulich (d. h. geheim) und authentisch kommunizieren wollen.

Neben der Identifikation von Instanzen – und damit sind im Kleinschen Sinne tatsächlich nur jeweils Rechnerknoten gemeint – der Schlüsselerzeugung, der Geheimhaltung, dem Nicht-Mißbrauch, der synchronisierten Zeitmessung, dem Einhalten von Protokollspezifikationen wird dort hauptsächlich auf die Frage nach den Empfehlungen anderer Instanzen eingegangen. Klein geht davon aus, daß in einem großen, verteilten Netz wohl kaum eine Instanz alle anderen Instanzen kennt und sich darum auch keine Meinung über deren „Vertrauenswürdigkeit" bilden kann. Instanzen sind deshalb auf „Einschätzungen" und „Empfehlungen" anderer Instanzen angewiesen.

Dabei hat Klein sehr gut die Problematik der Empfehlungen herausgearbeitet: „Instanzen müssen die Fähigkeiten und den 'Charakter' (gutwillig – böswillig) von anderen Instanzen einschätzen können und ihre Empfehlungen in Übereinstimmung damit abgeben. Sie dürfen keine falschen Annahmen über die Fähigkeiten der anderen treffen und auch nicht vorsätzlich eine nicht vertrauenswürdige Instanz als vertrauenswürdig empfehlen." (Klein 1993, S. 41) Dahinter steht auch die Problematik hierarchisch abgestufter Vertrauensinstanzen, von denen jede nur der übergeordneten und untergeordneten „vertrauen" muß. Es ist darüber hinaus auch ein komplexes Netzwerk von Nachbarschaftsbeziehungen denkbar, was die Sache gegenüber strengen Hierarchien komplizierter macht.

Problematisch ist, daß Klein den Vertrauensbegriff hauptsächlich für die Kommunikation zwischen Rechnerknoten, also für einen rein technischen Bereich, verwendet: „In großen Netzen ist ein Authentifikationsdienst über viele Instanzen, häufig Authentifiktionsserver (sic!) genannt, verteilt. Jeder Benutzer, jede Instanz ist mindestens einem Authentifikationsserver bekannt. An der Authentifikation zweier Instanzen in einem solchen Netz sind im allgemeinen mehrere Authentifiktionsserver (sic!) beteiligt. Es ist jedoch nicht unbedingt erforderlich, daß sich alle Server gegenseitig kennen. Authentifikationsserver können den ihnen bekannten Instanzen behilflich sein, sich zu authentifizieren, ohne daß sich die Authentifikationsserver direkt kennen." (Klein 1993, S. 8)

Mit der von uns gewünschten Unterscheidung spielt Vertrauen zwischen den Rechnern selbst gar keine Rolle. Genauer gesagt, haben in diesem Zusammenhang die oben ausgeführten Eigenschaften von Vertrauen keinen Entfaltungsraum. Hier geht es um technische Sicherheit bzw. Verläßlichkeit im Sinne von Security. Der Begriff des Vertrauens bedeutet in diesem Zusammenhang, ob die Betreiber eines Netzknotens denen eines anderen, mit dem sie in Verbindung treten, vertrauen. Sicherungsinfrastrukturen sind insofern Ausdruck eines inhärenten Mißtrauens und nicht wie man leicht denken könnte, Maßnahmenpakete zur Unterstützung von Vertrauen in der rechnervermittelten Kommunikation zwischen Menschen. Sie sind der Versuch einer Formalisierung und damit technischen Substitution von Vertrauen. Dabei kann nicht oft genug betont werden, daß kein Authentifikationsdienst ohne Vertrauen in die den Dienst zur Verfügung stellende Institution verwendet werden wird. Dahinter steht die Identität der Institution, die zugegebenermaßen ohne menschlische Beteiligung durch geeignete (hoffentlich verläßliche) Techniken und formale Kriterien überprüft werden kann.

Gestaltung

Eine der Kernfragen – von deren Beantwortung der Umgang mit Technik abhängt – ist, wie der Gestaltungsprozeß sich aus der Sicht der von der Systemeinführung Betroffenen darstellt. Das spaltet sich in zwei Bereiche auf: Die Vertrauenswürdigkeit der Konstrukteure, die als Experten für ein verläßliches System verantwortlich sind, und die Verläßlichkeit der Umstände, was sowohl die Einführung durch die *Systempromotoren* als auch den späteren Gebrauch betrifft. In diesem Zusammenhang verstehen wir unter Systempromotoren den Personenkreis, der die Einführung eines Systems fordert und fördert, aber die technische Realisation i.a. anderen überläßt.

Beim Teilbereich der Konstruktion handelt sich sich insbesondere bei großen technischen Systemen letzten Endes um das wohlbekannte Laien-Experten-Spannungsfeld. Damit wird die Frage der Verläßlichkeit zum Teil darauf abgebildet, ob die beauftragten Experten genügend Kompetenz vorweisen können. An dieser Stelle kommen auch gesellschaftliche Vorgaben ins Spiel, wie Ausbildungssysteme, Gesetzesvorgaben, Technische Überwachungsver-

eine (TÜV), aber auch die technische Normierung (DIN, ISO usw. – Wagner schlägt „technische Normierung als eine Institution der gesellschaftlichen 'Unsicherheitsabsorption'" vor (Wagner 1992, S. 18)). Andererseits heißt das aber auch, daß für so viel Transparenz über das Innere des Systems gesorgt werden muß, daß den Betroffenen insofern ein Grundverständnis von der jeweiligen Technik vermittelt werden kann, daß sie nicht blind auf das Funktionieren und die guten Absichten der Entwicklerinnen vertrauen müssen. Diese Problematik betrifft übrigens sowohl rein Betroffene, als auch Systempromotoren, die die Einführung eines Systems in ihrem eigenen Interesse vorantreiben.

Letztere sind allerdings in einer privilegierten Position. Schließlich besitzen sie i.a. die Kontrolle über die Einführung. Das bedeutet, sie können sowohl die Spezifikationen, als auch den Vorgang der Einführung und die Rahmenbedingungen (wenn auch nicht notwendigerweise die Umstände) des Gebrauchs bestimmen. Somit werden sie aus Eigeninteresse dafür sorgen, daß die Konstruktion für ihre Zwecke verläßlich wird. Andererseits liegt es in ihrer Möglichkeit und Verantwortung, die später Betroffenen einzubeziehen. Nicht zuletzt, weil sie ihnen ihre eigenen guten Absichten glaubhaft machen müssen. Damit wird klar, daß die Verläßlichkeit der Technik eine Bringschuld der Promotoren ist, die sie nur teilweise auf die Konstrukteure übertragen können und ohne die sich Vertrauen zwischen den beteiligten Parteien nicht entwickeln kann.

Beispiel: EC-Karten

Am Beispiel der aktuellen Diskussion über Sicherheit oder Unsicherheit der PIN von Scheckkarten können die Tücken des Gestaltungsprozesses erläutert werden. Anfänglich galt die vierstellige PIN den Banken als sicher genug (wenn auch z.B. die Schweiz sechstellige verwendet). Das heißt, die Verläßlichkeit der Technik galt zumindest den Banken als ausreichend, und entsprechend traten sie auch nach außen auf. Die Kunden hatten, wenn überhaupt, mehr Probleme damit, sich mit Geldautomaten statt mit Menschen am Schalter auseinandersetzen zu müssen. Alles in allem aber ging die Einführung weitgehend reibungslos, weil sowohl Kunden als auch Banken in der Technologie Vorteile sahen. Zwischenzeitlich konnte also davon ausgegangen werden, daß sich alle Beteiligten daran gewöhnt haben.

Inzwischen ist die Situation eingetreten, daß durch verschiedene Störungen – vom Kartendiebstahl, erfolgreichen öffentlich gemachten Manipulationen, der (angeblichen) Entschlüsselung der PIN auf der Karte, bis zum tatsächlichen Mißbrauch durch Kunden – diese Technologie problematischer wurde. Die Banken vertrauten vor allem anfangs ihren Kunden nicht, warfen ihnen grundsätzlich Betrug vor, wenn es nach wirklichen oder vorgetäuschten Kartenverlusten noch zu Abhebungen kam. Umgekehrt verlassen die Kundinnen sich vermehrt nicht mehr auf das Sicherheitsversprechen der Banken, es kommt vermehrt zu Gerichtsverfahren, wobei die Rechtslage noch im unklaren bleibt. Dabei enden die Verfahren widersprüchlich. z.B. das OLG Hamm (Urteil vom 17. März 1997 – 31 U 72/96) erkennt zumindest Zweifel an der Sicherheit an, während das Amstgericht Hannover (Urteil vom 9. Mai 1997 – 567 C 9676/94) die in besonderem Maße bestehende Sicherheit anerkennt (näheres hierzu FAZ vom 14. Juni 1997, S. 9). Die anfangs vermutete Verläßlichkeit der (Magnet-) Kartentechnologie einerseits, der Banken andererseits wird damit zumindest immer wieder in Frage gestellt – und dementsprechend liegt hier zur Zeit eine Vertrauensstörung vor. Es sei betont, daß in erster Linie vor allem das Vertrauen in die Aussagen der Banken bezüglich der Sicherheit geringer wird. Die Antwort darauf, das ist schon angekündigt, wird eine neue Technologie sein, die Chipkarte. Nur dürfte es diesmal schwieriger sein, die Verläßlichkeit glaubwürdig darzustellen, zumal der Wechsel aus der Sicht der Kunden praktisch unsichtbar ist.

Resümee

Die beiden Beispiele – Sicherungsinfrastrukturen und EC-Karte – sollten gezeigt haben, was die Anwendung des Vertrauensbegriffes in verschiedenen Zusammenhängen bewirkt. Wer bereit ist, sein Vertrauen tatsächlich so komplexen technischen Systemen zu schenken, wie sie z.B. Sicherungsinfrastrukturen inhärent sein müssen, liefert sich damit einer Virtualisierung des Vertrauens aus. *„Virtuelles Vertrauen"* bedeutet, die beteiligten Menschen mitsamt ihrer Verantwortlichkeit zu vergessen.

Eine andere Gefahr ist der instrumentelle Gebrauch von Vertrauen. Nicht ohne Grund werben z.B. Banken mit Vertrauen, liefert sich doch der Kunde ihnen häufig tatsächlich zumindest finanziell aus. Dabei kann die Instrumentalisierung von Vertrauen durchaus auch gegen den ursprünglichen Zweck wirken. Das obige Beispiel zur PIN-Problematik mag dies aufzeigen: Je mehr Banken auf die Verläßlichkeit der Technologie pochen, und damit ihre Vertrauenswürdigkeit als Institution in die Waagschale werfen, desto mehr riskieren sie, diese zu verlieren, wenn sie das über die Grenzen des Nachvollziehbaren hinaus tun. Wenn nun der Instrumentalisierung des Vertrauens durch die (wie wir hoffentlich klar genug herausgearbeitet haben) falsche Verwendung des Begriffs im Zusammenhang mit Technik Vorschub geleistet wird, ist das problematisch. Die *„Währung Vertrauen"* wird inflationär und folglich wertlos. Am Ende bleibt die Gewöhnung an die Technik, aber nicht die Erkenntnis ihrer sozialen Eingebundenheit. Ein Ausweg mag die von von uns vorgeschlagene konsequente begriffliche Trennung von „Verläßlichkeit der Technik" und „Vertrauen zwischen Entwicklern, Betreibern und Betroffenen" sein.

Literatur

Brüggemann, Hans und Gerhardt-Häckl, Waltraud (Hrsg.): Verläßliche IT-Systeme, Proceedings der GI-Fachtagung VIS '95, Braunschweig/Wiesbaden, 1995

Hammer, Volker: Gateway „Vertrauensinstanz", in: Datenschutz und Datensicherheit, 10/95

Klein, Birgit: Authentifikationsdienste für sichere Informationssysteme, Dissertation, Universität Karlsruhe, 1993

Luhmann, Niklas: Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität, Stuttgart, 3. Auflage, 1989

Marhöfer, M.: Einführung in die Podiumsdiskussion „Vor welchen Risiken schützen uns verläßliche Informationssysteme?", in: Weck, Gerhard und Horster, Patrick (Hrsg.): Verläßliche Informationssysteme, Proceedings der GI-Fachtagung VIS '93, Braunschweig/Wiesbaden, 1993

Offermanns, Matthias: Bürokratie und Vertrauen, Baden-Baden, 1990

Paris, Rainer und Sofsky, Wolfgang: Drohungen. Über eine Methode der Interaktionsmacht, in: Kölner Zeitschrift für Soziologie und Sozialpsychologie 39, 1987

Sauermann, Heinz und Selten, Reinhard: Anspruchsanpassungstheorie der Unternehmung, in: Zeitschrift für die gesamte Staatswissenschaft 118, 1962

Wagner, Gerald: Vertrauen in Technik. Überlegungen zu einer Voraussetzung alltäglicher Technikverwendung, Bericht WZB FS II 92-503, Berlin, 1992

Gerhard Banse, Käthe Friedrich

Informationstechnik: Sicherheit und Beherrschbarkeit

Digitale Signaturen im Blickfeld der Geistes- und Sozialwissenschaften

Aus einem Prospekt von TeleTrusT Deutschland e.V.

Immer rasanter entwickelt sich die Informationstechnik. Briefe auf dem Postweg zu befördern wird bald nur noch im Privatbereich üblich sein, denn die elektronische Abwicklung der Kommunikation ist schnell, effizient und stets aktuell. Nicht nur allgemeine Informationen werden den Datennetzen anvertraut, sondern auch wichtige Verträge, gravierende Vereinbarungen und sogar Register, wie das Grundbuch, werden künftig elektronisch geführt. Immer dringender wird der Ruf nach mehr Sicherheit, also nach Vertraulichkeit und Verbindlichkeit. Wie wird ein Brief verbindlich? Durch die Unterschrift! Aber wie kann man einen elektronischen Brief unterschreiben?

Doch es gibt eine sichere Lösung der Unterschriftsproblematik: die digitale Signatur![1]

1. Die digitale Signatur als Voraussetzung der rechtsverbindlichen elektronischen Kommunikation erfordert die Rahmensetzung der Sicherungsinfrastrukturen,[2] welche den mehrseitigen Sicherheitserfordernissen in verteilten Netzen und offenen Netzen Rechnung tragen. Dieses Konzept der Projektgruppe verfassungsverträgliche Technikgestaltung (provet e.V.) hat sich in der Diskussion um das Signaturgesetz durchgesetzt. Das Konzept geht davon aus, daß die Voraussetzung der Verwendung digitaler Signaturen die Entwicklung von vertrauenswürdigen Sicherungsinfrastrukturen ist. Die Sicherungsinfrastrukturen liefern das „Handwerkszeug" für digitale Signaturen:[3]

a) einheitliche Verfahren, um die Interoperabilität sicherzustellen,

b) Gesetze, die die Rechtsverbindlichkeit elektronischer Kommunikationsregeln festlegen, und

c) übergeordnete Instanzen, die zentrale Aufgaben übernehmen (Zertifizierungsstellen, Verteilerstellen, Kartenhersteller usw.)

2. Die Diskussion um die Sicherheit in der Informationstechnik hat sich in den letzten Jahren auf folgende Schwerpunkte und Kriterien konzentiert: Vertraulichkeit, Integrität, Authentifikation und Identifikation sowie Verbindlichkeit, Zugriffskontrolle, Robustheit, Wiederverwendbarkeit in anderen Kontexten und Kompatibilität zum Umfeld. Digitale Signaturen bringen einerseits in diese generelle Debatte kaum wesentlich neue Momente ein. Digitale Signaturen verschärfen jedoch andererseits nicht nur einige Positionen (z. B. Schutz persönlicher Daten als Teil technischer Infrastrukturen selbst, rechtliche Situationen in der Datenübertragung), sondern fordern darüber hinaus in weitaus stärkerem Maße verbindliche und akzeptable Antworten bzw. Richtungen der Beantwortung sowie entsprechende Festlegungen. Signaturverfahren erweisen sich als die Basistechnologie des elektronischen Rechts- und Geschäftsverkehrs.

3. Sicherheit entsteht nicht nur aus Wissen und Einsichten, aus rationalen oder als rational bezeichneten Entscheidungen und transparenten Handlungen. Sicherheit entsteht auch aus einem intuitiven Verständnis, aus Erfahrungen und Erwartungen, aus Hoffnungen und Ängsten, aus erlebten Mitgestaltungsmöglichkeiten bei technischen Problemlösungsprozessen oder zumindest wahrgenommenen Eingriffsmöglichkeiten in technische Abläufe bzw. aus Ohnmachtsgefühlen angesichts einer scheinbaren Eigendynamik des Technischen. Auch in der Informationstechnik zeigt sich der subjektive Charakter der Sicherheit darin, daß häufig neben den angestrebten Vorteilen bzw. dem zu realisierenden Nutzen die als bedeutsam angesehenen Bedrohungen, Gefährdungen oder Schädigungen entweder als übermächtig angesehen bzw. gleichsam ausgeschlossen werden, womit das verbleibende Risiko nicht bzw. nicht vollständig erfaßt wird. Sicherheit hat so eine starke subjektive Komponente und ist damit auch (oder vorrangig?) kultureller und dynamischer Natur. Über das individuelle Sicherheitsbedürfnis und -verlangen hinaus haben verschiedene soziale Gruppen einen je unterschiedlichen kollektiven Umgang mit Unbestimmtheiten, Gefahren und Risiken der Technik entwickelt, der sich als Hindernis für eine gemeinsame, umfassende „Sicherheitskultur" erweisen könnte (wenn diese anzustreben überhaupt sinnvoll ist). Auch für Organisationen und Gesellschaften, die eine gemeinsame Netzwerkinfrastruktur bereitstellen, ist diese Subjektivität nicht bzw. kaum handhabbar und muß durch eine gesellschaftliche „Objektivität", d. h. durch einen Konsens oder eine globale Akzeptanz des mit der Nutzung verbundenen Risikos erweitert werden. Eine Lösung der mit den individuellen und subjektiven Sicherheitsbedürfnissen verbundenen Probleme kann nur in der Entwicklung von angemessenen Sicherheitskulturen liegen, die dem Spannungsfeld von individueller und gesellschaftlicher Integrität gerecht werden. Diese Forderung ist so jedoch (zu) abstrakt, sie bedarf unbedingt einer Untersetzung und Erweiterung („Konkretisierung") im Hinblick auf operationalisierbare Handlungs- und Verhaltensoptionen, ein Prozeß, der bisher nur sehr langsam

1. Als digitale Signatur im Sinne des Signaturgesetzes wird nur ein Kryptogramm verstanden, dessen öffentlicher Prüfschlüssel von einer lizensierten Zertifizierungsstelle zertifiziert worden ist. Diese bescheinigt in einem Zertifikat durch ihre digitale Signatur die organisatorische Zuordnung des öffentlichen Schlüssels zu einer bestimmten natürlichen Person.
2. Wir schließen uns dem Vorschlag von provet e.V. an, den Begriff Sicher*heits*infrastruktur durch den Begriff Siche*rungs*infrastruktur zu ersetzen, vgl.: Roßnagel, A.: Das Signaturgesetz. In: DuD 1997, S. 78.
3. Weitere Informationen zu digitalen Signaturen und Sicherungsinfrastrukturen sind enthalten in: Glade, Reimer, Struif 1995; DuD 1997.

und nur auf Einzelphänomene bezogen in Gang gekommen ist.

4. Ausdruck einer solchen sich entwickelnden Sicherheitskultur, bestehend aus vorgeschriebenen Sicherungsvorkehrungen, die organisatorische, personelle und technische Maßnahmen in einem konkreten sozialen oder institutionellen Umfeld umfassen, sind gesetzlich geregelte Vereinbarungen über Sicherungsinfrastrukturen. Akteure, die infolge dieser Sicherungsvorkehrungen die vielfältigen Möglichkeiten im Rechtsverkehr, im Bankbereich, bei den Grundbüchern, im Gesundheitswesen, bei Behörden, im Handel, in der Wirtschaft, im Versicherungswesen und in der Industrie anwenden wollen und sollen, sind gezwungen, sich über die vertrauenswürdige (weil akzeptable!) Variante zu einigen, welche zuerst national entwickelt, darüber hinaus jedoch global anwendbar und wirksam werden könnte.

5. Sicherer Datenaustausch ist im digitalen Zeitalter kein Selbstzweck. Zunächst ist er, wie TeleTrusT e.V. zeigt, „schnell, effizient und stets aktuell", sodann allerdings nicht einfach. Immerhin wird er als technisch möglich eingeschätzt, eine starke Kryptographie vorausgesetzt. Grundansicht bleibt aber unbedingt, daß die Informationstechnik ein sehr dynamisches, räumlich und zeitlich vernetztes System darstellt, für das keine zeitlosen und umfassenden objektiven Regeln in der erforderlichen Konkretion existieren, sondern daß der entsprechende Regelungsbedarf nicht immer nur wieder aufs Neue herausgefordert wird und zu überprüfen ist, sondern daß ihm auch mit zeitgemäßen Lösungen entsprochen werden muß. Dies wirft nochmals die Frage nach den Akteuren bzw. Akteursgruppen, den von ihnen formulierten bzw. zu berücksichtigenden Risiken und Gestaltungszielen sowie den vorhandenen bzw. den geforderten und damit zu schaffenden Gestaltungsmitteln auf. Sicherheit in der elektronischen Datenübermittlung und -verwaltung ist ohne Verschlüsselung von (allen oder ausgewählten) Daten nicht zu haben. Digitale Signaturen ermöglichen, die Unverfälschtheit eines elektronischen Dokuments zu erkennen und die Identität seines Ausstellers nachzuweisen. Ohne sie können Sender, Empfänger und Dritte elektronische Willenserklärungen spurlos verändern. Es ist unstrittig, daß diese digitalen Signaturen in wenigen Jahren eine bedeutende Rolle in der Informationstechnik spielen werden.

6. Die Diskussion zeigt aber auch, daß es nicht reicht, nur einfach die Technik dieser Verschlüsselung sowie ihrer Speicherung und Übertragung einzusetzen, sondern es kommt vielmehr maßgeblich auf das „Wie?" dieses Einsatzes an. Innovative Technikgestaltung muß, um gesellschaftlich akzeptabel, verfassungskonform und wirtschaftlich erfolgreich zu sein, den bekannten Kriterien genügen:

- Recht auf informationelle Selbstbestimmung.
- Nachvollziehbarkeit: Alle Aktionen sollen leicht kontrollierbar sein, damit ein Mißbrauch von Daten auch nachträglich entdeckt werden kann. Es muß auch von neutralen Instanzen geprüft werden können, wer wann welche Daten erzeugt, geändert, weitergegeben oder versandt hat.
- Bindewirkung und Anerkennung: Vereinbarungen, die mittels Informationstechnik getroffen werden, müssen rechtswirksam sein und gerichtlich durchgesetzt werden können.
- Gestaltbarkeit: Die Technik muß als Teil des gesellschaftlichen Prozesses auch von Anwendern bzw. Nutzern gestaltbar sein. Mögliche Gestaltbarkeitskriterien wie die Korrigierbarkeit bestimmter (Teil-)Funktionen oder die Nutzungskomplexität müssen dabei in Betracht gezogen werden.
- Wie sind die Kommunikationspartner nun auf den Austausch multimedialer Informationen vorbereitet? Erkennen sie die Echtheit eines Dokumentes? Können sie bearbeitete, weiterbearbeitete oder gefälschte Teile identifizieren? Damit entwickeln sich Vertrauen und Vertrauenswürdigkeit zu einem Schlüsselproblem. Bisher wurde der Person im Zusammenhang mit ihrer eigenhändigen Unterschrift vertraut (wobei es dafür etwa in unserer (!!) Kultur verschiedene Abstufungen gibt, z. B. „anonym" vollzogene eigenhändige Unterschrift, Unterschrift in Gegenwart beliebiger Zeugen, Unterschrift vor bevollmächtigten Personen, beglaubigte Unterschrift usw.; üblich sind auch Unterschrift „i.V." und „i.A."). Nun wird Vertrauen in ein Verfahren, das die Signatur erzeugt, und eine Technik, welche die Signatur überträgt und prüft, gefordert, um auf diese Weise die vorhandenen komplexen Vermittlungen und Beziehungen in handhabbarer Weise zu reduzieren, um den Umgang mit Neuem durch bewußte Ausblendung von Ungewißheit und Unbestimmtheit zu ermöglichen. Wichtige sicherheitsrelevante Beziehungen sind in der Abb. 1 zusammengefaßt.[4]

7. Damit sind dann zugleich vielfältige Fragen verbunden, die die kulturelle Dimension betreffen: Sind die Nutzer bzw. Betreiber entsprechender technischer Systeme imstande, Wirkungen von Manipulationen zu erkennen oder mit Fälschungen umzugehen? Wie weit können Gefährdungen von Menschen ausgeschlossen und ihre Unversehrtheit – einschließlich des Rechts auf informationelle Selbstbestimmung – garantiert werden? Sind die Nutzer bereit und in der Lage, die „Prozedur" des Umgangs mit der digitalen Signatur auf sich zu nehmen und den damit verbundenen Erfordernissen zu entsprechen?[5] Wie wird gesichert, daß die Unterschriften durch die „Listigkeit des Alltags" nicht „delegiert" werden (können)? Erweisen sich nicht gerade Irrtum, Neugier, Nachlässigkeit und Sorglosigkeit möglicherweise in diesem Zusammenhang als unterschätzte Risiken? Ist es möglich, Erfahrungsräume so zu organisieren, daß sie – auch unter Berücksichtigung des mentalen Beharrungsvermögens – zu echten Lernfeldern für potentielle Nutzer werden? Wie können Kompetenzen und Gestaltungen der Handlungsräume der einzelnen Bestandteile der Sicherungsinfrastruktur abgegrenzt und überschaubar gemacht werden?

8. Technologien werden bei der Innovation häufig als in „geschlossenen Welten" existierend gedacht – z. B. in einer technischen, in einer ökonomischen oder auch in einer ökologischen, in einer zeitlich auf die unmittelbare Nutzungs-

4. Die Abbildung ist in geringfügig veränderter Weise entnommen aus: Müller, G., Kohl, U.: Safercom – Datenschutz und Datensicherheit für verteilte Klinikanwendungen – Anwenderbericht. Freiburg 1993, S. 7.
5. Siehe näher hierzu den Beitrag: Kumbruck, Ch.: Welche Kultur braucht die digitale Signatur? Erster Erfahrungsbericht aus der Zukunft. In: BSI 1997a, S. 37–52.

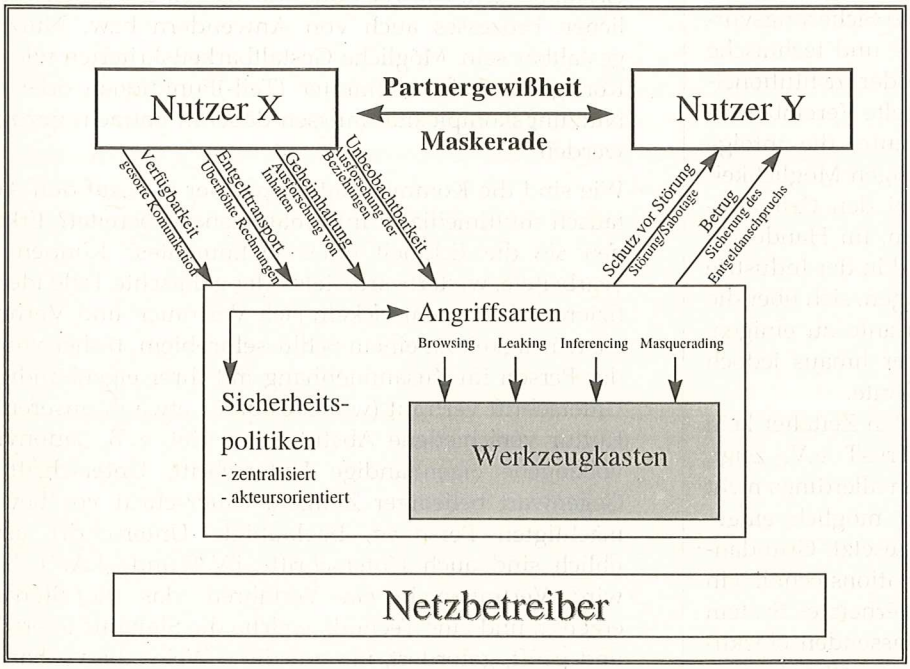


Abb. 1: Übersicht über wichtige sicherheitsrelevante Zusammenhänge[4]

dauer eingegrenzten oder nur ein eng definiertes Wirkungsspektrum einbeziehenden Welt. Damit werden – wie bereits erwähnt – häufig zwar Teil- oder Detailbereiche deutlich herausgehoben und einer weitergehenden wissenschaftlichen, politischen o. a. Betrachtung zugänglich gemacht, zugleich wird jedoch die lebensweltliche Vielfalt des Phänomens unbewußt vernachlässigt oder bewußt reduziert – ohne sich über die mit Vereinfachungen, Schematisierungen oder Ritualisierungen möglicherweise verbundenen Konsequenzen klar zu sein. Technikgenese als sozialen Prozeß zu gestalten, erfordert u. E. jedoch eine umfassende, „ganzheitliche" Betrachtung, vor allem im Hinblick auf individuelle, gesellschaftliche und kulturelle Kontexte bzw. Zusammenhänge, offen für neue Lösungen, offen für veränderte Gewichtungen bei veränderten Rahmenbedingungen („Kontexten") und offen vor allem für die Einbeziehung der potentiellen Nutzer.

9. Technikphilosophische Überlegungen zu den vielfältigen Probleme, die sich bei der Herstellung möglicher Sicherheit, bei der Beherrschbarkeit neuer technischer Lösungen und ihrer gesellschaftlichen Einbettung ergeben, sind vor allem Überlegungen, die ein einheitliches Herangehen auch an Informationstechnik provozieren und zum Konsens der Akteure beitragen können. Dazu gehört erstens die Betrachtung der Technik als soziotechnisches System. Auf diese Weise werden nicht nur die von Menschen gemachten Gegenstände („Artefakte") selbst interessant, sondern auch deren Entstehungs- und Verwendungszusammenhänge, die individuellen Handlungen und die institutionellen Bedingungen ihrer Hervorbringung und Nutzung. Beeinflußt werden diese wiederum von wissenschaftlich-technischen, ökonomischen, rechtlichen, politischen, (militärischen,) ökologischen und ethischen Faktoren. Dies zeigt die Technik in ihrer Entwicklung und Anwendung als auf das engste mit Wirtschaft, Gesellschaft, Politik und Kultur verflochten. Hinzu kommt zweitens die Berücksichtigung der Technikgenese (-entwicklung) als mehrstufiger Prozeß, als Abfolge sich wiederholender bewußter oder unbewußter Entscheidungen der Akteure zwischen verschiedenen Möglichkeiten der Gestaltung und Anwendung (Selektion). Und drittens gilt es, unterschiedliche Akteure in bezug auf informationstechnische Sicherheitslösungen (Entwickler, Hersteller, Vertreiber, Nutzer, „Angreifer") zu beachten. Hinzu kommen viertens die mit der Internationalisierung und Globalisierung verbundenen Probleme, die sich z. B. aus unterschiedlichen kulturell begründeten Werthaltungen oder unterschiedlichen rechtlichen Regelungen ergeben.

10. Herbert Kubicek stellte im Zusammenhang mit der Diskussion um Sicherheitskulturen fest, daß es nicht nur um die Sicherheit als Repräsentation von Objekten, sondern auch (oder vor allem?) um den Schutz von Informationen im Sinne der den Daten zugeordneten Bedeutungen geht. Auf der Grundlage dieser Prämisse sind nicht nur oder in erster Linie die Interessen der Betreiber von Systemen relevant, sondern vor allem der Schutz der Interessen all jener, die direkt oder indirekt von diesen technischen Lösungen betroffen sind. Insofern lautet unter dem zentralen Gesichtspunkt der Sicherheit kulturellen Beherrschbarkeit digitaler Signaturen u. E. eine (die?) zentrale Frage:

> *Wo sollte unter Sicherheits- und Beherrschbarkeitsaspekten aus humaner und kultureller Perspektive heute ganz auf den Einsatz von Informationstechniken verzichtet werden und welche Denkbemühungen bereits heute initiiert werden, damit morgen neuartige IT-Lösungen sozialverträglich und effektiv genutzt werden können?*

Weitere Literatur

BSI (Hrsg.) (1997a): Kulturelle Beherrschbarkeit digitaler Signaturen. Interdisziplinärer Diskurs zu querschnittlichen Fragen der IT-Sicherheit. Ingelheim 1997 (vor allem der Beitrag: Banse, G., Friedrich, K.: Sicherheit und kulturelle Beherrschbarkeit digitaler Signaturen – ein „ganzheitliches" Problem, S. 53–67).

BSI (Hrsg.) (1997b): Mit Sicherheit in die Informationsgesellschaft. 5. Deutscher IT-Sicherheitskongreß des BSI 1997. Ingelheim 1997 (vor allem der Beitrag: Banse, G.: Nichttechnisches in der IT-Sicherheit – Positionen und Probleme, S. 185–203).

DuD 1997: Thematisches Heft „Recht und Sicherheit in Informationsverarbeitung und Kommunikation" der Zeitschrift DuD Datenschutz und Datensicherheit, Heft 2/1997.

Glade, A., Reimer, H., Struif, B. (Hrsg.) (1995): Digitale Signatur & Sicherheitssensitive Anwendungen. Braunschweig, Wiesbaden 1995.

Annette Hillebrand, Franz Büllingen

Informations- und Telekommunikations-sicherheit in kleinen und mittleren Unternehmen

und die Bedeutung von Sicherungsinfrastrukturen

Die Frage der Sicherheit von Kommunikationsbeziehungen entwickelt sich immer mehr zu einer Schlüsselkategorie im Umgang mit Telekommunikationsdiensten. Die Integrität von Daten und Informationen und die Zugriffssicherheit gewinnen in dem Maße in der Informationsgesellschaft an Bedeutung, in dem personale Interaktion, Verwaltungsprozesse oder geschäftliche Transaktionen über offene Systeme durchgeführt werden. Die elektronische Geschäftsanbahnung, -abwicklung und -pflege über Netze wie das Internet wird von politischer Seite als Chance gewertet, Flexibilität und Wettbewerbsvorteile zu erringen sowie Standort- und Größennachteile auszugleichen.

Electronic Commerce

„Electronic Commerce" ist in Zukunft vor allem für kleine und mittlere Unternehmen ein wichtiger Wettbewerbsfaktor, so lautete das Credo der Bonner G7-Konferenz „Electronic Commerce" im April diesen Jahres. Von der EU veröffentlichte Schätzungen gehen davon aus, daß im Jahr 2000 über 200 Mio. Arbeitsplätze weltweit einen Internet-Anschluß haben, davon etwa 5% in Deutschland. Heute arbeiten bereits 98% der Großunternehmen in Europa mit dem Internet, aber nur 4% der KMU. In Deutschland sind es sogar nur 2–3%. Von den KMU stammen nicht einmal 6% der täglich 50. Mio. E-Mails europaweit. In Zukunft wird aber für mindestens zwei Drittel dieser Unternehmen die elektronische Geschäftsabwicklung überlebenswichtig, so das Resümee der Vorträge und Pressemitteilungen. Zum einen werden Lieferbeziehungen zu Großunternehmen in erster Linie online ablaufen. Zum anderen liegen die Vorteile für die KMU darin, daß Waren und Dienstleistungen kostengünstig weltweit und rund um die Uhr angeboten werden können. Benötigte Lagerkapazitäten schrumpfen, Vertragsabwicklung, Abrechnung, Wartung und Kundenbetreuung beschleunigen sich, die Integration der Logistik läßt die Transaktionskosten sinken.

Sicherheit in der Telekommunikation

In der Euphorie über die Chancen der Flexibilisierung und Effizienzsteigerung durch elektronische Geschäfte gerät aber leicht aus dem Blick, daß die intensive Nutzung der Telekommunikation auch Risiken in sich birgt. Der wirtschaftliche Erfolg von Unternehmen hängt zunehmend auch davon ab, inwieweit es gelingt, Datenbestände und Kommunikationsabläufe gegen Ausspähung, Manipulation und Verlust zu schützen. Schätzungen über die jährlichen Schäden durch „Computerkriminalität" sprechen von Milliardeneinbußen. Die Gewerkschaft der Polizei schätzt die jährlichen Kosten allein durch Ausspähung von Daten auf 20 Mrd. DM. Dabei spielt die Größe der Unternehmen eine untergeordnete Rolle. Daten, die für Dritte von Interesse sind, finden sich auch in kleinen Ingenieurbüros, High-Tech-Unternehmen oder in Kundenlisten von Händlern. Obwohl die Anzahl der Unternehmen, die regelmäßig Online-Dienste in Anspruch nehmen, Dienstleistungen über elektronische Netze anbieten oder Datenfernübertragung betreiben, steigt, ist bei der Mehrzahl ein Bewußtsein für die Risiken und Gefahren der Telekommunikation noch kaum entwickelt.

In regelmäßigen Befragungen zur Sicherheitssituation der Anwender, durchgeführt von der Fachzeitschrift KES, konnten Ansätze einer höheren Sensibilisierung für Sicherheitsfragen bei Großunternehmen festgestellt werden. Großunternehmen, d. h. Unternehmen mit über 1.000 Mitarbeitern, gelten aufgrund ihrer Finanzkraft, ihres Knowhows und ihrer personellen Kapazitäten an Datenverarbeitungs- und Telekommunikationsexperten bzw. Fachabteilungen als Vorreiter bei der Realisierung innovativer Sicherheitsanwendungen. Bei KMU dagegen sind überschneidende Funktions- und Aufgabenverteilungen, Schulungs- und Informationsdefizite sowie Kostenüberlegungen als Ursache für unzureichende Sicherheitsmaßnahmen zu vermuten. Wenn die Anzahl der KMU, die die Vorteile von Telekommunikationsdiensten und -anwendungen nutzen, in den nächsten Jahren merklich ansteigt, stellt sich die Frage, inwieweit diese Unternehmen schon heute für Sicherheitsbelange sensibilisiert sind und welche Trends für die Zukunft zu erwarten sind.[1]

Informations- und Telekommunikationssicherheit in KMU

Die Erhebung von Sicherheitsstandards in Unternehmen ist nicht unproblematisch – zum einen bleiben die meisten Sicherheitslücken unentdeckt und zum anderen werden Sicherheitsprobleme häufig nicht dem Management gemeldet. Darüber hinaus lassen sich Schäden nur schwer beziffern. Zum Beispiel sind Soft- und Hardwareschäden eher meßbar als Arbeitsausfälle und Imageverluste. Die Beurteilung von Risiken hängt zudem von vielfältigen subjektiven

1. Im Frühjahr 1996 beauftragte das Wissenschaftliche Institut für Kommunikationsdienste (WIK) das Unternehmen ExperTeam/Online Hanse mit der Durchführung einer empirischen Untersuchung zum Stand der Informations- und Telekommunikationssicherheit in KMU. Ziel der explorativen Studie war, mittels einer persönlichen Befragung der Geschäftsführung bzw. der IV-, IT- oder Organisationsleitung in 73 ausgewählten Unternehmen und in Expertengesprächen die Trends der Risikowahrnehmung und den Stand der Informations- und Telekommunikationssicherheit in KMU im Vergleich zu Großunternehmen vor dem Hintergrund zunehmender Risiken durch die steigende Nutzung von Telekommunikationsdiensten zu analysieren.

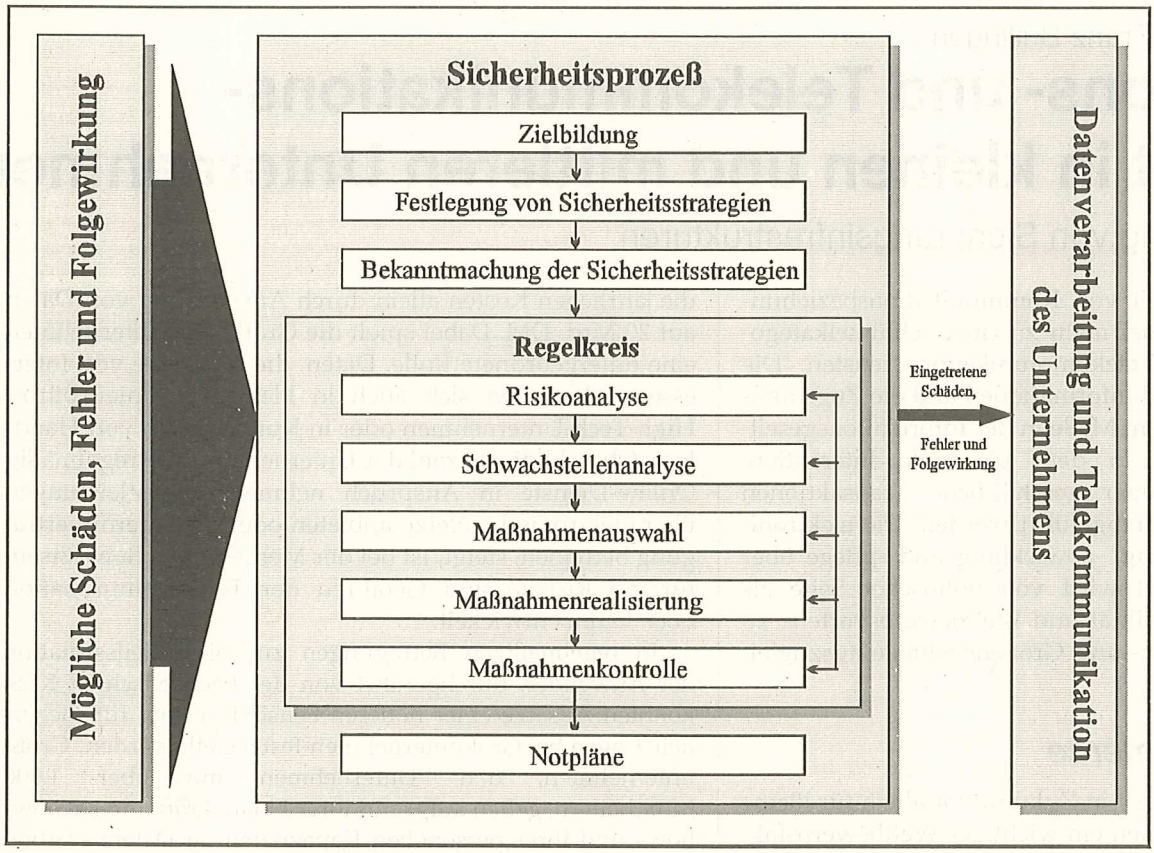


Abb. 1: Idealtypischer Sicherheitsprozeß im Unternehmen

Einschätzungen ab, die nicht immer der objektiv meßbaren Risikosituation entsprechen. KMU bewerten den Verlust von Daten und Informationen als „worst case" und nicht das Abhör- oder Manipulationsrisiko. Das Sicherheitsverständnis umfaßt vor allem technische Maßnahmen zum Schutz der zentralen und dezentralen Datenverarbeitung, Kommunikationsbeziehungen sind weit weniger geschützt. Während alle Unternehmen Maßnahmen zur Datensicherung ergreifen, zu über 90% Zugriffsrechte einschränken, in den meisten Fällen für Ausfälle der Hardware Ersatzlösungen vorhalten, und – wenn auch in geringerem Umfang – ihre dezentralen Systeme vor unbefugten Operationen schützen, finden sich nur in wenigen Unternehmen eine Firewall oder die Nutzung von Verschlüsselungsverfahren und digitalen Signaturen. Der Umgang mit Telekommunikationssicherheit im Unternehmen zeigt exemplarisch, welche Hürden bei der Implementation von Sicherheit in eine bestehende Organisationsstruktur auftreten. In der Regel werden nur diejenigen Techniken und Anwendungen als riskant betrachtet, die bereits zu Schäden geführt haben, und Maßnahmen werden erst dann ergriffen, wenn finanzielle Verluste aufgetreten sind. Die Risikowahrnehmung konzentriert sich in der Telekommunikationsnutzung in erster Linie auf bekannte Probleme wie Verlust von Daten und Informationen oder Hardwareausfälle. Scheinbar übertragen die Benutzer die ihnen vertrauten Risiken und potentiellen Schadenseintritte aus der Brief-, Telefon- und DV-Nutzung fälschlich auch auf Telekommunikationsanwendungen: Das Abhör- oder Manipulationsrisiko gilt allgemein als gering.

Diese Einschätzung zeigt sich auch in der Implementation von Sicherheitsstrategien. Eine Voraussetzung für die Erhöhung der Informations- und Telekommunikationssicherheit in KMU ist die Etablierung eines Sicherheitsprozesses (idealtypisch dargestellt in Abb. 1). Nicht einmal die Hälfte der KMU verfügt derzeit über Sicherheitsstrategien, während die in der KES-Studie 1996 befragten Unternehmen zu 90% Ziele sowie Grundsätze und Leitlinien zur Erhöhung der Sicherheit festgelegt haben. Nur zwei Drittel der KMU überprüft die Strategien, ein Viertel verzichtet darauf, diese ihren Mitarbeitern bekannt zu geben, obwohl dies eine essentielle Voraussetzung zur Sensibilisierung der Mitarbeiter für Sicherheitsfragen ist. Nicht einmal ein Fünftel der KMU hat bisher eine Risikoanalyse durchgeführt und diejenigen Unternehmen, bei denen eine solche Analyse vorgenommen wurde, konnten häufig deren Umfang und Überprüfung nicht spezifizieren.

Technische Maßnahmen überwiegen

Gegenwärtig und auch für die Zukunft werden technische Gefahren wie Hard- und Softwaredefekte sowie die eigene Belegschaft als bedeutendste Risikoquelle angesehen. In diesen Bereichen sollen in Zukunft verstärkt Anstrengungen getroffen werden. Dennoch wird die Erhöhung von Sicherheit weitgehend als ein Lösungsansatz verstanden, der durch den Einsatz von Technik, nicht aber durch organisatorische und personelle Maßnahmen verfolgt werden kann. Nur etwa ein Zehntel der KMU schulen ihre Belegschaft regelmäßig und wenn Schulungen durchgeführt werden, spielt die Weiterbildung von Sicherheitsexperten eine untergeordnete Rolle. Organisatorische und strukturelle TK-Sicherheitsmaßnahmen in Form von Informationssicherheitsbeauftragten oder Sicherheitsausschüssen bilden eher die Ausnahme. Wenn Informationssicherheitsbeauftragte vorhanden sind, wird ihre Funktion in erster Linie bei der Entscheidungsfindung und -vorbereitung und weniger im Bereich der Kontrolle und direkten Entscheidung gesehen.

Obwohl die befragten Unternehmen die eigenen Mitarbeiter als bedeutende Verursacher von Sicherheitsproblemen

einschätzen, sind nur geringfügige Erweiterungen im Bereich der Mitarbeiterschulung geplant. Für die Einstellung von Sicherheitsexperten sehen die Unternehmen wenig Bedarf. Auch bei der Umsetzung von Sicherheitskonzepten und bei ihrer Kontrolle erwarten sie keine größeren Hemmnisse. Es ist zu vermuten, daß in den KMU bisher kaum Anstrengungen zur Verbesserung der Informations- und Telekommunikationssicherheit geplant oder gar durchgeführt wurden, die aufwendige organisatorische Umstrukturierungen bzw. hohe Kosten zur Folge gehabt hätten. Vor diesem Hintergrund ist nicht überraschend, daß fehlende finanzielle Ressourcen von KMU nicht als große Behinderung bei der Erhöhung von Sicherheit angesehen werden.

Notwendigkeit der Implementation von Sicherheitsprozessen und Sicherungsinfrastrukturen

Die Ergebnisse der Studie zeigen, daß KMU derzeit den Herausforderungen einer „Risiko-Sicherheits-Spirale" noch kaum gewachsen sind: Um den immer ausgefeilteren Angriffsmöglichkeiten zu begegnen, müßten die Hürden zur Überwindung der Sicherheitssysteme schrittweise erhöht werden. Unkenntnis über Schutzmöglichkeiten und mangelndes Risikobewußtsein stehen dem zur Zeit noch entgegen und geben Anlaß zu der Befürchtung, daß KMU für die Zukunft nicht ausreichend gerüstet sind, wenn die Bedeutung von Electronic Commerce – auch mit Unterstützung staatlicher Förderprogramme – in dem Maße zunimmt, wie heute prognostiziert wird. Problematisch ist vor allem die zurückhaltende Implementation von organisatorischen und personellen Sicherheitsmaßnahmen zu bewerten. KMU benötigen im Zusammenhang mit der wachsenden Nutzung von Telekommunikation für die Erhöhung ihrer Sicherheit die Unterstützung von Dritten, sei es, daß von staatlicher Seite Regelungen für eine sichere TK-Infrastruktur oder für digitale Signaturen geschaffen werden oder daß Interessenvertretungen wie IHK und HWK eine Plattform für Informationsaustausch und Fortbildung bieten, und damit zu der konkreten organisatorischen Gestaltung eines kontinuierlichen Sicherheitsprozesses im Unternehmen beitragen.

Literatur

Hunnius G., KES-UTIMACO-Sicherheitsstudie 1996. So schätzen DV-Anwender ihre Sicherheit ein, in: KES/Zeitschrift für Kommunikations- und EDV-Sicherheit, Nr. 3, Juni 1996, S. 19–28 (Teil 1) und Nr. 4, August 1996, S. 22–27 (Teil 2)

Winkel, O., Büllingen, F., Sicherheit in der Telekommunikation – Soziale, institutionelle und organisatorische Voraussetzungen der Implementation von Sicherheit in telematischen Netzwerken, Wissenschaftliches Institut für Kommunikationsdienste, Diskussionsbeitrag Nr. 153, Bad Honnef, November 1995

Hillebrand, A./Büllingen F., Regelung elektronischer Unterschriften im IuKDG, in: WIK-Newsletter, Nr. 26, März 1997, S. 25–27

Hillebrand, A.; Büllingen, F., Dickoph, O.; Klinge, C., Informations- und Telekommunikationssicherheit in kleinen und mittleren Unternehmen, Wissenschaftliches Institut für Kommunikationsdienste, Diskussionsbeitrag Nr. 175, Bad Honnef, Juni 1997

Peter Pharow, Petra Wohlmacher

Health Professional Cards

Der Modellversuch in Magdeburg

Einleitung

Kaum ein anderer Bereich besitzt so mannigfaltige sensitive personenbezogene Daten wie das Gesundheits- und Sozialwesen. Medizinische oder allgemein Gesundheitsdaten sind Informationen, wie sie sensibler nicht sein können. Alle Daten dieses Bereiches unterliegen in ihrer Art der Datenhaltung, ihrer Gestaltung, Erhebung, Verarbeitung und der Kommunikationsform hohen Auflagen bezüglich Datenschutz und Datensicherheit. So müssen die Daten beispielsweise vor unbefugter Einsichtnahme geschützt werden – nicht umsonst gibt es den Begriff der „Ärztlichen Schweigepflicht". Würden sensible Daten erst einmal bekannt werden, wie beispielsweise Daten aus dem Umfeld einer Krebserkrankung, HIV-Infizierung oder Psychotherapie, können sie den Patienten heutzutage Arbeitsstelle und Existenz kosten. Aber auch Manipulationen der Daten müssen zweifelsfrei erkannt und nach Möglichkeit verhindert werden – werden beispielsweise Diagnosen oder Medikationen nicht korrekt übermittelt, dann sind die Folgen der sich daraus möglicherweise ergebenden Fehlbehandlung nicht abzuschätzen. Aber auch für den Mediziner entstehen zunehmend Konsequenzen aus der wachsenden Mündigkeit der Patienten.

Durch den zunehmenden Einsatz von moderner Informationstechnologie in allen Bereichen des Gesundheitswesens – bspw. steht die Einführung des deutschen Gesundheitsnetzes bevor – müssen die Auflagen bezüglich Datenschutz und Datensicherheit auf die Systeme der Informationstechnologie übertragen werden. Um die Anforderungen nach Vertraulichkeit, Authentizität und Integrität erfüllen zu können, müssen sowohl die nun in elektronischer Form vorliegenden Daten als auch die Datenkommunikation durch entsprechende Sicherheitsmaßnahmen geschützt werden. Hier kann die moderne Kryptographie in Verbindung mit dem Sicherheitswerkzeug Chipkarte und den im Bereich des Gesundheitswesens zu etablierenden Sicherungsinfrastrukturen ein großes Spektrum an Sicherheitsdiensten erbringen. Zur Bereitstellung und Gewährleistung der Sicherheit im Bereich des Gesundheitswesens sind bestimmte Dienste erforderlich, die von vertrauenswürdigen Instanzen ausgeübt werden müssen. Zu diesen Diensten zählen beispielsweise die Personalisierung von Chipkarten und ihre Ausgabe, Zertifizierung von kryptographischen Schlüsseln und beruflichen Qualifikationen, Verwaltung der Zertifikate sowie Zeitstempeldienste. Aus organisatorischen, rechtlichen und sicherheitstechnischen Gründen können diese Dienste nicht von einer einzigen Instanz erbracht werden. Hierzu sind viele Instanzen notwendig, die untereinander in Verbindung stehen, so daß sich eine komplette Infrastruktur – die Sicherungsinfrastruktur – ergibt, in der jede Institution ihren Teil zur Bereitstellung und Wahrung der Sicherheit wie Vertraulichkeit und Verbindlichkeit beiträgt.

Aufbauend auf früheren Projekten der EU wie dem „EuroCard"-Projekt und unter Berücksichtigung nationaler Aktivitäten z. B. des Arbeitskreises „Health Professional Card" der Arbeitsgemeinschaft „Karten im Gesundheitswesen" (Arbeitskreis Health Professional Card, 1996) in Deutschland wurde seit Januar 1996 innerhalb des europäischen Forschungsprojektes „TrustHealth 1" (Telematics Application Programme Project TrustHealth 1, 1996) eine Prozessorchipkarte mit Kryptocontroller für Berufstätige im Gesundheits- und Sozialwesen, die sogenannte „Health Professional Card (HPC)", und die dazu notwendigen Sicherungsinfrastrukturen spezifiziert. Mit der HPC soll sowohl Ärzten als auch allen anderen im medizinischen und angeschlossenen administrativen Bereich Beschäftigten ein elektronischer Berufsausweis in die Hand gegeben werden, mit dessen Hilfe alle Sicherheitsauflagen erfüllt werden können.

Die Anwendungsumgebung Tumorregister

Im Rahmen von TrustHealth 1 war neben der Spezifikation der Chipkarten und der erforderlichen Sicherungsinfrastrukturen auch die Umsetzung der Ergebnisse im Rahmen eines Modellversuches geplant. Als eine der ersten Erprobungsstätten in Deutschland wurde das Universitätsklinikum der Universität Magdeburg mit seinem „Regionalen Klinischen Tumorregister Magdeburg/Sachsen-Anhalt" als besonders geeignet ausgewählt; in Magdeburg ist seit Beginn der 90er Jahre ein modernes Krankenhausinformationssystem (KIS) in Client-Server-Architektur mit integriertem Krebsregister in Betrieb.

Das Tumorregister ist ein klinisches Dokumentationssystem, das alle für die Behandlung von Krebspatienten relevanten Daten von der Diagnose über die Therapie bis hin zur Nachsorge dokumentiert. Es stellt eine Form der elektronischen Krankenakte dar. Mit dem Tumorregister wird ein Einzugsgebiet von über 1,2 Millionen Einwohner im Norden und in der Mitte Sachsen-Anhalts abgedeckt; Daten von mehr als 50 Kliniken des Gebietes wie auch aus der Nachsorgeleitstelle der Kassenärztlichen Vereinigung, die die Krebsversorgung durch niedergelassene Ärzte und spezielle onkologische Praxen koordiniert, werden dort gespeichert. Mit Hilfe des Registers kann die Qualität der Krebsbehandlung durch fallbezogene Forschung und Weiterbildung über eine Zusammenarbeit und Kommunikation zwischen den einbezogenen Einrichtungen und Medizinern verbessert und gesichert werden. Hierbei ist die Aufnahme, Speicherung, Verarbeitung und Weitergabe der patientenbezogenen medizinischen Daten als besonders sensitive Informationen ein sowohl gesetzlich als auch ethisch sehr wichtiger Aspekt.

Auf einem Server ist die dem Tumorregister zugrundeliegende medizinische Anwendung „Giessener Tumordoku-

mentationssystem" (GTDS) installiert, ein System auf ORACLE-Basis, welches von der Universität Giessen entwickelt wurde. Bisher wird auf die Anwendung über Terminalemulation und Paßwortschutz zugegriffen. Die Authentifizierung der beteiligten Systeme und ihre vertrauliche Kommunikation wurden ermöglicht durch ein MACS (Modem Access Control System) für analoge Verbindungen sowie Kryptoguard LAN L3 Boxen für ISDN-Verbindungen zwischen dem sicheren Server und externen LAN-Systemen als geschlossenen Systemen. Die bisherige systemorientierte Sicherheitsarchitektur soll künftig durch den Einsatz der HPC in eine personen- und berufsorientierte Sicherungsinfrastruktur umgesetzt werden.

Mit der HPC kann der Berufstätige nun sowohl die Identität seiner Person als auch seine berufliche Qualifikation bzw. Position zweifelsfrei nachweisen. Diese Nachweise werden für die Zugriffskontrolle zur Datenbank und zu den medizinischen Daten verwendet. Darüber hinaus können mit den auf einer HPC gespeicherten Daten die Sicherheitsdienste Vertraulichkeit mittels Verschlüsselungsverfahren, Authentizität einer Kommunikation mittels Authentifizierungsverfahren, Authentizität und Integrität von Daten mittels digitaler Signaturverfahren erbracht werden (Wohlmacher, 1997). Die zwischen Client und Server übertragenen Datensätze können nun mittels der HPC signiert und verschlüsselt werden; die in der serverbasierten Datenbank abgelegten Daten werden zur Ursprungs- und Integritätssicherung später ebenfalls signiert.

Die Beteiligten

An der Vorbereitung, Ausrüstung und Durchführung des Magdeburger Modellversuches „HPC" sind neben der Abteilung Medizinische Informatik der Universität Magdeburg und dem Uniklinikum auch Partner aus Forschung und Industrie beteiligt. Hierzu zählen das GMD-Forschungszentrum Informationstechnik in Darmstadt und die Firma Giesecke & Devrient in München. Die einbezogenen Nutzer des Tumorregisters sind sowohl medizinische als auch nichtmedizinische Mitarbeiter, die den verschiedensten Kliniken und Instituten innerhalb, aber auch außerhalb des Uniklinikums angehören. Sie arbeiten als Arzt, Stationsschwester, medizinische Dokumentationsassistentin, Forscher, Entwickler oder Techniker.

Die Umsetzung

Die Umsetzung der Spezifikationen von TrustHealth 1 erwies sich zunächst als schwierig; viele der dort spezifizierten Schnittstellen lagen zum Startpunkt des Modellversuches lediglich auf Papier vor, was auch für die spezifizierten Chipkarten zutraf. Es war abzusehen, daß für den Modellversuch so schnell keine Produkte auf dem Markt verfügbar sein würden, die den Spezifikationen in allen Punkten entsprechen. Die aktuelle Situation am Markt zwang also zu Kompromissen.

Da im Rahmen des Modellversuches neben der technischen Komponente auch gesellschaftspolitische und organisatorische Aspekte (wie rechtliche Situation, Akzeptanz, Organisationsstrukturen, Infrastruktur, Einbeziehung existierender Institutionen, Szenario zur Erstellung und Ausgabe einer HPC etc.) betrachtet werden sollten, wurde und wird der Modellversuch bereits planungsseitig in zwei Phasen durchgeführt.

Für die erste Phase wurden zunächst die spezifizierten technischen und technologischen Voraussetzungen für die Durchführung des Modellversuches abgewandelt: Als HPC wurde eine auf dem Markt verfügbare Krypto-Co-Prozessorkarte verwendet, die der HPC-Spezifikation möglichst nahekam. Zehn solcher HPCs wurden an Ärzte und administratives Personal, welches das GTDS betreut, ausgegeben. Auch wurde die Sicherungsinfrastruktur noch nicht in ihrem spezifizierten Maß an Sicherheit realisiert. Diese Einschränkungen waren zum einen ökonomisch begründet (Kompromißlösungen), zum anderen konnte so aber trotzdem der weitaus wichtigere Teil, die angestrebten Funktionalitäten innerhalb der Sicherungsinfrastruktur, erprobt werden.

Nach Abschluß aller Tests und Versuche werden dann in der zweiten, noch durchzuführenden Phase, die als Übergang zur Nutzung der HPC im Routinebetrieb des Registers dient, die Mitarbeiter von Krankenhäusern und Kliniken des Bundeslandes Sachsen-Anhalt, die die medizinische Anwendung GTDS als Grundstein für eine verteilte elektronische Krankenakte nutzen, im Besitz einer HPC sein. Diese HPC und ihre Sicherungsinfrastruktur werden dann allen Spezifikationen genügen.

Neben der technischen Spezifikation und Umsetzung ergeben sich aber auch Fragen zu anderen Belangen: Was muß eine solche Karte samt Infrastruktur leisten, wie muß beides inhaltlich beschaffen sein, wie müssen die aufzubauenden Dienste aussehen? Wie groß ist die Akzeptanz seitens des Arztes, welchen Nutzen hat er davon, welche zusätzlichen Belastungen kommen eventuell auf ihn zu? Wie sieht das Verhältnis von Kosten und Nutzen aus, bezogen sowohl auf die Bereitstellung der Technik als auch auf den täglichen Betrieb? Für welche Anforderungen gibt es bereits etablierte Strukturen, wo sind sie in Vorbereitung, wo kann man noch Einfluß nehmen, was muß bei der Planung der Aktivitäten beachtet werden? Welche Standards existieren? Wo sind bereits jetzt bzw. in naher Zukunft rechtliche und ethische Grenzen gesetzt? Das sind die Fragen, auf die es allgemeingültige Antworten zu finden gilt. Dies wird Gegenstand einer weiteren Arbeit sein.

Die erste Phase diente vor allem auch dazu, die Institutionen des Gesundheitswesens für eine aktive Teilnahme an dieser Sicherungsinfrastruktur zu gewinnen (Telematics Application Programme Project TrustHealth 1, 1996). Da alle Daten über die berufliche Qualifikation und Position der Ärzteschaft bei den Ärztekammern liegen und die Ärztekammern für ihre Mitglieder eine Instanz des Vertrauens darstellen, wurde versucht, sie für eine Rolle bei der Realisierung der für die Sicherungsinfrastruktur notwendigen Instanzen (Autoritäten, engl. Authorities) zu gewinnen. Neben der Einrichtung und Etablierung von Autoritäten ist auch eine elektronische Umsetzung der bisher in Papierform vorliegenden Daten notwendig.

Im folgenden werden die für das Gesundheitswesen definierten Autoritäten und ihre gegenseitigen Beziehungen anhand eines Schemas kurz beschrieben (siehe Abbildung 1). Eine weitaus umfangreichere Darstellung und eine Erläuterung der einzelnen Funktionalitäten einschließlich eines Glossars findet sich in Farroukh et al., 1996.

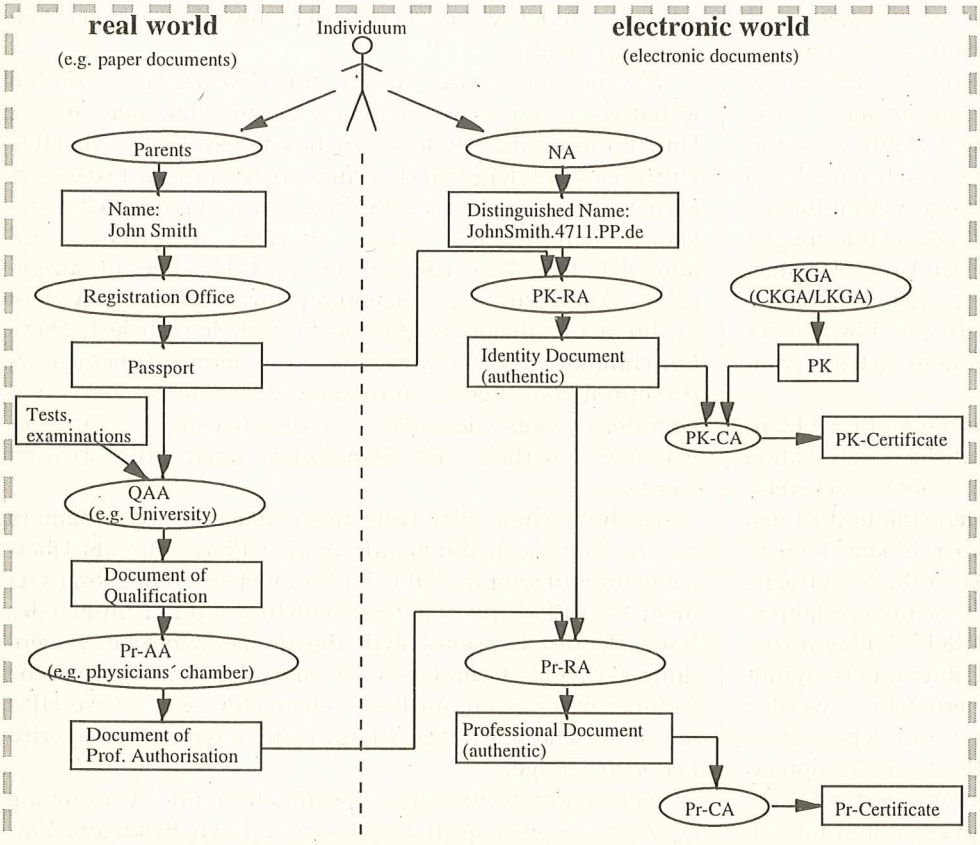


Abbildung 1: Autoritäten zur Erzeugung von Zertifikaten

Auf der linken Seite sind die für ein „Individuum" zuständigen Autoritäten der „realen", d. h. für uns greifbaren Welt, dargestellt. Auf der rechten Seite sind die Autoritäten der „elektronischen Welt", der Welt der Bits und Bytes, abgebildet. Die in der elektronischen Welt aufgeführten Autoritäten sind Komponenten einer Trusted Third Party. Über Schnittstellen werden die notwendigen Informationen aus der realen Welt an die elektronische Welt übermittelt. Mit diesen Informationen werden authentische Zusammenhänge zwischen einem Individuum und seinem öffentlichen Schlüssel (PK-Zertifikat) sowie zwischen einem Individuum und seiner Profession (Pr-Zertifikat) hergestellt, die für die zu erbringenden Sicherheitsdienste benötigt werden. Zwei der aufgeführten Autoritäten sind beispielsweise die Universität und die Landesärztekammer, die hier die vertrauenswürdigen Instanzen in der realen, in Zukunft aber auch in der elektronischen Welt darstellen. Sie können dann z. B. sowohl als Autorität zur Vergabe eindeutiger Namen innerhalb der elektronischen Welt (Naming Authority, NA) und zur Registrierung identitäts- und berufsbezogener Daten (Registration Authorities, PK-RA und Pr-RA) als auch als Autorität zur Erstellung von Zertifikaten (Certification Authorities, PK-CA und Pr-CA) agieren.

In der ersten Phase des Modellversuchs wurde die Ärztekammer des Landes Sachsen-Anhalt als Autorität (Pr-AA) eingesetzt. Die Ärzte und das administrative Personal stellten beim Tumorzentrum auf einem Papierformular einen Antrag auf ihre HPC. Die Anträge wurden von dort an die GMD weitergeleitet, die alle Autoritäten in der elektronischen Welt übernahm. Die personalisierten Chipkarten wurden von der GMD an das Tumorregister ausgehändigt, das die HPCs dann an alle Antragsteller ausgab.

Ausblick

Das EU-Projekt Trusthealth 1 wurde Juli 1997 erfolgreich abgeschlossen, einige Mitglieder des Konsortiums des Projektes TrustHealth 1 sind dabei, die dort spezifizierten Lösungen in Standards einzubringen (ISO, CEN). Während dieser Prozesse sowie anderer Projektaktivitäten ist es möglich, daß sich weitere gute Ideen ergeben, die dann die exakte Planung und Realisierung der zweiten Phase des Modellversuches beeinflussen werden. Darüber hinaus dienen die Ergebnisse von TrustHealth 1 mehreren europäischen Projekten als Vorlage bzw. als Anregung.

Das Nachfolgeprojekt „TrustHealth 2" ist bereits initiiert und von der europäischen Kommission bestätigt. TrustHealth 2 hat den großflächigen Einsatz der Ergebnisse von TrustHealth 1, also auch der dort spezifizierten HPC sowie der Sicherungsinfrastruktur, zum Inhalt. Parallel dazu läuft in Magdeburg auch die zweite Phase des Modellversuches, die aber über den Umfang der in TrustHealth 2 spezifizierten Anforderungen hinausgehen wird. Innerhalb von TrustHealth 2 wird das Universitätsklinikum Magdeburg als einer der Hauptpartner und als Koordinator für die deutschen Teilnehmer agieren. Der Start des Projektes wird für Ende diesen Jahres erwartet.

Bis dahin ist es natürlich einerseits möglich, sich an den beachtlichen Ergebnisse der getanen Arbeit zu erfreuen – oder aber bereits nächste Schritte in die vorgezeichnete Richtung zu gehen. Denn nicht die Spezifizierung von Schnittstellen allein ist es, die eine schnelle und gute Etablierung einer Sicherungsinfrastruktur bewirkt, sondern die Einbindung der existierenden Instanzen und Institutionen mit ihren bestehenden Beziehungen – und zwar derart, daß sie unter den heutigen und künftigen Nutzern dieser Infrastruktur eine hohe Akzeptanz verbunden mit einem hohen Maß an Vertrauen finden.

Literatur

Arbeitskreis Health Professional Card: *Deutscher Modellversuch – Health Professional Card.* Arbeitspapier der Arbeitsgemeinschaft Karten im Gesundheitswesen, Universität Göttingen, Göttingen, Oktober 1996

Farroukh, Hamid; Herbst, Marion; Pharow, Peter; Wenzlaff, Paul; Wohlmacher, Petra: *Die Deutschen Empfehlungen.* Arbeitspapier des Arbeitskreises 5M, Universität Göttingen, Göttingen, 1996

Telematics Applications Programme Project TrustHealth 1 (Trustworthy Health Telematics): *Functional Specification of TTP Services; Deliverable D 4.1.;* Brüssel 1996; http://www.ehto.be/projects/trusthealth/

Telematics Application Programme, Project TrustHealth 1 (Trustworthy Health Telematics): Peter Pharow, Petra Wohlmacher: *Progress Report of the German Site; Part of Deliverable D 4.4.;* Brüssel 1997; http://www.ehto.be/projects/trusthealth/

Wohlmacher, Petra: *Die Sicherheitsdienstleistungen von Health Professional Cards.* In: Proceedings des 5. IT-Sicherheitskongresses, Bonn, 28.–30.4.1997

Das Ladenburger Kolleg

Mehrseitige Sicherheit

Nutzer stärken, Anwendungen ermöglichen

„Sicherheit in der Kommunikationstechnik"

Die neuen Informations- und Kommunikationstechniken führen zu großen Veränderungen für den Einzelnen wie für die Gesellschaft insgesamt. Welcher Art diese Veränderungen sein werden, ist aber immer noch weitgehend unklar. Aus diesem Grund fördert die gemeinnützige Gottlieb Daimler- und Karl Benz-Stiftung (Ladenburg) das interdisziplinäre Kolleg „Sicherheit in der Kommunikationstechnik", das von Prof. Dr. Günter Müller (Gründungsdirektor des Instituts für Informatik und Gesellschaft der Universität Freiburg) geleitet wird.

Seit 1993 arbeiten Teilnehmer aus Hochschulen, öffentlichen und privaten Forschungseinrichtungen sowie führenden Unternehmen der Branche an Untersuchungen zu folgenden Fragestellungen:

- Welche Sicherheit brauchen Telekommunikationsnutzer in welcher Situation?
- Wie kann diese möglichst kostensparend realisiert werden?
- Welche Auswirkungen ergeben sich für das gesellschaftliche und wirtschaftliche Umfeld?

Schwerpunkt der Arbeit sind Methoden und Verfahren, die helfen sollen, daß Menschen berechtigtes Vertrauen zu der entstehenden Infrastrukturtechnologie „Informationsbahnen" finden können.

Computer verändern unsere Kommunikationsgewohnheiten

Computergestützte Telekommunikation bestimmt zunehmend Arbeitswelt und Privatleben: Der Austausch von Konstruktions- oder Produktionsdaten zwischen Unternehmen basiert genauso wie die Internet-Recherche von Privatpersonen auf computergestützter Telekommunikation. Selbst der schon „klassisch" anmutende Telefonanruf von „Mensch zu Mensch" wird durch Rechner technisch gestützt und vermittelt.

Zwar ist der Begriff „Datenautobahn" irreführend, aber an einer Stelle trifft der Vergleich: Unsere Gesellschaft ist, wie auf begeh- und befahrbare Straßen, auf die Telekommunikationsinfrastruktur angewiesen, und niemand kann sich ihr tatsächlich entziehen.

Kommunikation braucht Sicherheit

Unsere Lebenswelt, unsere „Wirklichkeit" bietet uns Schutz- und Freiräume. Auch in der virtuellen Welt, die durch den Austausch von Daten und Informationen über „Infobahnen" entsteht, haben Teilnehmer einen Schutzanspruch, selbst wenn dieser dort ganz anders aussehen wird.

Schutz- und Freiräume in der Telekommunikation setzen speziell die Sicherheit der dafür eingesetzten Kommunikationstechnik voraus. Deshalb sind für eine nachhaltige Nutzung der „Infobahnen" vor allem vier grundlegende Voraussetzungen zu beachten:

- *Vertraulichkeit*: Nachrichten wie beispielsweise Krankenakten, neueste Forschungsergebnisse oder Kontostände sollten nur den rechtmäßigen Empfängern bekannt werden und nicht beliebigen Personen. Bei Telefongesprächen ist oft schon der Name des Anrufenden schutzwürdig, etwa bei einem Gespräch mit der AIDS-Beratung.
- *Integrität*: Nachrichten, etwa die an einem Krankenhaus übermittelten Laborergebnisse oder Vertragsformulare, dürfen nicht unbemerkt verändert werden können.
- *Zurechenbarkeit*: Viele Nachrichten, etwa Bestellungen, müssen eindeutig einem Absender zugeordnet werden können, damit die Verantwortlichkeit klar ist.
- *Verfügbarkeit*: Die Sicherheit der Personen, die von Daten, etwa Krankenakten, abhängt, ist beeinträchtigt, wenn keine Verbindungen aufgebaut werden können.

Mehrseitige Sicherheit ist nutzerorientiert

Mehrseitige Sicherheit bedeutet, daß nicht nur die Sicherheit einer der an der Kommunikation beteiligten Parteien berücksichtigt wird. Dies gilt für Diensteanbieter, Netzbetreiber, aber auch für Teilnehmer bzw. Nutzer. Wichtig sind insbesondere der Schutz und die Stärkung der Nutzer, damit ernsthafte – etwa kommerzielle – Anwendungen überhaupt realisierbar sind. Der Einkauf via Internet ist problematisch, wenn man einerseits keine Kontrolle mehr über seine Finanzen hat und andererseits Einkäufe von anderen kontrolliert werden können.

Die Ansätze des Kollegs

Während der technische Fortschritt stark durch wirtschaftliche Faktoren bestimmt wird, ist der gesellschaftliche Fortschritt ein Ergebnis der Ausbalancierung gesellschaftlicher Kräfte. Drei Leitgedanken bestimmen deshalb die Arbeit des Kollegs:

1. Fortschritte auf dem Gebiet „Sicherheit in der Kommunikationstechnik" sind nur durch eine disziplin-

nenübergreifende Zusammenarbeit erreichbar, denn Sicherheit im umfassenden Sinne kann nicht durch technischen Fortschritt allein erreicht werden.

2. Für das technisch nicht vollständig erfaßbare Umfeld müssen gesetzliche und gesellschaftliche Übereinkommen greifen.
3. Ein Technikmoratorium im Bereich der persönlichen Sicherheit ignoriert die technische Entwicklung im Weltmaßstab, ebenso wie eine reine Technikorientierung den zivilisatorischen Konsens aufkündigen und damit die Zukunft der Gesellschaft (etwa durch Vorentscheidungen und nachfolgende Sachzwänge) gefährden kann.

Das Kolleg will das Bewußtsein für die interdisziplinäre Aufgabe „Sicherheit" wecken und die Benutzungsanforderungen in systematischer Weise erheben. Eine frühzeitige Konfrontation dieser Anforderungen mit der technischen Realität und die Umsetzung der dabei gesammelten Erkenntnisse können Akzeptanz wie Akzeptabilität neuer Kommunikationssysteme fördern.

Bei der technischen Realisierung mehrseitiger Sicherheit verfolgt das Kolleg vor allem zwei Ansätze:

- *Datensparsamkeit*: Je weniger Daten vorhanden sind, um so weniger Daten müssen aufwendig geschützt werden. Häufig lassen sich Kommunikationsdienste und Leistungsmerkmale, etwa die technische Erreichbarkeit bei der Mobilkommunikation, auch mit weniger Daten, als bislang verwendet, realisieren.
- *Dezentralisierung*: Werden Daten erhoben und gesammelt, sollten sie auf mehrere Instanzen verteilt werden. Auf diese Weise läßt sich das Risiko des Mißbrauchs reduzieren. Werden beispielsweise Girokontodaten und Telekommunikationsrechnungen bei verschiedenen Stellen gespeichert, lassen sich diese Daten weniger leicht zu Profilen verknüpfen. Ähnliches gilt für die Aufenthalts- und Kommunikationsdaten von Mobilfunkteilnehmern, die statt zentral besser dezentral oder in einer vertrauenswürdigen Umgebung der jeweiligen Nutzer gespeichert werden.

Projekte und Ergebnisse des Kollegs

Die Projekte des Kollegs lassen sich in drei Arbeitsfelder einordnen:

1. Warum mehrseitige Sicherheit für Vertrauen auf den „Infobahnen" nötig ist;
2. Mit welcher Technik mehrseitige Sicherheit ermöglicht werden kann;
3. Wichtige Rahmenbedingungen und Methoden.

1. Mehrseitige Sicherheit – eine Nutzerforderung

Wie psychologische Untersuchungen des Kollegs ergeben haben, nehmen Nutzer ihre Sicherheitsanforderungen oft nur verzögert wahr. Allerdings wird der Sicherheit dann eine um so höhere Priorität eingeräumt. Insbesondere befürchten die Nutzer, daß sie den Einfluß auf die sie betreffenden Kommunikations- und Datenverarbeitungsvorgänge im Netz verlieren könnten (sog. „Kontrollverlust").

Auf diese Befürchtungen antwortet das Konzept der „mehrseitigen Sicherheit" mit dem Schutz aller an der Kommunikation Beteiligten. Im Vordergrund steht dabei der Schutz der Nutzer. Untersuchungen der Kommunikation im Gesundheitswesen haben eindrucksvoll gezeigt, welche Bedeutung der mehrseitigen Sicherheit zukommt. Die Anonymität z.B. in der AIDS-Beratung muß ebenso garantiert werden können wie die Vertraulichkeit und Authentizität beim Austausch psychologischer Untersuchungs-ergebnisse. Im kommerziellen Bereich bestehen vergleichbare Anforderungen an die Sicherheit, etwa wenn im Internet mit elektronischem Geld bezahlt wird.

2. Technik für mehrseitige Sicherheit

Technik allein kann mehrseitige Sicherheit zwar nicht garantieren, sie ist jedoch eine wichtige Voraussetzung dafür. An welchen Stellen dabei angesetzt werden muß, zeigen die folgenden Beispiele einer „Technik für mehrseitige Sicherheit":

Erreichbarkeitsmanagement: lästige oder wichtige Anrufe?

Das Projekte „Erreichbarkeitsmanager" zeigt, wie gesteigerte Nutzersouveränität zu mehr Sicherheit und Akzeptanz führen kann. Belästigende Anrufe werden verhindert: trotzdem werden Anrufer nicht unbedingt gezwungen, ihre Rufnummer preiszugeben, sondern können z.B. die Dringlichkeit ihres Anrufs anonym signalisieren. Entwickelt wird ein Erreichbarkeitsmanagement auf der Basis von Newton Message-Pads und die zugehörigen Konfigurationsmöglichkeiten, die plattformunabhängig in HTML realisiert sind. Die Demonstratoren setzen auf GSM und ISDN auf.

Kommunikation ohne Datenspuren

Nutzer der neuen digitalen Kommunikationsnetze werden immer stärker durch die Möglichkeit von Kommunikations- und Bewegungsprofilen beunruhigt. Innovative und datensparsame Verbindungsaufbauprotokolle vermeiden bzw. reduzieren diese Gefahr. Entwickelt werden im Kolleg u.a. rechnergestützte Animationen und Simulationen der neuen Protokolle, die ihre Leistungsfähigkeit und den benötigten Aufwand erkennen lassen.

Vertrauensgewinn durch dezentralisierte Netzfunktionen

Viele Nutzer befürchten die zunehmende Abhängigkeit von Kommunikationsdiensten und den gleichzeitigen Verlust der Kontrolle über diese Dienste. Die Dezentralisierung von Vertrauensinstanzen und sensitiven Daten in

Kommunikationsnetzen reduziert das Risiko des Mißbrauchs. Zudem haben Nutzer die Möglichkeit, die Instanzen, denen sie vertrauen, selbst auszuwählen. Dazu sind jedoch Anpassungen der Netz- und Dienstestruktur erforderlich. Rechnergestützte Simulationen innovativer Protokolle und Topologien ermöglichen eine Abschätzung des nötigen Aufwandes.

3. Wichtige Rahmenbedingungen und Methoden

Der Schutz von Kommunikation mittels Technik kann nur in einem geeigneten politischen und organisatorischen Rahmen wirksam werden. Dazu werden die technischen (Nicht-)Auswirkungen und die unerwünschten Folgen der gegenwärtig diskutierten Kryptoreglementierung exemplarisch aufgezeigt. Eine Methode, schon während der Technikentwicklung Anwendungs- und Praxiserfahrung zu gewinnen, ist die im Kolleg vorbereitete Simulationsstudie.

Kryptographie – Fördern statt Reglementieren

Für sichere Kommunikation ist Verschlüsselung unter Kontrolle der Nutzer unentbehrlich. Als hinderlich und obsolet erweisen sich dabei immer mehr die teilweise noch aus den Zeiten des „Kalten Krieges" stammenden Reglementierungen. Sie taugen auch nicht zur Bekämpfung der organisierten Kriminalität. In harmlosen und unverdächtigen Daten (etwa Multimediadaten, Videokonferenzübertragungen oder gesprochener Sprache) lassen sich geheime Informationen verstecken und übertragen, ohne daß Außenstehende, etwa Strafverfolgungsbehörden, eine Chance haben, dies überhaupt zu bemerken. Mit Hilfe einer Kryptoreglementierung Entscheidendes zur Verbrechensbekämpfung beitragen zu können, ist vor diesem Hintergrund illusionär.

Im Gegenteil: eine Kryptoreglementierung schwächt den dringend nötigen Schutz der Kommunikation von Unternehmen und Privatleuten und unterstützt eher die, die sie bekämpfen sollte: kriminelle Interessen. Ein mangelhafter Schutz der Kommunikation sensibler und wichtiger Daten macht Unternehmen und Privatleute leicht zu Opfern von Erpressung oder verbrecherischen Manipulationen (z.B. Kreditkartenbetrug).

Erforderlich ist deshalb keine Beschränkung bzw. Reglementierung, sondern eine Förderung des Einsatzes kryptographischer Verfahren. Hierzu zählen die Grundversorgung und die längst überfällige internationale Normung.

Simulationsstudien als Praxistests

Die Entwicklung mehrseitig sicherer Kommunikationstechnik setzt Methoden voraus, die die Technikentwicklung und Praxiserprobung eng miteinander verknüpfen. Deshalb erprobt das Kolleg den Erreichbarkeitsmanager in einer „Simulationsstudie" im Gesundheitswesen. Echte Anwender werden mit prototypischer Technik und realitätsnahen Situationen aus ihrem Arbeitsalltag konfrontiert. Auf diese Weise können mit begrenztem Zeit- und Geldaufwand realitätsnahe Erfahrungen gesammelt werden.

Das Ladenburger Kolleg: Prof. Dr. Günter Müller (Leitung)
Dipl.-Inform. Kai Rannenberg (Koordination),Abteilung Telematik
Institut für Informatik und Gesellschaft, Universität Freiburg
Friedrichstraße 50
D-79098 Freiburg
Telefon:+49-761-203-4964
Telefax:+49-761-203-4929
E-Mail:kolleg@iig.uni-freiburg.de
WWW:http://www.iig.uni-freiburg.de/dbskolleg

Literatur

Günter Müller, Herbert Bunz (Hg.): Sicherheit in der Kommunikationstechnik (Themenheft); Informationstechnik und Technische Informatik (it+ti), 38/4 (August 1996)

Günter Müller, Andreas Pfitzmann (Hg.): Mehrseitige Sicherheit in der Kommunikationstechnik; Addison-Wesley; ISBN 3-8273-1116-0; im Erscheinen

Kai Rannenberg, Herbert Damker, Werner Langenheder, Günter Müller: Mehrseitige Sicherheit als integrale Eigenschaft von Kommunikationstechnik – Kolleg „Sicherheit in der Kommunikationstechnik" eingerichtet; in: Kubicek, Müller, Neumann, Raubold, Roßnagel (Hrsg.): Jahrbuch „Telekommunikation & Gesellschaft" 1995, R. v. Decker's Verlag, Heidelberg, 1995, S. 254 - 260; aktualisierter Nachdruck in: á la Card aktuell, 7. Jg. 1995, Heft 41, 22.12.1995, S. 10 - 14

Ralf Rohrer

Sicherungsinfrastrukturen

Weshalb sind Sicherungsinfrastrukturen überhaupt notwendig? Als Verantwortlicher für die Sicherheit des Internet-Zuganges eines großen Konzerns erlebe ich fast täglich Beispiele, die den Nutzen bestehender Sicherungsinfrastrukturen bestätigen oder den Bedarf an zusätzlichen Sicherungsinfrastrukturen verdeutlichen.

Ich möchte einen kleinen Spaziergang durch meinen Alltag mit Ihnen unternehmen. Es ist der Alltag eines Sicherheitsbeauftragten, der sich täglich mit diesem Thema befasst und täglich neue Erkenntnisse zu dieser Thematik sammeln kann. Ich möchte versuchen, die Komplexität dieses Themas partiell (durch *konstruierte* Beispiele) aufblitzen zu lassen, um Ansatzpunkte für Sicherungsinfrastrukturen aufzuzeigen.

Doch bevor wir unseren Spaziergang beginnen, möchte ich noch kurz ein paar grundlegende Gedanken vorausschicken. Bei dieser ganzen Diskussion darf nie aus dem Auge gelassen werden, daß geschützt werden muß und „was vor wem" zu schützen ist. Natürlich ist es wichtig, sozialverträgliche und für den Benutzer akzeptable Infrastrukturen zu schaffen. Doch das Ziel muß erreicht werden:

- Der private Bürger muß sicher sein können, daß seine bei Behörden und Unternehmen gespeicherten Daten dort absolut sicher sind und nur für den vorgegebenen Zweck verwendet werden!
- Die Unternehmen müssen in der Lage sein, ihre Daten gerade auf „öffentlichen"[1], unsicheren Übertragungswegen zu schützen!

Ich beschränke mich in dieser Diskussion auf den Schutz von Daten und Personen (ja: man kann auch Personen vor Daten schützen). Mit dieser Prämisse sind die in der Praxis relevanten Konstellationen:[2]

- Schutz firmeninterner Daten vor unbefugtem internen Zugriff,
- Schutz firmeninterner Daten vor unbefugtem externen Zugriff,
- Schutz von Personen (speziell Kindern) vor (z. B. ethisch) bedenklichen Daten,
- Schutz privater Daten vor externem Zugriff oder unerlaubter Weitergabe.

Als Sicherheitsbeauftragter bin ich täglich bemüht, Systemlücken[3] aufzuspüren und zu schließen. Dies läuft typischerweise so ab, daß entweder ein Systemhersteller selbst eine Lücke entdeckt oder bei irgend einem Anwender dieses Systems auf eine Lücke gestoßen wird (letzteres geschieht meist durch Zufall). Wenn nun beide verantwortungsvoll sind (und der Hersteller nicht Pressekritik und Konkurrenzkampf scheut und der Anwender nicht die Lücke mal bei Rechnern der Konkurrenz ausprobieren will), dann werde ich irgendwann – Tage oder Wochen später – über diese Lücke informiert. Dies kann recht schnell geschehen, wenn ich an den relevanten Newsgroups und Mailgroups im Internet partizipiere. Wenn ich mich dagegen nur auf unsere Wartungsverträge verlasse, dann können schon mal ein paar Wochen vergehen, bis ich vom Hersteller die Bugfixes[4] erhalte. Sie sehen also, selbst wenn Sicherheitslükken bekannt geworden sind, vergeht eine bestimmte Zeit bis diese Lücke geschlossen werden kann.

> *Stop: Wie wäre es denn, an dieser Stelle über Infrastrukturen nachzudenken, die eine schnellstmögliche Korrektur solcher Systemlücken erlaubt? Muss ein Hersteller seine Kunden informieren? Innerhalb welcher Frist hat ein Hersteller eine Sicherheitslücke zu schließen? Wer haftet wann?*

Nun habe ich guten Mutes die letzte Lücke auf meinem Firewall[5] geschlossen, da ruft mich der Technische Produktionsleiter an. Er klagt mir sein Leid mit seinem nicht funktionierenden Modem-Zugang. Und er muss doch so dringend am Wochenende über Fernzugriff neu implementierte, wichtige Produktionsprozesse überwachen. *Modemzugang???* In meinem Gehirn schrillen sämtliche Alarmglocken. Ich versuchen zu erläutern, daß das von Ihm verwendete Produkt vollkommen unbekannt ist und mir keine Informationen darüber vorliegen wie sicher oder unsicher dieses Produkt ist. Mein Gegenüber, welches – positionsgemäß – etwas andere Ziele voranbringen muß, beharrt auf einer Möglichkeit des Fernzugriffs. Wir treffen uns beim Geschäftsführer. Nach vielem hin und her, Pro und Contra, einigen wir uns darauf, einen Anschluß solange zu verzögern, bis ein mutmaßlich sicheres Produkt gefunden ist, um den Fernzugriff zu realisieren. Stellen Sie sich vor, der Technische Produktionsleiter hätte

1. „Öffentlich" im Sinne von „jeder, der bezahlt, darf es benutzen".
2. Aus meiner Sicht, ich erhebe hier keinen Anspruch auf Vollständigkeit.
3. Systemlücken sind technische Gegebenheiten, die ausgenutzt werden können, um Systeme zu zerstören, Daten zu manipulieren, zu löschen oder zu kopieren. Besonders gravierend können sich diese Systemlücken bei Systemen zur Zugangsüberwachung (z. B. Betriebssysteme) oder zur Datenübermittlung (z. B. Mailsysteme) auswirken.
4. Fehlerkorrigierte oder fehlerkorrigierende Software
5. System, um Computer-Netze gegeneinander abzuschirmen. Hauptanwendung: Abschirmung von Firmennetzen gegenüber unzulässigen Zugriffen aus dem Internet.

mich nicht angerufen! Kein Mensch hätte eventuell je von diesem Zugang zum Firmennetz erfahren.

Als Profi lasse ich es natürlich gar nicht so weit kommen. Vor Einführung jeder neuen Technik werden Sicherheitsrisiken geprüft und die Benutzer in einer sogenannten „Using Policy" auf den richtigen Umgang mit der neuen Technik eingeschworen (zu deutsch: Der Anwender erfährt, was er darf und was nicht). Während dieser Phase eines Projektes kommt es dann auch mal so weit, daß man in Newsgroups im Internet mit anderen Sicherheitsbeauftragten diskutiert, wie „Using Policies" zum Beispiel für einen Internet-Zugriff auszusehen haben. Im Handumdrehen erhalte ich über diesen Weg Tips und Anregungen (nicht immer, aber oft).

Stop: Wie wäre es denn, an dieser Stelle über Infrastrukturen nachzudenken, die es Sicherheitspersonal und Management erlauben, Datenflüsse[6] (vor allem nach außen) zu kontrollieren. Ein ganz großes Problem der EDV ist es, daß das Kopieren von Daten zum einen ein Kinderspiel ist und zum anderen nicht bemerkt wird (sofern kein spezielles Protokollierungssystem installiert wurde).

Zurück am Schreibtisch klicke ich mich durch diejenigen Mails, die mir von meinen Systemen zur Überwachung gesendet werden. Mal wieder ein paar falsch addressierte Internetmails. Ich öffne eine Mail, um mehr Details zu erhalten. Ach sieh an, da stecken ja die ganzen Gehaltsabrechnungen für unseren Standort in Norddeutschland drin – *unverschlüsselt!* Ja, warum schicken die solche Daten denn nicht verschl..., ach ja, da war doch noch was: Verschlüsselungsverbot durch unsere staatlichen Vordenker.

Stop: Hier muss über gesetzliche Rahmenbedingungen nachgedacht werden, die es einem Unternehmen erlauben, geheime Daten zu schützen. Gerade im Zeitalter des Internet, in dem es extrem wichtig ist, Informationen von allen Unternehmensstandorten in Minutenschnelle an einem Punkt dieser Erde zu konzentrieren.

Sie sehen, wie unbedarft schon in der Industrie mit dem Thema Sicherheit umgegangen wird. Dieses Verhalten ist bei genauerem Hinsehen recht verständlich, denn woher sollen die Mitarbeiter denn wissen, wie kritisch bestimmte Technik in ihrer Anwendung ist. Obwohl es hier im Interesse des Betriebes sein müßte, ein Bewußtsein für diese Thematik zu schaffen, geschieht auffallend wenig in deutschen Unternehmen. Daß aber derzeit die Mehrheit der weltweit operierenden Nachrichtendienste etwas zum Glück der jeweils heimischen Industrie beiträgt, ist kein Geheimnis mehr. Eigentlich verständlich: Würden Sie sich die Ohren zuhalten, wenn Ihr böser Nachbar gerade seiner Frau mitteilt, daß er eine Million im Lotto gewonnen hat? Natürlich nicht, Sie würden es Ihrer eigenen Frau erzählen. Und so muß man sich eine unverschlüsselte Mail tatsächlich vorstellen: Es bedarf keinerlei Gewaltanwendung, um eine Mail zu lesen. Ein Nachrichtendienst braucht nur „nicht wegzuhören"! Glauben Sie nun aber nicht, daß es der Ausstattung eines Nachrichtendienstes bedarf um an Ihre Daten zu gelangen!

Von den Attacken, die von innen geführt werden können, möchte ich an dieser Stelle gar nicht sprechen. Jeder Betrieb sollte sich klar machen, welche Daten wichtig sind und wie er sie schützen möchte. Dabei wird es unumgänglich sein, Mitarbeiter in kritischen Positionen besonders zu sensibilisieren und auch zu kontrollieren. Desweiteren Zugriffe auf vertrauliche Daten zu protokollieren und diese Protokolle unlöschbar zu hinterlegen. Sie sehen: Sicherheit läßt sich im Unternehmen aktiv gestalten (sofern Sie sich auf Ihre eigenen Mitarbeiter verlassen können). Aber wir kommen nicht umhin: Sicherheit hat auch etwas mit Kontrolle zu tun (denn ohne Kontrolle können Sie sich nicht *sicher* fühlen)! Dies kann für Mitarbeiter eines Unternehmens, aber auch für den Privatmann, zu unverständlichem Aufwand bei der Handhabung sicherheitskritischer Systeme führen. Hier sind Aufklärungsarbeit und populärwissenschaftliche Darstellung des „Warum & Weshalb" gefragt – Sicherheit zum Anfassen und Nachvollziehen.

Doch wie soll der Laie[7] vor Mißbrauch geschützt werden oder Sicherheit gar nachvollziehen? Er hat in der Regel keine Eingriffsmöglichkeiten in die Systeme die er benutzt. Er muß die Systeme benutzen „wie sie sind" (Beispiel: Privatmann, der per T-Online seine Überweisungen tätigt. Mittelständisches Unternehmen, das seinen Internet-Zugang durch einen Provider verwalten läßt). Er ist auf Sicherungsinfrastrukturen noch stärker angewiesen. Er benötigt Unterstützung! So mancher hat keine Ahnung, was denn so alles schützenswert ist (Sie gehören dazu, wenn Sie Ihre Kontoauszüge oder Überweisungsdurchschläge gleich im Papierkorb neben dem Bankautomaten entsorgen).

Stop: Hier sollte darüber nachgedacht werden, ob der Staat durch Gesetze dafür zu sorgen hat, daß Dienstleister noch schärferen und vor allem transparenten Sorgfaltspflichten unterliegen. Sollte diese Sorgfalt von Dritten überprüft werden?

Anstatt auf Literatur möchte ich auf die Möglichkeiten des Internet verweisen und dem interessierten Laien das Lesen von Newsgroups und Mailgroups empfehlen. Diese Dialoge sind (meist) international (daher in englischer Sprache gehalten) und verdeutlichen am besten Dynamik, Komplexität und nationale Eigenheiten anderer Länder in diesen Fragen.

6. Art der Daten und Weg, den die Daten nehmen. Ich schreibe hier bewusst von Daten und nicht von Informationen, da nicht zwingend gegeben ist, dass die übermittelten Daten für den Empfänger etwas Neues darstellen und es sich deshalb um eine Information im informationswissenschaftlichen Sinne handelt.

7. im Sicherheitstechnischen Sinne. Ich möchte an dieser Stelle unter diesen Begriff all diejenigen fallen lassen, die sich nicht von professioneller Seite beraten lassen (also durchaus auch Betriebe).

Claus Stark

Wie sicher ist eigentlich Sicherheit?

Mit Evaluation nach ITSEC mehr Vertrauen in IT-Sicherheit gewinnen

Unsichere Software ist heute der Normalfall. Selbst kleine Programmpakete haben oft große „Macken", an Programmabstürze und Viren haben wir uns schon gewöhnt:

- Eingeschleppte Computerviren zerstören wertvolle Datenbestände und programmieren unsere Bürosoftware gezielt um.
- Durch das Betriebssystem verschlüsselte Dateien und Paßwortdateien lassen sich oft genug mit kostenlosen Freeware-Programmen auslesen.
- Zugangssicherungssysteme für PCs lassen sich z.T. durch einfaches Booten vom Diskettenlaufwerk aus umgehen.
- Firewalls lassen sich gelegentlich von außen umkonfigurieren.
- Paßworte und elektronische Briefe werden im Internet oft unverschlüsselt übertragen.

Unsichere – oder vermeintlich sichere – Systeme führten bisher in der Praxis nicht zwangsläufig zum „GAU", da sie oft in unkritischen Bereichen eingesetzt wurden. In kritischen Bereichen – wie beispielsweise dem Militär, dem Geheimdienst und in der Medizin – wurden Computersysteme allerdings seit jeher auf Sicherheit überprüft, bevor sie eingesetzt werden durften.

Die Frage nach der Sicherheit von Computersystemen wird aber in Zukunft immer wichtiger, denn nun werden auch Bereiche informatisiert, die vorher – u. a. auch wegen der mangelhaften Sicherheit herkömmlicher IT-Konzepte – als nicht computerisierbar galten. Das Standardbeispiel ist hier die „Rechtsverbindliche Telekooperation": Das zum 1.8.1997 inkraftgetretene Signaturgesetz stellt die Grundlage der rechtsverbindlichen elektronischen Unterschrift dar – die Informationsgesellschaft will endlich erwachsen werden. Aber das führt langsam zu einer Sensibilisierung in der Bevölkerung und bei den Entscheidungsträgern in Wirtschaft und Politik.

Es soll der Beitrag „geprüfter IT-Sicherheit" für eine „sichere Informationsgesellschaft" diskutiert werden. Welche Rolle spielt das Konzept „Evaluation" beim Aufbau von Sicherungsinfrastrukturen? Dazu wird ein Blick in die tägliche Evaluationspraxis geworfen: Was ist IT-Sicherheit? Wie wird sie geprüft? Und was kann von einem Sicherheitszertifikat erwartet werden?

Was heißt hier „sicher"?

Heute versteht die Fachwelt unter Sicherheit – genauer: IT-Security – vorwiegend drei Dinge:

- **Vertraulichkeit**: Schutz vor unbefugter Einsichtnahme in Informationen
- **Integrität**: Schutz vor unbefugter Änderung von Informationen
- **Verfügbarkeit**: Schutz vor unbefugter Vorenthaltung von Informationen und Betriebsmitteln

Man mag darüber streiten, ob dieser Kanon erweitert werden sollte oder nicht. Der Begriff ist momentan genau definiert und umfaßt z. B. nicht „Safety", den Schutz von Leib und Leben vor wildgewordenen Computersystemen. Safety – zu Deutsch ebenfalls mit „Sicherheit" zu übersetzen – spielt z. B. bei medizinischen Geräten eine große Rolle. Dafür gibt es eigene Experten, Prüfkriterien und Laboratorien.

Sicherheit in Form von „Security" kann in Computersysteme eingebaut werden. Wenn man das nicht könnte:

- Würden Sie als Patient Ihre sensiblen medizinischen Daten einer Patientenchipkarte anvertrauen, wenn jedermann sie leicht lesen könnte?
- Würden Sie als Bankmanager einer Geld-Chipkarte trauen, wenn der auf ihr gespeicherte Betrag mit jedem PC manipuliert werden kann?
- Würden Sie einem TrustCenter ohne auf Einbruchssicherheit ausgelegte Computeranlage ihre kryptographischen Schlüssel zur Verwaltung anvertrauen?
- Würde Sie als Arbeitgeber einem unsignierten elektronischen Zeugnis eines Bewerbers glauben?

Sicher nicht! Zum Glück bauen ja die meisten Hersteller viele „Security-Features" in ihre Produkte ein! Aber – können wir dieser Sicherheit trauen?

Können wir der Sicherheit vertrauen?

Ohne IT-Sicherheit, ob Safety oder Security (oder auch noch andere Aspekte wie z. B. Privacy), wird es schwer sein, tragfähiges Vertrauen für die von vielen angestrebte „Informationsgesellschaft" zu gewinnen. Daten wollen wirksam vor fremden Blicken, Systeme vor unberechtigtem Zugriff geschützt werden, sollen sich Computersysteme erfolgreich in vielen relevanten gesellschaftlichen Bereichen durchsetzen. Elektronische Unterschriften sollten sich nicht fälschen lassen. Ohne Sicherheit geht es also nicht – aber sind die „sicheren" Systeme wirklich sicher, sicher genug für unsere Gesellschaft, um darauf eine „Kulturrevolution" wie die Einführung der Digitalen Signatur aufbauen zu können? Oder sind sie gar *zu* sicher? Diese eher demokratietheoretische Frage (ein heißes FIFF-Thema!) wird am Schluß dieses Beitrags kurz angerissen und soll hier nicht weiter diskutiert werden. Es gibt einige Produkte, die viel versprechen – und wenig halten. Und manchmal nutzt die beste Security nichts, wenn der Systemverwalter sie aus Bequemlichkeit leicht ausschalten kann. Die Herstellererklärungen sollten stets kritisch hinterfragt werden. Der Kunde ist aber (meistens) überfordert, die Produkte selber adäquat zu prüfen.

Es ist daher unverzichtbar, die technische Sicherheit von IT-Systemen von unabhängigen und fachkundigen Dritten

prüfen („evaluieren") und zertifizieren zu lassen. „Evaluation" ist somit ein wichtiger Baustein beim Aufbau und Betrieb von (Infrastruktur-)Einrichtungen der „Informationsgesellschaft". Eine Reihe von Institutionen und Firmen – wie beispielsweise die TÜViT GmbH in Essen – bieten Sicherheitsevaluation als Dienstleistung an.[1]

IT-Security-Evaluation im Internet

- ITSEC: http://www.itsec.gov.uk
- CC: http://csrc.ncsl.nist.gov/nistpubs/cc/
- Trusted Product Evaluation Program: http://www.radium.ncsc.mil/tpep/index.html
- TÜViT GmbH Essen: http://www.tuvit.de

Immer mehr Hersteller lassen ihre Systeme – ob Chipkartenbetriebssystem oder PC-Sicherheitssoftware – nach anerkannten Kriterien wie den im Sicherheitsbereich wichtigen ITSEC, den im Finanzbereich relevanten ZKA-Kriterien („Zentraler Kreditausschuß") oder nach anderen Kriterienwerken evaluieren. Die Hersteller nehmen die Zertifizierung als Chance einer zusätzlichen Qualitätskontrolle wahr, und sie erhoffen sich dadurch einen Marktvorteil gegenüber den Konkurrenten oder überhaupt den Marktzugang beim Kunden: Viele Anwendungsanbieter wie Banken oder große Telekommunikationsunternehmen verlangen von ihren Zulieferern die unabhängige Evaluation ihrer Produkte. Keine Bank würde einem Chipkartenhersteller für eine Geldkartenanwendung auch nur eine Chipkarte ohne unabhängige Prüfung abnehmen: Sie könnte ja durch Hacker – oder einfach nur durch eine Fehlfunktion – leicht kompromittiert werden, und das kann und will man sich nicht leisten. Die Evaluation bietet ein Maß, inwieweit der versprochenen IT-Sicherheit getraut werden kann. Die Bundesregierung beschäftigte sich übrigens im Signaturgesetz und in der dazugehörigen Signaturverordnung zum ersten Mal mit der ITSEC: Für rechtsverbindliche Konzepte zur Digitalen Signatur werden „vertrauenswürdiger Produkte und Systeme" gefordert. Die Hersteller entsprechender Systeme – von der Chipkarte bis zum ganzen TrustCenter – werden im Gesetz zur unabhängigen Prüfung nach ITSEC verpflichtet.

Kriteriengestützte Evaluationen von IT-Sicherheit geben Auskunft über die Vertrauenswürdigkeit, die man „objektiv" in die technische Sicherheit eines konkreten Produktes haben kann. Sie versprechen die Meßbarkeit von IT-Sicherheit. Das europäische Kriterienwerk, das diese Prüfung erlaubt, ist die 1991 vorgelegte ITSEC, die „Information Technology Security Evaluation Criteria" – Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (siehe auch Buchbesprechung ITSEC/ITSEM). Sie bieten 7 Stufen der Vertrauenswürdigkeit: Die Skala reicht von E1 (Basisvertrauen in die implementierte Sicherheit) bis hoch zu E6 (höchste Vertrauenswürdigkeit) – E0 (unzureichende Vertrauenswürdigkeit) sei der Vollständigkeit halber erwähnt. Je höher diese Stufe ist, umso tiefergehende und höherwertige Dokumente muß der Hersteller für die Evaluation bereitstellen. Die meisten zertifizierten Produkte pendeln momentan bei E2/E3 – eine langsame Verschiebung in Richtung E4/E5 wird erwartet. Nach E6 wurde in Europa noch kein Produkt evaluiert. In Deutschland und Europa wird vorwiegend nach ITSEC evaluiert – und vom BSI (dem Bundesamt für Sicherheit in der Informationstechnik in Bonn) zertifiziert. Ein etwas älteres Kriterienwerk ist das „Orange Book", die US-amerikanischen „TCSEC" („Trusted Computer Security Evaluation Criteria") von 1985. Die ITSEC gilt allerdings als abstrakt und bürokratisch, die TCSEC schlicht als veraltet: Die Zukunft soll nun den CC gehören, den „Common Criteria for IT-Security Evaluation" – sie soll von der Standardisierungsorganisation ISO als weltweite Norm anerkannt werden und die aktuellen Kriterienkataloge langfristig ablösen. Aber zunächst müssen sich die beteiligten Länder und Institutionen über Form, Inhalt und Umsetzung einigen, bevor es die ersten internationalen Zertifikate geben wird – das wird nicht einfach sein. Und es wird genau zu prüfen sein, ob mit den CC ein echter Fortschritt in der Sache verbunden sein wird.

Die E-Stufen der ITSEC

Maß des Vertrauens in die Korrektheit

- E0: Unzureichende Vertrauenswürdigkeit
- E1: Es wurden Sicherheitsziele und -funktionalität definiert (Sicherheitsvorgaben), eine informelle Beschreibung des Systems wurde geprüft (Architekturentwurf). Es finden Tests zur Überprüfung der Sicherheitsfunktionalität statt.
- E2: Zusätzlich zu E1 muß ein Designentwurf vorgelegt werden (Feinentwurf). Die Entwicklungsumgebung wird überprüft.
- E3: Zusätzlich zu E2 muß der Hersteller den Quellcode zur Verfügung stellen.
- E4: Zusätzlich zu E3 müssen zu den Sicherheitsvorgaben ein formales Sicherheitsmodell, zu den sicherheitsspezifischen Funktionen semiformale Spezifikationsdokumente zur Verfügung gestellt werden.
- E5: Zusätzlich zu E4 muß der enge Zusammenhang zwischen Feinentwurf und Quellcode nachgewiesen werden.

E6: Zusätzlich zu E5 müssen sicherheitsspezifische Funktionen und der Architekturentwurf in formaler (beweisbarer) Notation vorliegen, die konsistent mit dem formalen Sicherheitsmodell sind.

Die Prüfung nach ITSEC – Ein Blick über die Evaluatorschulter

Mittelfristig gilt in Europa und in Deutschland die ITSEC als das Maß aller IT-Sicherheit. Aber was kann praktisch von erfolgreich evaluierten Produkten erwartet werden? Ist beispielsweise ein nach E4 zertifiziertes Chipkartenbetriebssystem geeignet, medizinische Daten vertrauenswürdig zu speichern? Ein Blick in die Evaluationspraxis soll helfen, eine Zertifizierung besser einzuschätzen.

1. Eine vollständige Liste der akkredierten Prüfstellen ist beim BSI erhältlich.

Die ITSEC umfaßt vorrangig die Bewertung technischer Sicherheitsmaßnahmen. Organisatorische, personelle, administrative Maßnahmen stehen nicht im Mittelpunkt der Analyse, werden aber berücksichtigt. Das Kriterienwerk ist dabei so allgemein gehalten, daß sowohl Hardware als auch Software und Firmware (sowie deren Kombination) evaluierbar ist. Jede ITSEC-Evaluation soll objektiv und unvoreingenommen sein – darauf sind die deutschen vom BSI akkreditierten Prüfstellen geprüft und verpflichtet.

Die konkrete Prüfung eines Produktes (oder eines Systems) nach ITSEC erfolgt auf Initiative des Herstellers bzw. eines seiner (potentiellen) Kunden. Der Antragsteller sucht sich dazu eine von der nationalen Zertifizierungsbehörde (in Deutschland: BSI) akkreditierten Prüfstellen aus. Die Evaluation erfolgt in enger Kooperation zwischen Antragsteller[2], Hersteller, Prüfstelle – und ggf. dem BSI.

Der Hersteller beschreibt möglichst genau sein zu evaluierendes Produkt oder System, den „Evaluationsgegenstand" (EVG). Nur dieser EVG wird evaluiert. Ist ein System zu komplex, um es als Ganzes zu evaluieren, wird ein geeigneter Teil des Produktes als EVG bestimmt. Diese Abgrenzung muß sehr sorgfältig erfolgen, denn die Abhängigkeiten von anderen Systemkomponenten, die auch von Drittherstellern stammen können, lassen oft eine genaue Aufteilung der „Sicherheitsverantwortung" nur schwer zu: Baut beispielsweise ein Sicherheitsprodukt seine Sicherheitsfunktionalität auf Leistungen des darunterliegenden (ungeprüften?) Betriebssystems auf oder stellt es diese selbst zur Verfügung? Die Schnittstellen des EVG mit seiner (technischen) Umwelt und die Einsatzbedingungen spielen naturgemäß eine besondere Rolle in der Evaluation.

Phasen der Evaluation nach ITSEC

- Vorstudie (optional)
- Festlegen des EVG und der Sicherheitsvorgaben
- Festlegen der angestrebten E-Stufe und der Mechanismenstärke
- ggf. Antrag auf Zertifizierung beim BSI
- Korrektheitsuntersuchungen
- Wirksamkeitsuntersuchungen
- Tests am Produkt in der definierten Einsatzumgebung
- Zertifikat, ggf. durch das BSI

  Ggf. Re-Evaluation bei Änderungen am Produkt

Der Hersteller hat mit dem EVG auch die Ziele, die er mit ihm nachprüfbar erreichen möchte, definiert: Welche Sicherheitsziele werden angestrebt? Welche Funktionalität soll durch das Produkt bereitgestellt werden? Was sind die angenommenen Bedrohungen, denen entgegengewirkt werden soll? Für ein PC-Sicherheitsprodukt ist es vielleicht die Vertraulichkeit von Dateien, die es vor unbefugten Blicken schützen soll, für eine Firewall ist sicherlich ein unverzichtbarer Aspekt die „Einbruchssicherheit". Die ITSEC schlägt einige Sicherheitsfunktionen in Form von Funktionalitätsklassen (wie „F-C2") vor. Dem Hersteller steht es aber frei, die zu evaluierende Sicherheitsfunktionalität individuell zu wählen – die ITSEC ist in dieser Hinsicht sehr flexibel: Aus generischen Oberbegiffen wie „Identifikation & Authentisierung" oder „Beweissicherung" lassen sich eine Vielzahl konkreter Sicherheitsfunktionalitäten für eine Vielzahl von Produkten und Systemen ableiten. Die Sicherheitsvorgaben und die Festlegung des EVG stellen die Basis für die gesamte Evaluation dar.

Die Stufen der ITSEC bestimmen die Prüftiefe: Für niedrige Stufen (E1/E2) stellen die Hersteller den Evaluatoren informelle Dokumentation zur Verfügung – damit kann aber mit der Evaluation natürlich nur eine niedrige Stufe der Vertrauenswürdigkeit bescheinigt werden. Soll nach höheren E-Stufen (E3–E6) evaluiert werden, werden Dokumente wesentlich höherer Qualität vom Hersteller gefordert – das geht bis zur Bereitstellung von nachvollziehbar dokumentiertem Quellcode, semiformalen Spezifikationsdokumenten und beweisbaren formalen Sicherheitsmodellen. Schon bei niedrigen Stufen ab E2 wird der Entwicklungsprozeß selbst überprüft: Wird Konfigurationsmanagement betrieben und mit einer definierten Entwicklungsumgebung gearbeitet? Ab E3 müssen die verwendeten Programmiersprachen klar definiert sein (z. B. nach ISO). Die Anforderungen an die vorzulegenden Dokumente hängen von der angestrebten Evaluationsstufe ab.

Die Evaluatoren beginnen damit, die Korrektheit der Dokumente zu prüfen: Sind die Sicherheitsziele in den Sicherheitsvorgaben eindeutig festgelegt? Von welchen Bedrohungen wird ausgegangen? Wie werden vom EVG adäquate Sicherheitsfunktionen bereitgestellt, die den angenommenen Bedrohungen entgegenwirken sollen? Lassen sich die definierten Sicherheitsfunktionen im Architektur- und im Feinentwurf des EVG wiederfinden und vom Rest des EVG abgrenzen? Im Prinzip wird so geprüft, ob die in der obersten Stufe aufgestellten globalen Sicherheitsfunktionen und -mechanismen in allen Dokumenten, die – immer feiner werdend – bis auf Quellcodeebene gehen können, eindeutig nachverfolgt und identifiziert werden können („traceability"). Neben den Entwicklungsdokumenten wird u. a. noch die Benutzer- und Administrator-Dokumentation daraufhin untersucht, ob sie den Umgang mit den sicherheitsrelevanten Komponenten des Produktes auch adäquat erklärt. Treten Brüche in den Korrektheitsuntersuchungen auf, muß nachgebessert werden: Dem Hersteller wird in solchen Fällen empfohlen, entsprechende Änderungen an seinem Produkt und in seiner Dokumentation vorzunehmen – oder einer Rückstufung in der angestrebten E-Stufe zuzustimmen. Gilt nämlich auch nur ein Aspekt als nicht erfüllt, kommt es zum Ergebnis „E0 – unzureichende Vertrauenswürdigkeit" – die ITSEC ist kompromißlos!

Nach diesen Korrektheitsuntersuchungen wird überprüft, ob die implementierten Mechanismen den Bedrohung auch wirksam entgegenwirken können (Wirksamkeitsanalyse). Lassen sie sich schon durch einfache Handgriffe durch Laien „aushebeln" oder braucht man Know-How, Spezialwerkzeug und sehr, sehr viel Zeit? Jeder einzelne Mechanismus wird auf seine Stärke, den Bedrohungen entgegenzuwirken, hin bewertet. Hier müssen Szenarien entwickelt und gedanklich durchgespielt werden, wo konstruk-

2. Da die Rolle des Antragstellers oft mit der Rolle des Herstellers zusammenfällt, sei der Einfachkeit halber im Folgenden nur noch vom Hersteller die Rede.

tive oder operative Schwachstellen vorhanden sind – und wie diese in der Praxis ausgenutzt werden können.

Mechanismenstärke als Maß der Wirksamkeit:

- niedrig: Sicherheitsmechanismus ist durch Laien schnell zu überwinden.
- mittel: Es wird Expertenwissen und Zeit zum Überwinden benötigt.
- hoch: Sicherheitsmechanismus ist praktisch nicht zu überwinden.

Liegen alle Erkenntnisse über Funktionsweise, Architektur, Feinentwurf und Schwachstellen des EVG vor, kann mit den direkten Tests am Produkt begonnen werden: Die Prüfstelle führt eigene Tests durch, um vorhandene Schwachstellen auf Ausnutzbarkeit zu prüfen („Penetrationstests") – lassen sich die Sicherheitsfunktionen direkt oder indirekt austricksen? Die Prüfstelle untersucht auch die Benutzerfreundlichkeit des Produktes – unter „Benutzerfreundlichkeit" versteht ITSEC die Nichtvortäuschbarkeit „sicherer Zustände" in unsicheren Situationen. Daneben werden die Funktionstests der Hersteller nachvollzogen oder eigene Tests durchgeführt, um beispielsweise zu prüfen, ob spezielle Mechanismen auch korrekt implementiert wurden (wie spezielle Verschlüsselungsalgorithmen). Die Testphase kann daher sehr aufwendig sein.

Sind schließlich alle Dokumente erfolgreich geprüft, alle Tests zur Zufriedenheit der Prüfstelle verlaufen, wird das Ergebnis durch die Prüfstelle mit dem Sicherheitsgutachten bescheinigt. Im Falle einer BSI-Zertifizierung erfolgt mit der Ausstellung des Zertifikats der Eintrag in die offizielle „Liste zertifizierter Produkte" und der Hersteller darf das Produkt mit dem Attribut „BSI-zertifiziert nach ITSEC" anbieten.

Das Zertifikat ist kein Freibrief!

Einige Grenzen des Zertifikats wurden bereits deutlich: Es wird bescheinigt, daß die vom Hersteller definierten Sicherheitsziele mit der zur Verfügung gestellten Sicherheitsfunktionalität des EVG erreicht werden. Ob die Funktionalität und die Vertrauenswürdigkeit für konkrete Einsatzgebiete ausreicht oder nicht, muß in jedem Einzelfall vom Kunden selbst geprüft werden. Es ist auch stets zu prüfen, wie alt das Zertifikat ist – bei zu alten Produkten haben es Angreifer vielleicht in der Zwischenzeit gelernt, die Sicherheitsbarrieren zu umgehen.

Das (BSI-)Zertifikat gilt nur für die „eine" evaluierte Version der Software. Bei Versionsänderung des Produktes gilt das Zertifikat nicht mehr – es muß eine Re-Evaluation durchgeführt werden. Hersteller – vor allem die kleineren Firmen – stöhnen hier zwar im Hinblick auf die hohe Innovationsrate im Softwarebereich und auf die Kosten, aber bei intelligenter und kooperativer „entwicklungsbegleitender Evaluation" sollte das kein Handikap darstellen. Es ist auf jeden Fall kein Fehler, „Sicherheit" von Anfang an als explizites Gestaltungsmerkmal in der Entwicklung zu berücksichtigen – und entsprechend explizit zu dokumentieren und zu testen.

Zertifikate gelten nur in Verbindung mit dem dazugehörigen Zertifizierungsreport, der vom Hersteller an Interessenten und Kunden ausgegeben wird. Darin werden Auflagen und Voraussetzungen zum „sicheren Betrieb des EVG" gemacht, ohne deren Erfüllung das Zertifikat nicht gilt. Hier böte sich an, bei komplexeren Systemen oder in sensiblen Bereichen die korrekte und sichere Installation des EVG und seinen sicheren Betrieb beim Kunden durch eine – die Evaluation ergänzende – „Systemakkreditierung" zu bescheinigen. Die TÜViT bietet eine solche Akkreditierung als Dienstleistung an.

Es sollte klargeworden sein, daß ein Zertifikat kein Ersatz für den gewissenhaften Umgang mit der konkreten Technologie darstellt. Nachlässigkeit beim Definieren und Umsetzen von Sicherheitsstrategien werden auch durch Zertifikate nicht tolerierbar. Zertifizierte Produkte – gewissenhaft eingesetzt – können aber ein hohes Maß an Sicherheit garantieren.

Security ist gesellschaftlich nicht unumstritten

Nun noch kurz zum gesellschaftspolitischen Aspekt von Sicherheit, denn Security ist nicht unumstritten: Durch sie würden Machtstrukturen gefestigt, die gesellschaftlich unerwünscht seien. Spielte doch „Security" bislang vor allem im militärischen und geheimdienstlichen Bereichen (Geheimhaltung) eine tragende Rolle – hier haben ITSEC und „Orange Book" schließlich auch ihren Ursprung. Wie aber sind „militärische" Sicherheitskonzepte mit der „anarchischen" Freiheit des Internet (welches übrigens einst auch ein militärisches Projekt war) vereinbar? Würde es nicht dem stromlinienförmigen und „abgesicherten" Datasuperhighway weichen, auf dem sich dann nur noch Behörden und Industrie in ihren rechtsverbindlichen geschlossenen Intranets tummeln würden? Ärzte könnten nur noch mit gültiger und von der Bundesärztekammer herausgegebener Health Professional Card eine Patientenakte einsehen. Das könnte das Gleichgewicht der Kräfte auf technokratische Weise unzulässig in eine Richtung verschieben und im schlimmsten Fall unsere Demokratie gefährden.

Diese Diskussion ist sehr wichtig und muß heute offensiv geführt werden, damit wir morgen nicht eine „Kontroll- und Steuerinfrastruktur" haben, vor der Kritiker zu Recht warnen. Sozial verträgliche und gesellschaftlich gewünschte Sicherungsinfrastrukturen sind aber möglich: „Privacy", Konzepte zu pseudonymem Handeln und zur Nichtverfolgbarkeit (d. h. die Vermeidung von personenbezogenen Datenspuren), heute große Themen der Datenschützer und Informationsökologen, werden bald auch Themen der „technischen Security" sein! FIFF muß sich für diesen gesamtgesellschaftlichen Diskurs um wünschenswerte Ziele einer Sicherungsinfrastruktur einsetzen. Dieses Themenheft der FIFF-KOMMUNIKATION soll die breite Diskussion anregen.

Diese so im gesellschaftlichen Prozeß gewonnenen Erkenntnisse müssen aber letztendlich auch wieder adäquat in Technik gegossen werden. Und da schließt sich der Kreis bei der Evaluation, der unabhängigen Prüfung von Zielen und Implementierung! IT-Sicherheitsevaluation ist auch unter dieser Prämisse ein unverzichtbarer Baustein auf dem Weg in die sichere *und* gesellschaftlich gewünschte Informationsgesellschaft.

Detlef Hühnlein

Generische Sicherheit

Die GSS-API und drei Ihrer Mechanismen

Zusammenfassung: Die gebräuchliche Sicherheitstechnologie unterliegt im Laufe der Zeit oft starken Veränderungen. Außerdem wird das Anwendungsgebiet der Sicherheitstechnologie immer vielfältiger. Eine Möglichkeit diese Entwicklungen weitgehend zu 'entkoppeln' ist mit der GSS-API[1] gegeben. Im folgenden wollen wir kurz das Konzept dieser Schnittstelle und drei der heute verfügbaren darunterliegenden Mechanismen vorstellen. Schließlich wollen wir die Vor- und Nachteile dieser Mechanismen, d.h. Kerberos, SPKM und SECUDE herausarbeiten und gegenüberstellen.

Einleitung

In Zeiten offener Telekooperation wird die ***Authentizität, Vertraulichkeit, Integrität*** und ggf. die ***Verbindlichkeit*** der Kommunikation durch kryptographische Methoden erreicht. Nun ist aber die Sicherheitstechnologie und Kryptographie in der mißlichen Situation, daß die verwendeten Verfahren nur so lange zu gebrauchen sind, bis ihre Sicherheit durch neue Forschungsergebnisse in Frage gestellt wird. In diesem Fall müssen die verwendeten Verfahren durch andere, als sicher geltende, ersetzt werden. Außerdem wird der Anwendungsbereich der Sicherheitstechnologie immer vielfältiger. Immer mehr Anwendungsprogramme können sich dem Ruf nach sicherer Kommunikation nicht verschließen. Im folgenden wollen wir uns mit einer Möglichkeit beschäftigen, diese beiden Entwicklungen zu 'entkoppeln' - der GSS-API. Diese Schnittstelle bietet generische Sicherheitsdienste an, die von der Anwendung genutzt werden können, ohne daß die konkrete Ausprägung des darunterliegenden Sicherheitssystems bekannt ist. Neben der kurzen Vorstellung der wichtigsten GSS-Aufrufe in Kapitel 2 wollen wir uns hier mit drei der heute zu Verfügung stehenden darunterliegenden Mechanismen beschäftigen. So ist Kapitel 3 dem Kerberos-, Kapitel 4 dem SPKM[2]- und Kapitel 5 dem SECUDE-Mechanismus gewidmet. Abschließend wollen wir die wichtigsten Vor- und Nachteile der einzelnen Mechanismen und deren bevorzugte Einsatzgebiete aufzeigen.

GSS - API

Wie bereits angedeutet, ist es sinnvoll Anwendungen unabhängig von konkreten Sicherheitsbausteinen zu entwickeln. Zu diesem Zweck wurde von der Netzwerk-Arbeitsgruppe der IETF[3] in [GSS-API] eine Schnittstelle vorgeschlagen, die es ermöglicht, bestehende und neue Anwendungen durch das Hinzufügen der dort spezifizierten GSS-Aufrufe zu sichern. Dabei sind die im Anwendungsprogramm vorhandenen Aufrufe unabhängig von verwendeten Sicherheitsmechanismen und Protokollen. Im folgenden stellen wir uns stets eine zu sichernde Kommunikation zwischen **Client** und **Server** vor. Von einer sicheren Kommunikation wollen wir sprechen, wenn

- der Server weiß, daß er mit dem richtigen Client 'spricht', ***Authentizität.***
- evtl. auch der Client weiß, daß er mit dem richtigen Server 'spricht', ***wechselseitige Authentifizierung.***
- der Datenstrom nicht durch Dritte einsehbar ist, ***Vertraulichkeit.***
- der Datenstrom nicht unbemerkt verändert werden kann, ***Integrität.***
- bestimmte Nachrichten später eindeutig einer bestimmten Partei zugeordnet werden können, ***Verbindlichkeit.***

Um diese Ziele zu erreichen, werden Client und Server zu Beginn der Kommunikation einen sogenannten ***Sicherheitskontext*** aufbauen, wobei die Authentizität der beteiligten Parteien sichergestellt und gleichzeitig ein geheimer Schlüssel (Session-Key) ausgetauscht wird, der (optional)[4] die Vertraulichkeit in der laufenden Kommunikation ermöglicht. Die Integrität der Nachrichten (per-message-tokens) wird durch Anfügen von kryptographischen Prüfsummen und Sequenznummern an die eigentlichen Datenpakete ermöglicht.

Bevor Client und Server einen ***Sicherheitskontext*** aufbauen können, müssen sie sogenannten ***credentials*** besitzen. Diese 'Ausweise' dienen zur Authentifikation der beteiligten Parteien. Die Frage, was man sich konkret unter diesen Ausweisen vorstellen kann, werden wir in den folgenden Kapiteln wieder aufgreifen. Wir nehmen nun also an, daß Client und Server einen solchen Ausweis besitzen. Der Aufbau eines Sicherheitskontexts (mit wechselseitiger Authentifikation) könnte nun vereinfacht folgendermaßen aussehen:

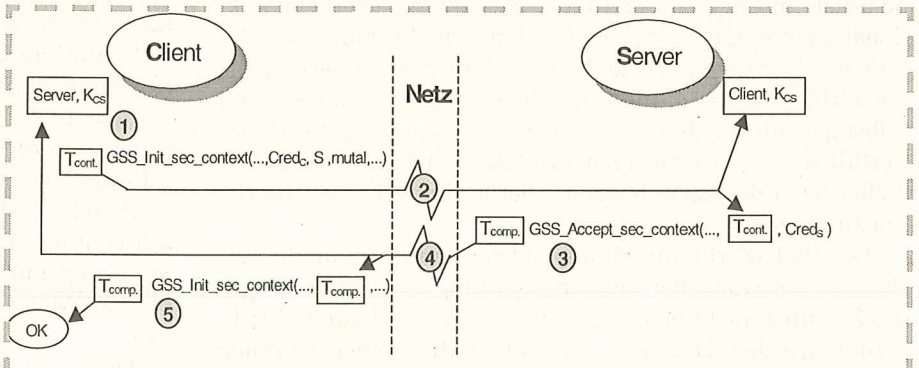


Abbildung 1: Aufbau des GSS-Sicherheitskontexts

Der Client packt in (1) ein Paket (ein sog. *Context-Level-Token*), das er in (2) zum Server schickt. Dieses Paket ist tatsächlich eine codierte Zeichenfolge, die alle für den Server benötigten Informationen enthält. So z.B. steckt der Ausweis des Clients

1. Generic Security Service Application Program Interface
2. Simple Public Key Mechanism
3. Internet Engineering Task Force
4. Der Grund, daß eine solch zentrale Forderung an die Kommunikation, wie die Vertraulichkeit nicht zwingend gefordert wird, ist in erster Linie politischer Natur, da so u.U. die Exportierbarkeit des Systems erleichtert wird.

in diesem Paket. In (3) ruft der Server eine Funktion auf, die aus dem erhaltenen Paket die nötigen Informationen extrahiert, den Client-Ausweis überprüft und wieder ein Paket (diesesmal für den Client) verpackt. Dieses Paket enthält jetzt den Ausweis des Servers und den verschlüsselten geheimen Session-Key K_{CS} und wird in (4) zum Client zurückgeschickt. Der Client packt dieses Paket in (5) wieder aus, überprüft den Server-Ausweis. Ist der Ausweis in Ordnung, so 'merkt' er sich den gemeinsamen Session-Key und der Kontext-Aufbau ist erfolgreich abgeschlossen. Der *symmetrische* Session-Key wird, falls die Kommunikation verschlüsselt ablaufen soll, in allen GSS-Mechanismen ausgetauscht, da asymmetrische Verschlüsselung großer Nachrichtenblöcke zu zeitaufwendig ist. D.h. auch bei den public-key basierten Mechanismen wird während der Nachrichtenübermittlung eigentlich ein *Hybrid-Verfahren* verwendet.

Nun sind sich Client und Server sicher, daß mit der richtigen Gegenseite kommuniziert wird, und außerdem ist auf beiden Seiten der gemeinsame, geheime Session-Key K_{CS} bekannt, der bei der eigentlichen Datenübertragung zum Authentizitätsnachweis und optional zum Verschlüsseln des Datenstroms mit verwendet werden kann.

Geht bei diesem Kontext-Aufbau irgendetwas schief, ist z.B. ein Ausweis nicht in Ordnung, so wird der Aufbau abgebrochen und die bereits aufgebauten Kontext-Teile verworfen. Wird ein GSS-Kontext nicht mehr gebraucht, so wird er einfach gelöscht. Für eine detailierte Beschreibung der angesprochenen Funktionen und weitere administrative Routinen sei der geneigte Leser an [GSS-API] und [GSS-C-Bindings] verwiesen.

In den folgenden Kapiteln wollen wir nun konkrete Sicherheitsmechanismen vorstellen, die sich hinter den angesprochenen GSS-Aufrufen verbergen können. Der Unterschied besteht weniger in den Paketen, die die Nachrichten gesichert übertragen (sog. *'Per-Message-Tokens'*), als in den oben verschickten *'Context-Level-Tokens'*, die für den Kontext-Aufbau und die Beschaffung der Ausweise zuständig sind. Die eben angesprochene Beschaffung der Ausweise wird übrigens durch den GSS-Aufruf **GSS_Acquire_cred( )** angestoßen. Was dann vom unterliegenden Sicherheits-System gemacht wird ist natürlich für jeden GSS-Mechanismus verschieden.

In GSS sind nur *Schnittstellen für Funktionen* festgelegt, die von einer Anwendung aufgerufen werden können. Was in diesen Funktionen genau geschieht, was genau in diese Pakete gepackt wird und wie mit dem Inhalt konkret umgegangen wird, ist nicht in GSS, sondern in der Beschreibung der einzelnen Mechanismen (wie z.B. Kerberos, SPKM oder SECUDE) geregelt.

Kerberos

Ein möglicher GSS-Mechanismus ist *Kerberos V5*. Hierbei handelt es sich um ein vom MIT Mitte der 80'er Jahre entwickeltes Sicherheitspaket, das wir im folgenden kurz erläutern wollen. Der Name 'Kerberos' stammt übrigens aus der griechischen Mythologie. Dort war Kerberos der dreiköpfige Wachhund der Unterwelt[5]. Auch hier stellen wir uns den gesicherten Verbindungsaufbau zwischen Client und Server vor. Jeder Teilnehmer (Client und Server) teilt zu Beginn einen geheimen DES-Schlüssel mit dem Authentifikations-Server von Kerberos. Tatsächlich wird der Client beim Login sein Paßwort eingeben, woraus durch eine kryptographische Hash-Funktion dieser Schlüssel K_C abgeleitet wird. Nach diesem Login wird nun die Anwendung den Aufruf **GSS_Acquire_cred( )** absetzen, der wiederum die unten aufgeführten Schritte (1) bis (4) bewirkt. Eine technisch vollständige Darstellung findet sich beispielsweise in [Schneier94], S. 417 ff. oder [Kerberos].

Ziel der Schritte (1) bis (4) ist es ein sogenannten Server-Ticket

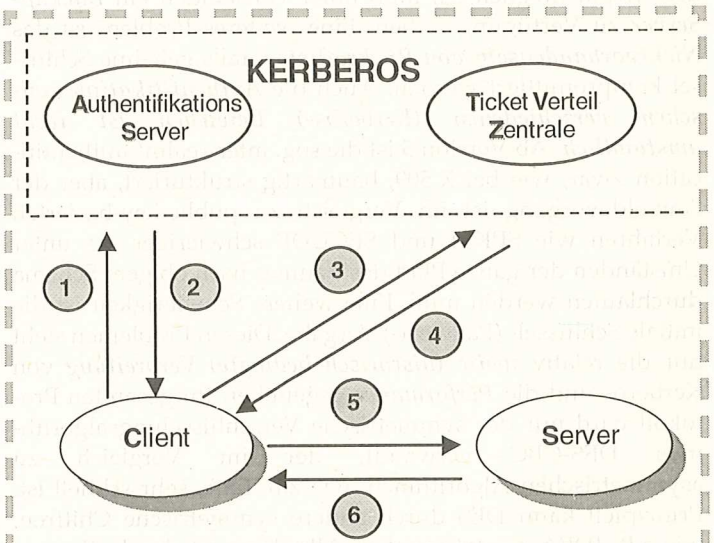


Abbildung 2: Kerberos Authentifikation

zu erhalten, das in der GSS-Sprache dem *credential* entspricht. Um diesen Ausweis zu erhalten wird sich der Client in (1),(2) ein Ticket für die Ticket-Verteil-Zentrale (TVZ) abholen. Mit diesem TVZ-Ticket, kann er nun von der TVZ das gewünschte Server-Ticket erhalten ((3),(4)). Ein solches Ticket hat eine begrenzte Lebensdauer, enthält u.a. den Session-Key zwischen Client und der angesprochenen Stelle (d.h. TVZ oder Server) und ist schließlich mit dem geheimen Schlüssel der addressierten Stelle verschlüsselt. Deshalb kann nur die angesprochene Stelle, z.B. die TVZ oder der Server mit dem Ticket 'etwas anfangen'. Die beiden letzten Schritte (5) und (6) dienen der eigentlichen Authentifikation, wie in Kapitel 2 skizziert.

Die Philosophie hinter dem Kerberos-Protokoll ist uns sicherlich von (meist amerikanischen) Volksfesten her bekannt. Dort wird man zuerst zur Kasse (TVZ) gehen und einen Bon (Ticket) erwerben, bevor man sich (am Server) z.B. ein Bier abholt. Diese Vorgehensweise bringt neben der scheinbaren 'Umständlichkeit' auch einige Vorteile mit sich: Stellen wir uns vor, wir hätten jedesmal panische Angst vor einem räuberischen Überfall, wenn wir den Geldbeutel zum Bezahlen zücken[6]. Dieses Vorgehen erlaubt es uns den Geldbeutel nur einmal aus der relativ sicheren Hosentasche zu nehmen, egal wieviel Durst wir haben. Hier ist es ähnlich. Der geheime Schlüssel zwischen Client und Kerberos ist nur für kurze Zeit (1)-(2) im unsicheren Speicher. Gelingt es einem Angreifer den Speicher auszulesen, so erhält er sehr wahr-

5. Wenn man davon ausgeht, daß Kerberos heute die Daten großer Unternehmen 'bewacht', hat sich in den letzten Jahrtausenden kaum etwas verändert.

6. Sie halten diese Angst für übertrieben? Sie haben wahrscheinlich recht! Doch die Grenze zwischen solidem Sicherheits-Design und Paranoia ist fließend.

scheinlich nur das Ticket mit begrenzter Lebensdauer und nicht den geheimen Schlüssel K_C.

Schließlich wollen wir uns noch über die Vor- und Nachteile von Kerberos Gedanken machen. Eine große Schwierigkeit für die Praxis dürfte der *physikalisch zu sichernde Kerberos-Server* sein. Gelingt es einem Angreifer unerlaubt auf den Kerberos-Server und die dort gespeicherten geheimen Schlüssel zuzugreifen, so kann er unbemerkt alle beteiligten User und Server maskieren. Da ohne diesen zentralen Dienst kein Login möglich ist, muß unter Umständen ein *Backup-Server* zu Verfügung stehen. Eine weiteres Problem ist das *Nichtvorhandensein von Rückruflisten*, falls geheime Schlüssel kompromittiert werden. Auch die *Authentifikation zwischen verschiedenen (Kerberos-) Bereichen ist recht umständlich*. Ab Version 5 ist die sog. inter-realm[7] authentification zwar, wie bei X.509, baumartig strukturiert, aber der Anmeldevorgang ist im Vergleich zu public-key-basierten Verfahren wie SPKM und SECUDE schwieriger, da unter Umständen der ganze Pfad des Baumes nach obigem Schema durchlaufen werden muß. Eine weitere Schwierigkeit ist die initiale Schlüssel- (Paßwort-) Vergabe. Diesen Problemen steht nur die relativ *weite (historisch bedingte) Verbreitung* von Kerberos und die *Performance* gegenüber. Im gesamten Protokoll wird nur der symmetrische Verschlüsselungsalgorithmus DES-CBC verwandt, der im Vergleich zu asymmetrischen Algorithmen, wie z.B. RSA, sehr schnell ist. Prinzipiell kann DES durch andere symmetrische Chiffren, wie z.B. IDEA ersetzt werden. Allerdings ist durch die ausschließliche Verwendung von symmetrischen Verschlüsselungsalgorithmen die *Kommunikation stets abstreitbar*.

SPKM

Aus den oben genannten Gründen wurde in [SPKM] ein GSS-Mechanismus vorgeschlagen, der mit public-key-Verfahren arbeitet. Auch hier wollen wir nur ein Gefühl für die dahinterliegenden Ideen vermitteln. Für eine technische Dokumentation sei der geneigte Leser an [SPKM] verwiesen.

Die Grundidee hinter SPKM[8] ist, sich die offensichtlichen Vorteile der public-key-Kryptographie zunutze zu machen. Das bedeutet, daß die Forderung eines Trusted Servers, wie bei Kerberos *nicht nötig* ist. Die benötigten credentials (Ausweise) sind hier geheime asymmetrische Schlüssel und X.509-Zertifikate der öffentlichen Schlüssel. Das Schlüsselmanagement für SPKM und eine Möglichkeit die aus Sicherheitsgründen sehr sinnvolle 'Ticket-Philosophie' von Kerberos auf SPKM und SECUDE zu übertragen wurde in näher [CredMan] beleuchtet. Der Verbindungsaufbau erfolgt in einer Ein-, Zwei- oder Drei-Wege-Authentifikation zwischen Client und Server. Bei der Ein- und Zwei-Wege Authentifikation sind sichere *Zeitstempel* nötig, damit ein Angreifer nicht einfach die möglicherweise aufgezeichneten Authentifikations-Token ein weiteres Mal verschicken und damit z.B. den Client maskieren kann. Bei der Dreiwege-Authentifikation sind diese Zeitstempel nicht nötig, da hier eine 'frische' *Zufallszahl* mitgeschickt und später mit der Zufallszahl in der zurückerhaltenen Nachricht verglichen wird.

Damit eine größtmögliche Flexibilität erreicht werden kann, schreibt SPKM nicht die Verwendung bestimmter Algorithmen vor, sondern läßt Client und Server vielmehr aus einer Reihe verfügbarer Algorithmen auswählen. Einige Algorithmen stellen die 'Mindestanforderungen' für den Betrieb dar. So sind als Integritäts-Algorithmen[9], neben den DES-basierten MAC's (wie bei Kerberos), auch wirkliche Signatur-Algorithmen, wie **MD5WithRSA** vorgesehen. In Anwendungsgebieten, in denen die Nichtabstreitbarkeit der Kommunikation gefordert werden muß (z.B. Vertragsabschlüsse, Bestellungen, ...) ist die Anwendung solcher Signatur-Algorithmen nicht zu umgehen. Andererseits ist es klar, daß die Erstellung einer RSA-Signatur wesentlich länger dauert, als die simple DES-Verschlüsselung des Hashwertes der Nachricht. Für die (optionale) Verschlüsselung[10] ist, wie bei Kerberos und SECUDE auch, z.B. **DES-CBC** vorgesehen. Für die Authentifikation[11] ist u.a. **RSAEncryption** vorgesehen. Da die Schlüssellänge der zum Kontext-Aufbau verwendeten Algorithmen in der Regel nicht mit der Schlüssellänge des Verschlüsselungsalgorithmus übereinstimmt, sind schließlich Einweg-(Hash-) Funktionen für die Ableitung des Session-Keys angegeben.

Durch den flexiblen Ansatz müssen sich Client und Server natürlich zu Beginn des Kontext-Aufbaus auf die verwendbaren Algorithmen einigen. Derartige Verhandlungen sind jedem Touristen, der der jeweiligen Landessprache nicht mächtig ist, bestens bekannt. "Entschuldigen Sie, sprechen Sie deutsch?" - Kopfschütteln - "Maybe, we could speak english?" - ... . Es ist klar, daß die Aushandlung der Algorithmen unter Umständen einige Zeit dauern kann und nicht in jedem Fall erfolgreich sein muß. Da bei diesen Verhandlungen eine ganze Menge an (ASN.1) Codierung und Decodierung nötig ist, geht beim Verbindungsaufbau zusätzliche Zeit verloren.

Lassen Sie uns schließlich auch hier die Vor- und Nachteile von SPKM nocheinmal explizit zusammentragen. Im Gegensatz zu Kerberos ist *kein vertrauenswürdiger Authentifikations-Server nötig*. Dafür müssen für die beteiligten Parteien Zertifikate der öffentlichen Schlüssel vorhanden oder leicht zu beschaffen sein. Das dürfte mittelfristig nicht das große Problem sein, da nach Inkrafttreten des Signaturgesetzes diese Public-Key-Infrastruktur für PEM und ähnliche Anwendungen sowieso vorhanden sein muß. Die Kommunikation kann durch den Einsatz von digitalen Signaturen *nichtabstreitbar* gemacht werden. Ein weiteres Plus ist die *Flexibilität*, da verschiedenste Algorithmen verwendet werden können. Der Preis, der dafür bezahlt wird ist der *Verhandlungs-Overhead* zu Beginn der Kommunikation. Nicht zu vergessen ist, daß der Verbindungsaufbau zu *bereichsfremden Gegenstellen*, im Gegensatz zu Kerberos, *keine zusätzlichen Probleme* macht.

SECUDE

In diesem Abschnitt wollen wir uns schließlich, wie versprochen mit einem weiteren GSS-Mechanismus befassen. SECUDE ist eigentlich mehr, als ein GSS-Mechanismus. SECUDE[12] ist ein multifunktionaler Werkzeugkasten für die Entwicklung sicherer Anwendungen, der im Rahmen von Sicherheits-Forschungsprojekten in der GMD entwickelt wurde. Ein Baustein dieses Sicherheitspaketes ist nun der im

7. Ein Paar aus Authentifikations-Server und TVZ ist immer für einen Kerberos-realm (Bereich) zuständig. Eine inter-realm authentication tritt also auf, wenn ein User z.B im Bereich mit.edu (Massachusets Institute of Technology) mit einem Server im Bereich cmu.edu (Carnegie Melon University) kommunizieren will.
8. Simple Public-Key Mechanism
9. in **GSS_GetMIC( )**
10. in **GSS_WRAP( )**
11. in **GSS_Init_sec_context( )** und **GSS_Accept_sec_context( )**
12. SECUrity Development Environment

folgenden kurz erläuterte SECUDE-GSS-Mechanismus. Aus der Diskussion der Kerberos- und SPKM-Mechanismen sollte klar geworden sein, daß der Einsatz von Public-Key-Verfahren zur Authentifikation (wie bei SPKM) entscheidende Vorteile mit sich bringt. Allerdings bringt der flexible Ansatz von SPKM einen gewissen Overhead mit sich, der nicht in jedem Fall nötig ist. Man könnte sich vorab auf die verwendbaren Algorithmen einigen und somit eine Menge ASN.1-(De-) Codierung und das Verhandlungsprotokoll zu Beginn sparen. Da sichere Zeitstempel nicht überall garantiert werden können, entscheidet man sich für die Drei-Wege-Authentifikation (mit 'frischen' Zufallszahlen). Allerdings sind bei der klassischen X.509-Drei-Wege-Authentifikation auf jeder Seite drei recht kostspielige z.B. RSA-Operationen nötig, wobei die letzte (auf jeder Seite) durch schnellere symmetrische DES-Verschlüsselung, mit dem in den ersten beiden Schritten vereinbarten Session-Key, ersetzt werden kann. Außerdem muß bei der X.509 Drei-Wege-Authentifikation der Client bereits vor dem ersten Schritt im Besitz des Server-Zertifikates sein, was die Existenz eines Message-Servers voraussetzt, der über die aktuell verfügbaren Server Buch führt und die entsprechenden Server-Zertifikate bereitstellt. Für Anwendungsszenarien in denen dieser Message-Server nicht zu Verfügung steht, wurde der im folgenden kurz geschilderte SECUDE-GSS-Mechanismus entwickelt.

Nach dem Login (1), bei dem sich der Client durch sein Passwort bei seiner persönlichen Sicherheitsumgebung (PSE, z.B. Chipkarte) identifiziert und damit Zugriff auf seinen geheimen Schlüssel hat, schickt er in (2) sein Zertifikat $Zert_C$ zusammen mit einer Zufallszahl R zum Server. Der Server überprüft in (3) das mitgeschickte Zertifikat, generiert den geheimen (DES-CBC-) Session-Key K_{CS}, verschlüsselt diesen mit dem öffentlichen Schlüssel des Clients (d.h. $M=Enc(K_{CS},Pk_C)$) und signiert schließlich den Hashwert h(M|R) aus dem für den Client verschlüsselten Session-Key und der Zufallszahl mit seinem geheimen Schlüssel Sk_S (d.h. $S=Dec(h(M|R),Sk_S)$). In (4) schickt er die Signatur S, den (asymmetrisch) verschlüsselten Session-Key M und sein Zertifikat $Zert_S$ zum Client. Dieser überprüft wiederum (in Schritt (5)) das mitgeschickte Zertifikat des Servers, entschlüsselt mit seinem geheimen Schlüssel den Session-Key K_{CS}, überprüft mit dem im Zertifikat enthaltenen öffentlichen Schlüssel Pk_S des Servers die Signatur über den Hashwert h(M|R). Ist alles ok, so verschlüsselt er den Hashwert der Zufallszahl R mit dem ausgehandelten Session-Key K_{CS} und schickt $\{h(R)\}K_{CS}$ zum Server zurück. Der Server überprüft schließlich, ob auch der Client im Besitz des Session-Keys ist, indem er das empfangene Token mit dem Session-Key entschlüsselt und mit h(R) vergleicht.

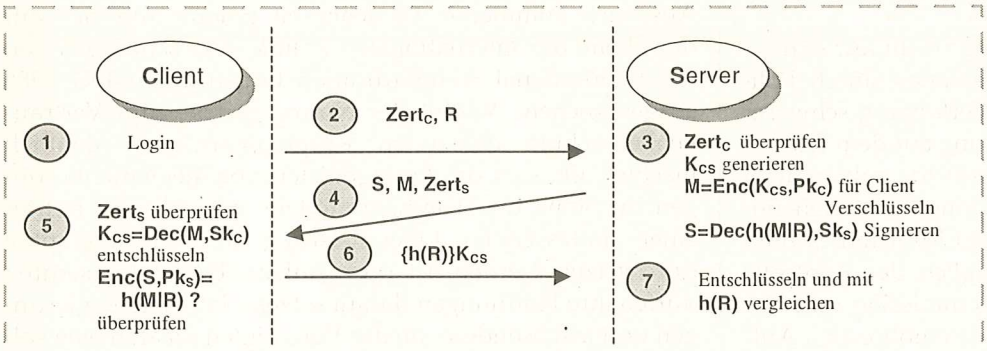


Abbildung 3: SECUDE Authentifikation

Der *Unterschied zur klassischen X.509-Drei-Wege-Authentifikation*, wie sie in SPKM Verwendung findet, ist wie gesagt, daß die Zufallszahl in (2) *nicht* vom Client *signiert* wird und die Verschlüsselung (6), mit der sich der Client beim Server authentifiziert, mit einer schnellen *symmetrischen Verschlüsselung* durchgeführt wird.

Zusammenfassung

Abschließend wollen wir die Vor- und Nachteile der vorgestellten Mechanismen hier noch einmal zusammentragen und bevorzugte Einsatzgebiete aufzeigen.

Für den Einsatz von **Kerberos** als GSS-Mechanismus spricht nur der *schnellere Verbindungsaufbau*, da keine kostspieligen RSA-Operationen benötigt werden, sowie die relativ weite Verbreitung. Dafür muß aber ein *physikalisch sicherer Authentifikations-Server* zu Verfügung stehen. Müssen Teile der Kommunikation *verbindlich* sein (für z.B. Verträge oder Bestellungen) oder häufig Verbindungen über *Bereichsgrenzen* hinaus aufgebaut werden, so *scheidet Kerberos aus*.

Ist eine *Public-Key-Infrastruktur* (z.B. für PEM, S/MIME, ...) vorhanden oder relativ leicht bereitzustellen, so sollte in jedem Fall **SPKM** oder **SECUDE** verwendet werden.

Kann die Existenz eines koordinierenden *Message-Servers* oder die Verfügbarkeit der Server-Zertifikate zu Beginn garantiert werden, und *nicht* abgesehen werden, daß *alle beteiligten Parteien über die gleichen Algorithmen verfügen*, so sollte **SPKM** verwendet werden.

Kann man sich jedoch vorab *auf die verwendbaren Algorithmen einigen* und stellt die initiale Verteilung der *Server-Zertifikate unter Umständen ein Problem* dar (d.h. kein Message-Server), so sollte der **SECUDE**-Mechanismus bevorzugt werden. Der *Verbindungsaufbau ist um einiges schneller* als bei SPKM. In einer kommenden Version des SECUDE-Werkzeugkastens wird neben dem 'hauseigenen' Mechanismus auch SPKM enthalten sein.

Literatur

[Cred-Man] D. Hühnlein: "Credential Management and Secure Single Login for SPKM", eingereicht für Internet Society Symposium on Network and Distributed System Security, März 1998

[GSS-API] J. Linn: "Generic Security Service Application Program Interface", RFC 1508*, Sep. 1993

J. Linn: "Generic Security Service Application Program Interface", Version 2", RFC 2078*, Jan. 1997

[GSS-C-Bindings] J. Wray: "Generic Security Service API: C-bindings", RFC 1509*, Sep. 1993

[Kerberos] J. Kohl, C. Neumann: "The Kerberos Network Authentication Service (V5)", RFC 1510*, Sep. 1993

J. Linn: "The Kerberos Version 5 GSS-API Mechanism", RFC 1964*, Juni 1996

[Schneier94] B. Schneier: "Applied Cryptography, Protocols, Algorithms and Source Code in C", J. Wiley & Sons, New York, 1994

[SPKM] C. Adams: "The Simple Public-Key GSS-API Mechanism (SPKM)", RFC 2025*, Okt. 1996

* alle RFC's können übrigens über http://www.internic.net/ds/rfc-index.html bezogen werden

[SECUDE]"SECUrity Development Environment for Open Networks - Online Dokumentation", http://www.darmstadt.gmd.de/secude/Doc/index.htm

Olaf Winkel

Elektronische Kryptographie

Herausforderung für die demokratische Gesellschaft

Die digitale Verschlüsselung als politisches Problem

Die elektronische Kryptographie stellt ein wirksames Mittel dar, um die Informationen und Kommunikationsbeziehungen von Bürgerinnen und Bürgern in telematischen Netzwerken vor einer unerwünschten Kenntnisnahme durch Dritte zu schützen. Die Verbreitung digitaler Schlüsselsysteme ermöglicht aber nicht nur eine effektive Abwehr illegaler Übergriffe, sondern verhindert auch legale Abhöraktionen zur Bekämpfung krimineller und verfassungsfeindlicher Aktivitäten durch staatliche Sicherheitsbehörden. Damit prallen die für sich legitimen Interessen der Wahrung von Fernmeldegeheimnis und Datenschutz auf der einen Seite und der Aufrechterhaltung der staatlichen Ordnung auf der anderen Seite in der virtuellen Welt der Netze unvermittelt und mit großer Wucht aufeinander.

In der Bundesrepublik sind allerdings nicht nur richterlich angeordnete Überwachungsmaßnahmen durch Polizei, Staatsanwaltschaft und Zoll zur Verfolgung schwerer Straftaten zulässig, die einer Überprüfung auf dem Rechtsweg offenstehen. Zur gängigen Abhörpraxis zählen auch die in einer Grauzone liegenden Aktionen von Geheimdiensten und Verfassungsschutz, die per Ministerbeschluß angeordnet werden können und lediglich der Kontrolle einer exklusiven parlamentarischen Kommission unterliegen. Dies hat in der Vergangenheit einer emotionalen Aufheizung der Diskussion um einen sinnvollen gesellschaftlichen Umgang mit der digitalen Kryptographie Vorschub geleistet, was angesichts der ständig wachsenden Bedeutung dieser Frage bedauerlich ist.

Die mit der Entwicklung und Verbreitung elektronischer Schlüsselsysteme verbundenen Probleme sucht man derzeit in unterschiedlichen Staaten mit unterschiedlichen kryptopolitischen Strategien zu bewältigen, und zwar auf den Wegen des generellen Verbotes, der unbeschränkten Freigabe und der treuhänderischen Hinterlegung kryptographischer Schlüssel. Angesichts der Globalität der Netzwerke und neuer technischer Verfahren, die nationalstaatliche Regulierungen weitgehend ins Leere laufen lassen, mehren sich inzwischen die Befürworter der Freigabestrategie.

Prinzipiell zulässig ist vertraulichkeitsschützende Kryptographie etwa in Schweden, Dänemark, der Schweiz und Deutschland[1], generell verboten ist sie in Rußland, und sie war es noch bis vor kurzem in Frankreich. Die Regierung der Vereinigten Staaten setzt trotz massiver innenpolitischer Widerstände weiterhin auf das vermittelnde Modell der Schlüsselhinterlegung, nach dem Duplikate der von den Teilnehmern verwendeten Schlüssel bei Treuhandeinrichtungen zu hinterlegen und den Sicherheitsbehörden zum Zwecke legaler Abhöraktionen auszuhändigen sind. Allerdings verfolgt Washington das Treuhandkonzept nicht in seiner Reinform – was erstens die Zulassung von in ihrer Länge unbeschränkten Schlüsseln, zweitens die Einrichtung behördenunabhängiger Treuhandstellen und drittens die Schaffung rechtsstaatlich einwandfreier Regelungen für die Herausgabe von Schlüsselduplikaten voraussetzen würde – sondern in einer abgewandelten Variante, die zwar zu Recht auf Mißtrauen gestoßen ist, das gesamte Modell aber zu Unrecht diskreditiert hat. Frankreich und Großbritannien verfolgen seit kurzer Zeit einen ähnlichen kryptopolitischen Kurs wie die Vereinigten Staaten, widersetzen sich aber Bestrebungen, eine US-Lösung auf die internationale Ebene zu übertragen.

Diese Heterogenität der Strategien und die darin zum Ausdruck kommende Unsicherheit potenzieren sich auf der Ebene der internationalen Politik, was schon das von der International Standardisation Organisation ISO 1986 ausgesprochene Verbot der Normung von zum Vertraulichkeitsschutz dienenden Kryptoalgorithmen deutlich machte[2]. Ob sich die Protagonisten von Reglementierungen im Sinne des Treuhandmodells oder die Verfechter einer umfassenden Liberalisierung der Kryptographie durchsetzen werden, ist noch unklar. Die erstgenannten dürfen ihre Hoffnungen darauf setzen, daß viele Regierungen und insbesondere die der Vereinigten Staaten eine solche Position zu ihrer innenpolitischen und außenpolitischen Leitlinie gemacht haben. Die letztgenannten können sich dagegen auf technische Sachzwänge berufen, die immer mehr Fachleute dazu veranlassen, von jeder Form der Regulierung abzuraten.

1. Zwar verpflichtet die im Mai 1995 verabschiedete Fernmeldeüberwachungsverordnung die Betreiber von mit kryptographischen Sicherheitsmechanismen ausgestatteten Telekommunikationsnetzen zur Bereitstellung von Schnittstellen, die im Bedarfsfall Überwachungsaktionen der Sicherheitsbehörden ermöglichen sollen, die Anwender können digitale Schlüsselsysteme aber weiterhin auf dem freien Markt erwerben und legal einsetzen. So darf sich ein Mobilfunkteilnehmer, der den Verschlüsselungsdiensten der D-Netze oder des E-Netzes mißtraut, bei der Kommunikation in diesen Netzen durchaus eigener Verschlüsselungstechnik bedienen. Dies macht die Fernmeldeüberwachungsverordnung zu einem weitgehend wirkungslosen Instrument und kann durchaus als weiteres Indiz für die These angesehen werden, daß die rasante Ausbreitung der Computernetze die tradierten Formen des gesellschaftlichen Risikomangementes mit dem Ergebnis überfordert, daß unterschiedliche Akteure an unterschiedlichen Stellen des Systems unkoordinierte Entscheidungen produzieren.
2. Die Normierung derartiger Algorithmen, die den wesentlichen Kern moderner Schlüsselsysteme bilden, wäre eine grundlegende Voraussetzung dafür, daß in offenen Systemen Nachrichten ohne vorbereitende Maßnahmen vertraulich ausgetauscht werden können. Während Normen in vielen anderen Bereichen lediglich der Wirtschaftlichkeit dienen, stellen sie im Fernmeldewesen und in der Kryptographie nämlich eine funktionsnotwendige Voraussetzung dar.

Die Irritationen und Kontroversen, die die elektronische Kryptographie nicht nur in den einzelnen Ländern, sondern auch auf der angesichts der Globalität der Netze entscheidenden internationalen Ebene hervorruft, resultieren aus deren besonderer und vielschichtiger politischer Bedeutung. Die Frage eines sinnvollen gesellschaftlichen Umgangs mit der digitalen Verschlüsselung ist nämlich nicht nur innenpolitisch, wirtschaftspolitisch und gesellschaftspolitisch von großer Brisanz, sondern ragt sogar in die sensibelsten Bereiche der internationalen Politik hinein. Sollte es nämlich einem staatlichen Akteur in einer sich zunehmend virtualisierenden Welt gelingen, den Zugriff auf weltweit eingesetzte Schlüssel zu erhalten, würde er sich damit uneinholbare Vorteile gegenüber anderen Nationen verschaffen. Bei allen Überlegungen zur Demokratieverträglichkeit von elektronischer Verschlüsselung muß daher berücksichtigt werden, daß diese zwar eine wichtige, aber keineswegs die einzige Dimension des Kryptographieproblems aufgreifen.

Die Demokratie als System mit mehreren Ebenen

Da die elektronische Verschlüsselung eine wirksame Abschirmung von Informationen und Kommunikationsbeziehungen gegenüber Dritten ermöglicht, ist sie prinzipiell auch geeignet, die freie Rede zu schützen. Dieser Umstand reicht aber noch nicht aus, um diese Technik generell als Gewinn für die demokratische Gesellschaft erscheinen zu lassen, denn Demokratie ist mehr als das Recht der freien Rede allein. Sie setzt darüber hinaus ein System von Regeln und Sanktionsmechanismen voraus, das die freie Rede in politisch konstruktive Bahnen der kollektiven Willensbildung und Entscheidungsfindung lenkt und dafür sorgt, daß der die demokratische Gesellschaft konstituierende Wertkonsens unangetastet bleibt. Demokratie hat also nicht nur einen libertären Aspekt, sondern auch einen Herrschaftsaspekt, und das hohe demokratische Niveau der modernen Gesellschaft resultiert vor allem daraus, daß sich in der Tradition Montesquieus ein System von Gewichten und Gegengewichten herausgebildet hat, mit dessen Hilfe diese widerstreitenden Anforderungen immer wieder in ein ausgewogenes Verhältnis gebracht werden können. Auch die Frage nach den Auswirkungen, die die unterschiedlichen kryptopolitischen Strategien im Hinblick auf die Entwicklung des demokratischen Systems im elektronischen Zeitalter in Aussicht stellen, verlangt nach einer in dieser Weise differenzierenden Antwort. Um die Probleme auf den Punkt zu bringen, wird in den folgenden Betrachtungen das Szenario einer digitalisierten Informationsgesellschaft zugrunde gelegt, d. h. einer Gesellschaft, die sich unter anderem dadurch auszeichnet, daß wesentliche soziale und damit auch politische Funktionen exklusiv über telematische Systeme abgewickelt werden. Daß andere Szenarien nicht nur denkbar, sondern auch plausibler sind, bleibt dabei unbestritten.

Die Demokratieverträglichkeit der Freigabestrategie

Durch die Freigabe von vertraulichkeitsschützender Krypotographie könnte der Schutz der Privatsphäre in einer sich zunehmend virtualisierenden Welt nicht nur wirksam fortgeführt, sondern sogar perfektioniert werden; erhielten die Bürgerinnen und Bürger auf diese Weise doch erstmals die Chance, die Verwirklichung des Fernmeldegeheimnisses und des Rechtes auf informationelle Selbstbestimmung mit eigenen Mitteln sicherzustellen. Verwehrte man ihnen dagegen den Zugang zur Verschlüsselung, könnte dies unter den soziotechnischen Bedingungen einer digitalisierten Informationsgesellschaft Bespitzelungsaktionen in einem nie zuvor gekannten Ausmaß nach sich ziehen. Nicht von der Hand zu weisen sind aber auch die Einwendungen der Sicherheitsbehörden, die beklagen, daß die freie Verfügbarkeit digitaler Schlüsselsysteme ein wichtiges Mittel zur Bekämpfung krimineller und verfassungsfeindlicher Aktivitäten wirkungslos werden ließe. Zwar bestünde in diesem Falle weiterhin die Möglichkeit, in Telekommunikationsnetzen legale Abhöraktionen durchzuführen, diese förderten dann aber nur noch unlesbares Chiffrat zutage und wären damit wertlos.

Daß Kriminelle und Verfassungsfeinde zu jenen Kräften gehören, die sich die Vorteile der modernen Verschlüsselungstechnik von Beginn an zunutze gemacht haben, ist längst erwiesen. Die Verbreitung von Kinderpornographie und nationalsozialistischer Propaganda gehört heute zum Alltag des Internet. Außerdem ist davon ausgehen, daß sich mit dem Übergang der modernen Gesellschaft in das elektronische Zeitalter nicht nur neue Kriminalitätsformen wie elektronische Geldwäsche, elektronisches Glücksspiel oder neue Formen der Erpressung entwickeln werden, sondern ebenso neue Formen des Terrorismus wie das Einschleusen von Viren in die Informationssysteme von Behörden und Unternehmen.

In einem Netz, das große gesellschaftliche Bedeutung hat, aber keiner hoheitlichen Sanktionierung unterliegt, könnte es schließlich auch zu einer Beeinträchtigung und Deformation politischer Prozesse kommen. Nicht nur, daß es in einer virtuellen öffentlichkeit keine Mittel gibt, die digitale Versendung von sexistischen, antisemitischen und anderen rassistischen Nachrichten zu verhindern oder zumindest durch Gegendarstellungen zu entschärfen und strafrechtlich zu ahnden, es könnten sich zudem kommerzielle Einrichtungen etablieren, die im Auftrag finanzstarker Interessengruppen politisch mißliebige Stimmen zum Verstummen bringen, indem sie deren Netzzugänge unerkannt und ungestraft mit Datenmüll blockieren. Damit wäre die Verbreitung der elektronischen Kryptographie unter bestimmten Umständen sogar geeignet, nicht nur die Regelungssysteme, die Sanktionsmechanismen und die Geltung der Grundwerte der demokratischen Gesellschaft in der virtuellen Welt außer Kraft zu setzen, sondern auch das Recht der freien Rede selbst.

Vor diesem Hintergrund bleibt festzuhalten, daß die Freigabestrategie, deren Realisierung den geringsten technischen und organisatorischen Aufwand erfordert und

auch den einfachsten Weg zu einer sicheren grenzüberschreitenden Telekommunikation weist, im Hinblick auf ihre Verträglichkeit für das demokratische System durchaus ernstzunehmende Probleme aufwirft.

Die Demokratieverträglichkeit der Verbotsstrategie

Ein generelles Verbot von Kryptierverfahren würde das Spannungsverhältnis von bürgerlichem Freiheitsanspruch und staatlichem Machtanspruch in einer sich zunehmend virtualisierenden Welt einseitig zugunsten des letztgenannten Aspektes auflösen. Daß eine solche Praxis mit den verfassungsmäßigen Grundlagen einer modernen Demokratie kaum zu vereinbaren wäre, liegt auf der Hand. Andererseits erscheint sie aber zumindest auf den ersten Blick am besten geeignet, unter den veränderten technischen Bedingungen weiterhin effektive Abhöraktionen der Sicherheitsbehörden zu ermöglichen. Bei näherer Betrachtung offenbaren sich jedoch auch in dieser Hinsicht gravierende Probleme, da ein Kryptographieverbot von widerstrebenden Teilnehmern durch die Verwendung illegaler Schlüsselsysteme leicht unterlaufen werden könnte. Daß sich gerade die für die staatliche Überwachung besonders interessanten Kreise wie kriminelle und extremistische Organisationen einem solchen Verbot unterwerfen würden, ist nicht anzunehmen. Um es unerkannt zu umgehen, könnten diese etwa auf die sogenannte Steganographie zurückgreifen, mit deren Hilfe sich Geheimnisse in scheinbar unverfänglichen Informationen – etwa im Hintergrundrauschen einer übertragenen Nachricht – verbergen lassen, so daß selbst die Tatsache der Verschlüsselung geheim bleibt. Das Nachsehen hätten wohl vor allem die gesetzestreuen Bürgerinnen und Bürger, denen man die technische Realisierung des Privatheitsschutzes verweigerte.

Die Strategie eines generellen Verbotes erscheint daher zur Lösung des Kryptographieproblems nicht nur unter verfassungsrechtlichen Gesichtspunkten, sondern auch unter Praktikabilitätsaspekten äußerst fragwürdig.

Die Demokratieverträglichkeit der Treuhandstrategie

Im Ansatz der treuhänderischen Schlüsselhinterlegung kommt – wenn er in seiner Reinform verwirklicht und nicht zur Verschleierung anderer Interessen mißbraucht wird – der Wunsch zum Ausdruck, das in der modernen Gesellschaft erreichte Gleichgewicht von individuellen Freiheitsrechten und staatlichen Machtansprüchen durch die Schaffung eines differenzierten Systems von Regeln und wechselseitig wirksamen Kontrollmechanismen in das elektronische Zeitalter hinüberzuretten. Dies ist seine Stärke, und hier liegt seine Existenzberechtigung. In Deutschland würde eine konsequente Implementation des Treuhandmodells allerdings eine Neuregelung der Abhörrechte von Geheimdiensten und Verfassungsschutz voraussetzen, da diese in ihrer gegenwärtigen Form einer angemessenen und transparenten Regelung der Herausgabe von Schlüsselduplikaten entgegenstehen.

Inwieweit das Schlüsselhinterlegungskonzept dazu dienen kann, den Spielraum der Behörden zur Bekämpfung krimineller und verfassungsfeindlicher Aktivitäten im technischen Wandel zu sichern, ist umstritten. Wie bei einer Verbotslösung muß man auch bei einer Treuhandlösung davon ausgehen, daß das organisierte Verbrechen und verfassungsfeindliche Organisationen auf lückenlose Kryptierungsverfahren nicht verzichten würden, was das Verhältnis von Aufwand und Ertrag einer solchen Strategie auch unter demokratiespezifischen Aspekten empfindlich zu Lasten der Ertragsseite verschiebt.

Daneben weist die Treuhandstrategie einen weiteren gravierenden Mangel auf: Er liegt darin, daß die Schutzmaßnahmen nur solange wirksam sein könnten, wie sich die Schlüsselduplikate in den Treuhandeinrichtungen lückenlos gegenüber rechtswidrigem Zugriff abschotten ließen. Mit der zunehmenden Übertragung sozialer Funktionen von Menschen auf telematische Systeme und mit wachsendem Sicherheitsbedürfnis der Telekommunikationsteilnehmer würden sich diese aber zwangsläufig zu äußert gefährdeten Bereichen entwickeln, zur Achillesferse des gesamten Systems. Wer sich Zugriff auf die Schlüsselduplikate verschaffen könnte, verfügte nämlich über eine nie gekannte Machtfülle. Mit ihrer Hilfe wäre es Angreifern etwa möglich, virtuelle Geldströme nach Belieben umzuleiten, Wirtschaftsgeheimnisse oder militärische Geheimnisse unerkannt auszuspähen und lebenswichtige Versorgungsinfrastrukturen zu zerstören. Bei einer umfassenden Realisierung der Treuhandstrategie müßte man daher mit einem großen Unsicherheitsfaktor leben, der auch zu erheblichen Akzeptanzproblemen führen könnte.

Hinzu käme, daß die in den Treuhandeinrichtungen tätigen Mitarbeiter als bevorzugte Objekte von Bestechungs- und Erpressungsversuchen nicht nur äußert gefährdete, sondern auch äußerst gefährliche Menschen wären. In einer solchen Lage bliebe dem Staat kaum etwas anderes übrig, als Kontrolleure einzusetzen, die das mit der Registrierung, Speicherung, Wartung und Weitergabe der Schlüssel befaßte Personal lückenlos und dauerhaft zu überwachen. Daß auch die Ehepartner, Verwandte, Freunde und Bekannte dieser Mitarbeiter ohne deren Wissen in entsprechende Maßnahmen einbezogen werden, müßte man dabei in Kauf nehmen. Um für die Mehrheit der Bevölkerung ein ausgewogenes Verhältnis zwischen individuellem Freiraum und staatlichem Herrschaftsanspruch und damit gewohnte Standards der demokratischen Gesellschaft aufrechtzuerhalten, erscheint es nach diesem Szenario also unvermeidlich, die liberalen Rechte einer Minderheit zu beschneiden oder sogar weitgehend außer Kraft zu setzen. Vieles spricht daher dafür, daß die Einführung des Treuhandmodells weniger eine völlige Entschärfung als eine Verlagerung der in der digitalisierten Informationsgesellschaft auftretenden Gefahren für das demokratische System bewirken würde.

Fazit: Selbst wenn sich die Treuhandstrategie wider Erwarten gegenüber der zunehmend an Befürwortern gewinnenden liberalen Strategie durchsetzen sollte, könn-

ten die auf diesem Wege zu erzielenden Ergebnisse vor diesem Hintergrund weder unter praktischen noch unter demokratiespezifischen Aspekten in vollem Umfang überzeugen.

Resümee und Ausblick

Abschließend bleibt festzuhalten, daß sich in der Kontroverse um die Nutzung elektronischer Kryptographie in telematischen Netzwerken bis heute keine Strategie abzeichnet, die eine Übertragung der bisher erreichten Ausgewogenheit von liberalem Freiraum und staatlichem Herrschaftsanspruch auf die virtuelle Welt der Netze ermöglicht. Da die Bewahrung dieser Ausgewogenheit eine entscheidende Voraussetzung für die Verteidigung der in der modernen Gesellschaft erreichten demokratischen Standards ist, führt kein Weg an der Erkenntnis vorbei, daß die elektronische Kryptographie zumindest unter den Bedingungen einer digitalisierten Informationsgesellschaft prinzipiell nicht demokratieverträglich ist. Soweit sie nicht mißbraucht wird, um die Netzzugänge Andersdenkender unerkannt mit Datenmüll zu versperren, schützt sie zwar die freie Rede, unter vielen anderen für die Entwicklung des demokratischen Systems relevanten Aspekten verursacht sie aber gravierende Probleme.

Dieser Befund unterstützt die Position derer, die den Potentialen einer virtuellen Demokratie eher mit Skepsis gegenüberstehen. Auch mit Blick auf die durch die elektronische Kryptographie verursachten Probleme erscheint es sinnvoll, bei der Übertragung herkömmlicher politischer Abläufe auf telematische Netzwerke trotz des zunehmenden gesellschaftlichen Bedarfs an neuen politischen Steuerungsformen Vorsicht walten zu lassen. Hier sollte nicht übereilt gehandelt, sondern ein Lernprozeß nach dem Prinzip von Versuch und Irrtum in Gang gesetzt werden. Dieser könnte etwa damit beginnen, daß herkömmliche Verfahren der Informationsbeschaffung und des politischen Diskurses sukzessive durch Anwendungen wie die Präsentation behördlicher Dokumente im Netz und die Einführung virtueller Diskussionsforen ergänzt werden, was mancherorts bekanntlich auch schon geschehen ist. Ein gesellschaftliches Stadium, in dem wesentliche Funktionen der politischen Meinungs- und Willensbildung ganz auf die Netzwerke übertragen worden sind, und in dem man ausgewählte Sachfragen mit Hilfe telematischer Systeme direktdemokratisch entscheidet, sollte dagegen allenfalls am Ende eines solchen Prozesses stehen.

Literatur

Bizer, Johann: Kryptokontroverse. Der Schutz der Vertraulichkeit in der Telekommunikation, in: Datenschutz und Datensicherung 1/1996, S. 5 ff.

Buchstein, Herbert: Bittere Bytes: Cyberbürger und Demokratietheorie, in: Deutsche Zeitschrift für Philosophie. 4/1996, S. 583 ff.

Rihaczek, Karl: Die Kryptokontroverse: das Normungsverbot, in: Datenschutz und Datensicherung 1/1996, S. 15 ff.

Roßnagel, Alexander: Die Infrastruktur einer sicheren und rechtsverbindlichen Telekommunikation, Bonn 1996.

Winkel, Olaf: Netzwerksicherheit als gesellschaftliches und politisches Problem, in: Online 1/1997:S. 62 ff.

Dr. Simone Fischer-Hübner

Die Ausbildung in IT-Sicherheit und Datenschutz

Anforderungen und Studienprogramme

Einleitung

In den letzten Jahrzehnten haben zahlreiche Sicherheitseinbrüche die Unsicherheit heutiger Systeme und die Verletzbarkeit der Informationsgesellschaft gezeigt. Beispiele hierfür liefern Hacker-Angriffe, eine drastisch steigende Anzahl von Computerviren sowie Netzwerkanomalien wie Würmer, Kettenbriefe oder maliziöse Applets. Vor allem das Internet ist für eine Vielzahl an Sicherheitsvorfällen und Sicherheitslücken bekannt. Da Sicherheit ab initio beim Systemdesign berücksichtigt werden muß, können auch die in IP v.6 vorgesehenen Sicherheitsnachbesserungen bestenfalls Sicherheitsrisiken minimieren.

Die direkten Auswirkungen von Sicherheitseinbrüchen können große finanzielle Verluste bis hin zur Bedrohung der Existenz des betroffenen Unternehmens, die Verletzung von Datenschutzrechten oder sogar die Bedrohung von Menschenleben sein. Auf dem Weg in die globale Informationsgesellschaft mit einer zunehmenden Vernetzung nahezu aller Lebensbereiche steigen zugleich die Sicherheitsgefährdungen und Datenschutzrisiken.

Aus diesen Gründen gewinnt das Gebiet der IT-Sicherheit und des Datenschutz zunehmend an Bedeutung. Informatik-Studenten waren in der Regel stets an Datenschutzfragen und sind zunehmend auch an Sicherheitsthemen interessiert. In der Berufspraxis und in der Forschung ist zugleich ein ansteigender Bedarf an IT-Sicherheitsfachleuten zu verzeichnen. Um Sicherungsinfrastrukturen kompetent gestalten und aufbauen zu können, sind Sicherheitsexperten mit einer soliden Ausbildung in den technischen, organisatorischen und rechtlichen Seiten der IT-Sicherheit erforderlich.

Datenschutz sollte schon aus dem Grunde, daß Informatiker für eine gesetzmäßige und sozialverträgliche Systemgestaltung und Systemeinsatz mitverantwortlich sind, ein verbindlicher Bestandteil der Informatik-Ausbildung sein. Durch eine datenschutzgerechte Systemgestaltung lassen sich Datenschutzprobleme von vornherein vermeiden. Dem Prinzip der Vermeidung personenbezogener Daten folgend, lassen sich z.B. IT-Systeme gestalten, welche Anonymität und Pseudonymität für die Benutzer und Betroffenen durchsetzen. Da die Betroffenen meist am Systementwicklungsprozeß unbeteiligt sind, werden ihre Datenschutzinteressen in der Regel vernachlässigt. Informatiker sollten daher die Datenschutzinteressen der Betroffenen vertreten und für eine datenschutzgerechte Systemgestaltung mitverantwortlich sein [Nothdurft 1994, Fischer-Hübner 1996]. Dazu müssen sie mit Verfahren zur Abschätzung von Datenschutzrisiken sowie mit Konzepten zur datenschutzgerechten und sicheren Systemgestaltung vertraut sein.

Anforderungen an die Informatik-Ausbildung

IT-Sicherheit ist nur zum Teil ein technisches Problem und hat zugleich auch bedeutende organisatorische, physikalische, personelle, soziale und rechtliche Seiten. Daher muß IT-Sicherheit auch mit einem ganzheitlichen Sicherheitskonzept durchgesetzt werden. Entsprechend sollte auch die IT-Sicherheitsausbildung holistisch ausgerichtet sein und technische, mathematische, organisatorische, rechtliche sowie soziale Aspekte abdecken.

In der Berufspraxis werden zunehmend Sicherheitsexperten mit Kompetenzen in folgenden Gebieten benötigt:

- **Risikoanalyse und Sicherheitsplanung:**
  Diese Verfahren werden bei jedem größeren Unternehmen eingesetzt. Zudem verlangt auch der Bundesrechnungshof von Bundesbehörden, daß sie vor jeder neuen Systemanschaffung eine Risikoanalyse durchführen.
- **Unfallaufklärung:**
  Aufgrund der Unsicherheit heutiger Systemtechnologien wie PCs oder das Internet werden Experten benötigt, die Sicherheitsangriffe (z.B. Softwareanomalien) und Systemfehler aufdecken und beheben können. Dafür müssen Kenntnisse in den spezifischen Systemimplementationen, Angriffstechniken, Methoden des *Reverse Engineering*, Sicherheitskonzepten vorhanden sein.
- **Entwurf sicherer Systeme:**
  In den Bereichen Forschung und Entwicklung sicherer Systeme sind u. a. Kenntnisse über Sicherheitsmodelle, Konzepte sicherer Betriebsysteme, sichere Datenbanksysteme, Kryptosysteme, Kryptoprotokolle und Schlüsselmanagement erforderlich.
- **Datenschutz:**
  Unternehmen besetzen häufig die Position des betrieblichen Datenschutzbeauftragten mit Informatikern, die nach § 36 II BDSG die zur Erfüllung ihrer Aufgaben erforderliche Fachkompetenz besitzen müssen. Im Rahmen der Umsetzung der EU-Datenschutzrichtlinie soll zudem das Amt eines internen Datenschutzbeauftragten in öffentlichen Stellen eingerichtet werden. Auch in anderen EU-Mitgliedsländern wird zur Zeit die Umset-

zung des Konzeptes der „*Data Protection Officials*" nach Art. 18. EU-Datenschutzrichtlinie diskutiert.

Aufgrund der Vielfältigkeit der Anforderungen, ist zur Ausbildung von Sicherheitsexperten ein mehrere Kurse umfassendes IT-Sicherheitscurriculum erforderlich. Weiterhin ist es wünschenswert, daß im Informatikstudium neben des Angebotes eines IT-Sicherheitscurriculums auch in anderen Fachvorlesungen (über Betriebssysteme, Netzwerksysteme, Datenbanksysteme, Softwareengineering, Informatik-Anwendungen) relevante Sicherheitsaspekte behandelt und somit Querbezüge aufgezeigt werden.

Die IT-Sicherheitsausbildung an europäischen Hochschulen

Im folgenden soll ein kurzer Überblick zu den wichtigsten an europäischen Hochschulen angebotenen Kurse in IT-Sicherheit (siehe auch [Yngström 1995, Erasmus 1995a]) und Datenschutz gegeben werden. Die an den einzelnen Universitäten angebotenen Ausbildungen in IT-Sicherheit und Datenschutz lassen sich als Programme (Curricula), welche mehrere aufeinander abgestimmte Veranstaltungen umfassen, oder als einzeln angebotene Veranstaltungen klassifizieren.

IT-Sicherheitsprogramme werden u. a. an der Universität Hamburg, der Universität Stockholm sowie an den englischen Universitäten in London (Royal Holloway College), Leicester, York und an der London School of Economics angeboten.

Universität Hamburg:

Seit 1988 wird am Fachbereich Informatik der Universität Hamburg ein IT-Sicherheitscurriculum (Curriculum in IT-Security and Safety) unter der Leitung von Prof. Klaus Brunnstein veranstaltet, mit welchem sich Studenten im Hauptstudium im Gebiet „IT-Sicherheit und Datenschutz" vertiefen können.

Das Curriculum, das einen interdisziplinären Ansatz verfolgt und sowohl technische und mathematische, als auch organisatorische und rechtliche Aspekte abdeckt, besteht aus vier zweistündigen Vorlesungen InfoSec I-IV, welche die folgenden Themen behandeln:

1. InfoSec I (Einführung in die IT-Sicherheit): Behandlung von IT-Mißbrauchstechniken, Fallstudien, Einführung in IT-Sicherheitstechniken, rechtliche Aspekte (Datenschutz, Computerkriminalität, Urheberrecht).
2. InfoSec II (Konzepte sicherer Systeme I): IT-Sicherheitskriterien, Sicherheitsmodelle, Konzepte sicherer Betriebssysteme,
3. InfoSec III (Konzepte sicherer Systeme II): Datenbanksicherheit, Kryptographie, Netzwerksicherheit.
4. InfoSec IV (Risiko- und Unfallanalyse): Analyse von IT-Unfällen, sicherheitskritische IT-Systeme, Risikoanalyse, Sicherheitsplanung.

Ergänzt wird dieser 4-semestrige Vorlesungszyklus durch das vierstündige Projektseminar „Aktuelle Probleme der IT- und Netzsicherheit", in welchem aktuelle Vorfälle diskutiert werden und die Methodologie und Praxis des *Reverse Engineering*, Verfahren zum Testen von IT-Sicherheitsprodukten sowie die Erstellung von Sicherheitsprodukten praktisch gelehrt werden.

Ergänzend werden weiterhin vertiefende Seminare und Vorlesungen zu Themengebiete wie Kryptologie, Chipkarten, Sicherheitsmodelle, Datenschutz angeboten.

Universität Stockholm:

An der Universität Stockholm und an der KTH (Royal Institute of Technologie) werden die drei folgenden interdisziplinär ausgerichteten Programme angeboten:

1. Sicherheitsinformatik (*Security Informatics* – SI): Bachelor-Studienprogramm, seit 1985, richtet sich an Informatikstudenten im dritten Studienjahr oder an Berufspraktiker mit genügend akademischen Hintergrundwissen, erfordert den Aufwand eines vollen akademischen Jahres, 6 Kurse und eine schriftliche Abschlußarbeit.
2. Sicherheit von Informationen in IT-Umgebungen (*Information Security in IT Environments* – ISITE): Master-Studienprogramm, seit 1993, erfordert ebenfalls den Aufwand eines vollen akademischen Jahres mit dem Besuch von 6 Kursen und einer schriftlichen Abschlußarbeit.
3. Rechnersicherheit (*Computer Security* – CS): Master-Studienprogramm, seit 1994, richtet sich an Ingenieurstudenten, erfordert den Aufwand eines 3/4 Studienjahres, drei Kurse und eine schriftliche Abschlußarbeit.

Folgende Kurse, die jeweils aus acht dreistündigen Vorlesungen bestehen, werden für die verschiedenen Programme (jeweils in Klammern angegeben) angeboten: Sicherheit I –Generelle Systemtheorie (SI), Sicherheit II – Grundsätze sicherer Systeme (SI), Sicherheit III – Organisatorische, Management-, soziale und ethische Aspekte (SI, ISITE), Netzwerk- und Kommunikationssicherheit (SI,CS), Sicherheit in Software (SI), Testverfahren, Zuverlässigkeit, Fehlertoleranz (SI, ISITE), Globale Wirkungen der IT-Sicherheit (ISITE), Betriebsystem-Sicherheit (ISITE), Sicherheit in standardisierten Netzen und Anwendungen (ISITE, CS), Sicherheitsarchitekturen für offene verteilte Systeme (ISITE,CS), Entwicklung und Gebrauch von sicheren Anwendungen, Sicherheitsmanagement (ISITE), Evaluation von IT-Sicherheitsprodukten und -systemen (ISITE).

Master-Studienprogramme an englischen Universitäten:

Seit Anfang/Mitte der neunziger Jahre werden auch an verschiedenen englischen Universitäten Master-Sudienprogramme zu IT-Sicherheit angeboten. Die British Computer Society hat 1994 zusammen mit der Confederation of British Industry und dem National Computer Users Forum Richtlinien zur IT-Sicherheitsausbildung (IT-Security Training Guidelines) entworfen, die eine umfassende Liste von IT-Sicherheitsthemen enthält, welche Ausbilder und Stu-

denten über die für eine professionelle Sicherheitsausbildung erforderlichen Kursinhalte informieren soll.

An der **London School of Economics** wird seit 1994 ein einjähriges Master-Programm mit dem Abschluß *„MSc (Master of Sciences) in Information Systems Security"* angeboten. Es handelt sich herbei um ein multidisziplinäres Programm, das sowohl informatische, organisatorische, rechtliche als auch ethische Aspekte behandelt und einen sozio-technischen Ansatz von einer Sicherheit von Informationssystemen lehrt.

Ein einjähriges Master-Programm *„MSc in Security Management and Information Technology"* wird an der **Universität Leicester** angeboten. Der Schwerpunkt dieser Ausbildung liegt auf Risiko- und Sicherheitsmanagement sowie der Bekämpfung von Computerkriminalität. Es werden vor allem rechtliche und organisatorische Aspekte behandelt.

Das **Royal Holloway College** der **Universität London** bietet zwei verschiedene einjährige Master-Programme an: Seit 1992 wird ein interdisziplinäres Programm mit dem Abschluß *„MSc in Information Security"* angeboten, das sowohl technische als auch organisatorische Aspekte abdeckt. Für diesen Ausbildungsgang müssen u. a. Kurse in Sicherheitsmanagement, Kryptographie, Netzwerksicherheit, Betriebssystemsicherheit absolviert werden. Zudem wird seit 1994 ein Programm *„MSc in Dependable Computer Systems"* gelehrt, welches mathematische, technische und organisatorische Aspekte behandelt. Zu diesem Programm gehören u. a. obligatorisch Kurse in Sicherheitsmanagement, Einführung in Rechnersicherheit, formale Methoden, sicherheitskritische Systeme, Sicherheitsstandards und -kriterien.

An der **Universität York** können Studenten seit 1995 an einem Programm mit dem Abschluß *„MSc in Safety Critical Systems Engineering"* teilnehmen. Dabei handelt es sich um eine eineinhalb bis dreijährige Ausbildung, die sich an zukünftige Entwickler sicherheitskritischer Systeme richten soll.

Neben diesen, bisher nur an wenigen Universitäten angebotenen IT-Sicherheitscurricula, werden an weiteren europäischen Universitäten regelmäßig einzelne Einführungs- und Vertiefungsveranstaltungen zu IT-Sicherheitsthemen angeboten, wobei die meisten davon zumindest Kryptographie und Betriebssystemsicherheit behandeln. In Deutschland werden u. a. an den Universitäten in Dresden, Frankfurt, München, Hildesheim, Siegen, Essen, Mainz, Freiburg und Karlsruhe IT-Sicherheitskurse mit verschiedenen Schwerpunkten veranstaltet. Weiterhin wird im europäischen Ausland z.B. an der an der Copenhagen Business School, Universität Oulu, Universität Lund, Universität Linköping, Chalmers Technische Universität, Universität Plymouth, Katholischen Universität Leuven, Universität Wien, Technischen Universität Graz sowie der Universität Zürich IT-Sicherheit in speziellen Kursen gelehrt.

Während IT-Sicherheit an vielen Universitäten in den letzten Jahren Einzug in die Ausbildung erhalten hat, wird speziell Datenschutz nur an wenigen Hochschulen angemessen berücksichtigt. So ist in Deutschland das Thema Datenschutz nur an wenigen Universitäten, wie an der TU Berlin, Universität Bremen und an der Universität Hamburg, obligatorischer Bestandteil der Informatik-Ausbildung. An einigen Universitäten, wie z.B. der TH Darmstadt, wird Datenschutz für Informatikstudenten mit Nebenfach Rechtswissenschaften gelehrt. An der Fachhochschule Ulm am Fachbereich Technische Informatik wird seit 1987 ein zweisemestriges Zusatzstudium im Bereich Datenschutz und Datensicherheit angeboten, mit welchem sich Informatikstudenten zu fachkundigen Datenschutzbeauftragten gem. § 36 II BDSG weiterbilden können. Auch an der Fachhochschule München wird im Fachbereich Informatik/Mathematik seit dem Wintersemester 1994/95 „Betrieblicher Datenschutz" als Zusatzausbildung im Umfang von 16 SWS angeboten.

Schlußbemerkungen

Zusammenfassend läßt sich sagen, daß in der Praxis ein zunehmender Bedarf an qualifizierten Sicherheits- und Datenschutzexperten zu verzeichnen ist, welche aufgrund vielfältiger Anforderungen nach einem umfassenden IT-Sicherheitscurriculum ausgebildet werden müssen. Zur Zeit werden nur an wenigen europäischen Universitäten entsprechende IT-Sicherheitsprogramme angeboten.

Im Rahmen der Erasmus/Socrates-Programmes *„IT-Security & Safety Education"*, an welchem 21 europäische Universitäten aus insgesamt 11 EU-Ländern beteiligt sind, ist ein Mustercurriculum in *„Information Security, Dependability and Safety"* für *Postgraduate*-Studenten entwickelt worden [Erasmus 1995b], welches akademischen Institutionen Vorschläge für eineinhalbjährige Masterstudiengänge bieten soll. Dieses Curriculum soll zunächst beispielhaft an der Universität Athen umgesetzt werden. Weiterhin ist geplant ausgewählte Kurse des vorgeschlagenen Programms in dreiwöchigen Sommerschulen (*Summer Schools*) in Europa anzubieten.

Weiterhin ist zur Zeit auch die IFIP (*International Federation for Information Processing*), Arbeitsgruppe WG 11.8 (*„IT Security Education"*) damit beschäftigt, Vorschläge für IT-Sicherheitsprogramme und praktische Sicherheitskurse zu diskutieren und zu erarbeiten.

Literatur:

[Erasmus 1995a] „University Programmes on Information Security, Dependability and Safety", Hrsg: D. Gritzalis, European Commission, Erasmus ICP-94(&95)-G-4016/11, Report IS-CD-3c, Athen, Juli 1995

[Erasmus 1995b] „A Proposal for a Postgraduate Programme on Information Security, Dependability an Safety", Hrsg.: S.Katsikas, D.Gritzalis, European Commission, Erasmus ICP-94(&95)-G-4016/11, Report IS-CD-4a, Athen, September 1995.

[Fischer-Hübner 1996] Simone Fischer-Hübner, „Teaching Privacy as a Part of the Computer Science Curriculum", in: Proceedings of the IFIP TC-3/TC-9 Conference „The Impact of IT – From Practice to Curriculum", Chapman & Hall, Hrsg.: Y.Katz et al., Israel, März 1996.

[Nothdurft 1994] Kai Nothdurft, „Datenschutzrechtliche Anforderungen an die Systemgestaltung und die deutsche universitäre Ausbildung", Diplomarbeit, Studiengang Informatik, Universität Bremen, 1994.

[Yngström 1995] Louise Yngström, „Education in IT-Security in Europe", IFIP WG 11.8 Workshop „Current and Future Needs, Problems and Prospects", Kapstadt, Mai 1995.

Lesen Neues für den Bücherwurm – kurz belichtet

Tobias Pflüger

Die neue Bundeswehr. Mit neuer Strategie, Struktur und Bewaffnung in den Krieg.

Die hochaktuelle Studie hat sich zum Ziel gesetzt, Informationen über die „neue Bundeswehr" zu liefern, die in den letzten Jahren systematisch in eine Interventionsarmee umgebaut wird. Pflüger beschreibt diese Entwicklung als einen Dreischritt: Zunächst die Änderung der Strategie, eingeleitet mit den „verteidigungspolitischen Richtlinien" vom November 1992. Es folgte die Anpassung der Struktur der Bundeswehr (hin zu einer international einsetzbaren Eingreiftruppe, Stichwort „Krisenreaktionskräfte") – ab Mai 1993 war die Bundeswehr in Somalia, im April 1994 folgte die Verfassungsgerichtsentscheidung zur deutschen Beteiligung an friedenssichernden Operationen der Vereinten Nationen. Als dritten Schritt nennt Pflüger die sich an den aktuellen Beschaffungsvorhaben der Bundeswehr zeigende Neubewaffnung. Der Weg von den „verteidigungspolitischen Richtlinien" über die zur „Akzeptanzbeschaffung" (S. 104) notwendigen humanitären Einsätze bis zum ersten Kampfeinsatz der Bundeswehr Juli 1995 in Bosnien verlief unglaublich glatt und schnell und wäre kaum möglich gewesen ohne die spätestens seit dem Golfkrieg feststellbare schleichende Militarisierung der Gesellschaft. Und so enthält das Buch folgerichtig auch die Warnung vor einer „Militarisierungsspirale", angetrieben auch von der deutschen Rüstungsindustrie und vom Wunsch, Deutschland stärkeren Einfluß auf den außen- und sicherheitspolitschen Bereich der EU zu verschaffen (NB: man denke auch an die Diskussion, Deutschland einen ständigen Sitz im Weltsicherheitsrat zu verschaffen). Das Buch endet mit Überlegungen zum weiteren Vorgehen gegen die Militarisierungswelle, wobei Pflüger vor allem den notwendigen Widerstand gegen die neuen Beschaffungs- und Ausrüstungsprojekte der Bundeswehr hervorhebt. Wenn es gelingt, solche „Eisbergspitzen" zu kappen, so Pflüger, würden damit auch wichtige Symbole der Militarisierung kippen. Insofern plädiert er auch für Widerstand gegen die einschlägigen Aktivitäten der großen Rüstungskonzerne.

Der Autor – Fachreferent und Vorstandsmitglied der *Infomationsstelle Militarisierung* (IMI) e.V. in Tübingen – hat mit diesem Buch eine gleichermaßen informative als auch interessant zu lesende Bestandsaufnahme vorgelegt. Der große Bogen, den die Studie schlägt, wird durch konkrete Einzelkapitel z.B. über Daimler-Benz/DASA als Hauptausrüster der neuen Krisenreaktionskräfte oder über das „Kommando Spezialkräfte" in Calw als Elitetruppe für den Kriegseinsatz untermauert und illustriert. Nicht zuletzt machen die eingeschobenen Tabellen und Aufzählungen in Verbindung mit dem umfassenden aktuellen Zahlenmaterial das handliche Buch für alle zu einem Muß, die sich in Politik, Bürgerbewegung oder Wissenschaft mit Fragen von Krieg, Frieden, Rüstung und Militarisierung auseinandersetzen.

(Ralf E. Streibl)

Claudia Jenkes:

Friedensbewegung und Medien

Das Buch der Diplomjournalistin Claudia Jenkes ist bewußt keine kommunikationswissenschaftliche Analyse aus der Distanz. Ihr eigenes politisches Engagement führte die Autorin zu der Fragestellung nach der „Schnittstelle zwischen den Medien und sozialem Engagement" (S.9). Aufbauend auf theoretischen Überlegungen und auf der Basis von Gesprächen mit Aktiven der Friedensbewegung soll die Studie „die komplexen Auswirkungen der Massenmedien auf politisches Engagement beleuchten und zum Teil auch bewerten" (S. 10). Das Buch gliedert sich in mehrere Teile: Im ersten Kapitel faßt die Autorin knapp die Geschichte der Friedensbewegung vom NATO-Doppelbeschluß bis heute zusammen und zieht eine trotz aller Rückschläge insgesamt positive Bilanz der Wirkungen: „Sie hat Spuren in der Gesellschaft hinterlassen, die nur schwer zu verwischen sind" (S. 21). Die nächsten Kapitel sind der Medienkritik gewidmet, insbesondere den funktionalisierbaren Strukturen der Medienbetriebe, die von gewieften PR-Strategen genutzt werden, um für ihre Ziele „Öffentlichkeit zu machen". Jenkes beschreibt dabei zunächst die zunehmende symbolische Inszenierung von politischen Inhalten und kritisiert die „Scheinhandlungen einer Placebo-Politik" (S. 26), auf die am Ende die Politiker selbst wieder reinfallen. Anschließend nimmt sie sich gezielt das „Wirtschaftsunternehmen Massenmedium" vor, und zeigt an einigen Beispielen die bestehenden Selektionsmechanismen für Nachrichten auf. Doch nicht nur gegen das abstrakte Medium richtet sich ihre Kritik, sondern auch gegen die Arbeitsweise derjenigen Medienschaffenden, deren Journalismus sich an der industriellen Produktionsweise orientiere und die vor allem erwartungskonforme Inhalte und gängige Stereotype transportieren.

An die genannten Vorüberlegungen angeschlossen ist der Bericht über eine Untersuchung der Autorin, in deren Mittelpunkt Leitfaden-Interviews mit AktivistInnen der Friedensbewegung aus dem Umfeld des Ruhrgebietes stehen. Die Inhalte dieser Gespräche sind in dem Buch in reportageartigen Zusammenfassungen wiedergegeben. Ziel der Autorin ist es – erklärtermaßen ohne Anspruch auf Repräsentativität – beispielhaft zu zeigen, welche Rolle Massenmedien im Zusammenhang mit dem friedenspolitischen Engagement dieser Menschen subjektiv spielen. In der abschließenden Bewertung ihrer Ergebnisse arbeitet Jenkes heraus, wie wichtig erfolgreiche Pressearbeit für viele politische Initiativen ist – aus erfolgreichem Medienecho kann auch neue Motivation

geschöpft werden –, gleichzeitig verweist sie aber auch auf die bestehenden Gefahren einer zu starken Medienorientierung: Dies könne zum einen dazu führen, daß durch die Anpassung an die Strukturen des Medienbetriebes deren Selektionsmechanismen zunehmend die eigene politische Arbeit beeinflussen, zum anderen das medienvermittelte Bild der Friedensbewegung die Wahrnehmung der AktivistInnen stärker prägt als die tatsächlichen Gegebenheiten. Jenkes bezieht sich hier v.a. auf die mühsame, aber dennoch wichtige „Kleinarbeit" (S. 92) von Aktiven der Friedensbewegung (z.B. in Ex-Jugoslawien), über die nur selten in den Medien berichtet wird. Kurz wird in dem Buch auch die Verunsicherung durch die mangelnde Glaubwürdigkeit der Medien (Bsp. Golfkrieg) angerissen und die Entmutigung vieler Aktiver durch die Kriegsbilder aus Bosnien thematisiert. Jenkes Buch ist lesenswert sowohl für diejenigen, die selbst aktiv Friedensarbeit machen, als auch für diejenigen, die sich wissenschaftlich für derartige soziale Bewegungen interessieren. Nicht zuletzt sollten sich auch viele Medienschaffende dieses Buch zu Gemüte führen – zwar ist die in dem Buch enthaltene Medienkritik nicht neu, aber anhand des Beispiels Friedensbewegung gut nachvollziehbar dargestellt.

(Ralf E. Streibl)

Peter Imbusch & Ralf Zoll (Hrsg.):

Friedens- und Konfliktforschung. Eine Einführung mit Quellen.

Endlich ein umfangreiches Handbuch zu dem Thema! – So war mein erster Eindruck, als ich das Buch, den ersten Band einer neuen Reihe zu Friedens- und Konfliktforschung, in Händen hielt. Das über 500 Seiten umfassende Werk beinhaltet 13 Beiträge und darüber hinaus 29 sogenannte „Quellentexte" – so bezeichnen die Herausgeber Textausschnitte und teilweise überarbeitete und gekürzte Artikel verschiedener AutorInnen aus Wissenschaft, Politik und Gesellschaft (u.a. Ulrike C. Wasmuth, Ulrich Beck, Boutros Boutros Ghali, Thomas Dominikowski, Hans Lenk, Wolfgang Schäuble, Dieter Senghaas), die zur Unterstützung und Vertiefung der einzelnen Kapitel dienen sollen. Beide Herausgeber arbeiten am Institut für Soziologie der Universität Marburg, an welcher – erfreulich in Zeiten, in denen Friedensforschung nicht unbedingt en vogue ist – ein zunächst sozialwissenschaftlich orientierter Nebenfachstudiengang „Friedens- und Konfliktforschung" entwickelt wurde.

Dem Band zugrunde liegt ein konflikttheoretischer Ansatz, der Konflikte als „ubiquitäre soziale Erscheinungen" ansieht, die zunächst weder gut noch schlecht sind. Im ersten Teil werden nach einem Überblick über die Geschichte der Friedens und Konfliktforschung (Karlheinz Koppe) zentrale Begriffe der Friedens- und Konfliktforschung erläutert. Thorsten Bonacker und Peter Imbusch erläutern auf anspruchsvolle, aber dennoch verständliche Weise verschiedene Definitionsansätze zu „Konflikt", „Gewalt", „Krieg" und „Frieden". Ein zu Recht umfangreiches Kapitel (Peter Imbusch) ist „Konflikttheorien" gewidmet. Der erste – „Grundlagen" überschriebene – Teil des Buches endet mit einem Kapitel über „Friedens- und Konfliktforschung als Studiengang" (Ralf Zoll). Darin wird – neben einer Schilderung der Schwierigkeit, das Fach in Gegenstand, Theorien und Methoden zu beschreiben – die Konzeption des Marburger Studiengangs vorgestellt. Zur Ergänzung und Illustration dieses Beitrages wäre es schön gewesen, wenn an dieser Stelle auch erste Erfahrungen berichtet worden wären.

Der zweite Teil des Sammelbandes trägt die Überschrift „Konfliktanalysen". Darin finden sich – stellvertretend für verschiedene Bereiche und Ebenen – Beiträge zum Konflikt in Ex-Jugoslawien, zur deutschen Vereinigung (Peter Imbusch), zur Rahmenrichtlinie Gesellschaftslehre in Hessen, zum Thema Automobil und Umwelt, zum „Radikalenerlaß" (Ralf Zoll) und zum Abtreibungsurteil des Bundesverfassungsgerichtes (Monika Gerstendörfer). Beschlossen wird der Band mit drei Beiträgen zu Friedensethik (Michael Haspel), Friedenserziehung (Hans Nicklas) und zur Konfliktregelung auf gesellschaftlicher Ebene im Angesicht der aktuellen Bürgerkriege (Berthold Meyer).

Fazit: Der erste Eindruck trog nicht: der Sammelband ist für verschiedene Bereiche gut nutzbar und gibt einen – im Rahmen der Möglichkeiten solch eines Werkes – guten ersten Überblick über das breite Gebiet der Friedens- und Konfliktforschung aus sozialwissenschaftlicher Perspektive. Ein Bereich, der sicherlich zu kurz kam, ist die Frage des produktiven Umgangs mit Konflikten. Hier verspricht jedoch der angekündigte dritte Band der gleichen Reihe Abhilfe, „Formen der Konfliktregelung" von Berthold Meyer (Leske+Budrich 1997). Ausgesprochen ärgerlich ist allerdings das Fehlen eines Namens- und eines Sachwortregisters – gerade bei der Zielsetzung solch eines Bandes sollte man diesen Aufwand keinesfalls scheuen.

(Ralf E. Streibl)

WSI-Mitteilungen Heft 3/1997

Informationsgesellschaft – Schlagwort oder gesellschaftlicher Umbruch?

Der Begriff „Informationsgesellschaft" stand zunächst für eine industriepolitische Leitidee zur Schaffung einer einheitlichen Informations-Infrastruktur. Erst allmählich wird – nicht zuletzt durch die Initiative von Gewerkschaften und anderen gesellschaftlichen Gruppen – nach dem sozialen Nutzen von Marktöffnung und neoliberalem Wirtschaftsprimat und nach den Vorstellungen von Demokratie und Gesellschaft in einer Informationsgesellschaft gefragt.

Das Schwerpunktheft 3/1997 zur Informationsgesellschaft versteht sich als ein Teil einer Debatte über die künftige Gesellschaftsgestaltung. Inzwischen mehren sich die Stimmen, die die einseitige technische und ökonomische Ausrichtung an der Diskussion um die Informationsgesellschaft kritisieren und eine andere Orientierung fordern: statt Marktautonomie ist aktive Struktur- und Beschäftigungspolitik erforderlich, statt wirtschaftlicher müssen auch soziale und ökologische Kriterien eine Rolle

spielen; die Technikdominanz in der Forschungspolitik muss durch politische Technikgestaltung ersetzt werden, gegen Deregulierung und Auflösung herkömmlicher Arbeits- und Betriebsformen müssen gewerkschaftliche Reformvorstellungen eingebracht werden. Das Heft enthält Beiträge von Roland Schneider, Gerhard Bosch, Grudrun Trautwein-Kalms, Michael Schwemmle, Sabine Helmers, Rainer Rilling, Peter Wedde u.v.a.

(Ute Bernhardt)

Wissenschaften, Technik und Ethik.

Forschung und Lehre an Hochschulen in der Bundesrepublik Deutschland mit Einzelbeispielen aus anderen europäischen Ländern.

Herausgegeben von Wolfgang Bender und Linda Hartenberger im Auftrag des International Network of Engineers and Scientists for Global Responsibility (INES) gefördert von der Berghof-Stiftung für Friedens- und Konfliktforschung.

Diese Broschüre versteht sich als Beitrag zur Förderung interdisziplinärer Forschungs- und Lehrprojekte speziell im Grenzbereich zwischen Natur- und Ingenieurwissenschaften einerseits und Ethik andererseits. Sie dokumentiert die Entwicklung der Forschungsrichtung „Ethik in den Wissenschaften" und gibt einen ausgewählten Überblick über Inhalte von Forschungsprojekten und Lehrveranstaltungen. Aus dem erheblichen Missverhältnis zwischen anerkannter Notwendigkeit interdisziplinärer Forschung und Lehre und den ungesicherten institutionellen und finanziellen Rahmenbedingungen ergeben sich für die AutorInnen weitergehende Folgerungen und Forderungen hinsichtlich einer festen Verankerung und Stärkung dieses Bereichs.

(Ute Bernhardt)

Industriegewerkschaft Metall – Vorstand

Software. Eine Technologie verändert die Welt

Diese Broschüre ist für die gewerkschaftliche Arbeit gedacht. Sie erklärt, was Software ist, was mit ihr gemacht wird und in welchen Technologien Software zum Einsatz kommt. Darüberhinaus werden die Folgen der Software kurz beschrieben, etwa bei Gestaltung und Organisation von Arbeit bis hin zu neuen Managementkonzepten. Die Broschüre gibt eine kleine Einführung in die Software-Ergonomie und listet einige Gestaltungsregeln für den Bildschirmarbeitsplatz auf.

(Ute Bernhardt)

Bibliographie zu „Elektronischer Demokratie"

Mittlerweile liegen eine ganze Reihe von Texten zur „Elektronischen Demokratie" vor, die von Rainer Rilling unter http://staff-www.uni-marburg.de/~rillingr/net/netmat/netdem.htm zusammengestellt worden sind.

(Ute Bernhardt)

Einkaufsliste:

- **Die neue Bundeswehr.** Mit neuer Strategie, Struktur und Bewaffnung in den Krieg. Köln: ISP, 1997. ISBN 3-929008-63-7, DM 14.80
- **Friedensbewegung und Medien.** Schriftenreihe „Probleme des Friedens", hrsg. von Pax Christi – Deutsches Sekretariat. Idstein: Komzi-Verlag, 1997. ISBN 3-929522-38-1, DM 19.80
- **Friedens- und Konfliktforschung.** Eine Einführung mit Quellen. Opladen: Leske+Budrich, 1996. ISBN 3-8100-1650-0, DM 36.00
- **Informationsgesellschaft – Schlagwort oder gesellschaftlicher Umbruch?** Zu bestellen bei: Wirtschafts- und Sozialwissenschaftliche Institut (WSI) in der Hans-Boeckler-Stiftung, Bertha-von-Suttner-Platz 3, 40227 Düsseldorf, Tel. 0211/7778-0, http://www.boeckler.de
- **Wissenschaften, Technik und Ethik.** Bezug: INES, Gutenbergstr. 21, 44139 Dortmund, email: R.BRAUN@LILLY.PING.DE
- **Software. Eine Technologie verändert die Welt.** Bezug: Union-Druckerei, Theodor-Heuss-Allee 90-98, 60486 Frankfurt, Bestell-Nr. 1237, ISBN: 3-922 454-41-0

Tagungen

VIS '97

Verläßliche IT-Systeme, Zwischen Key Escrow und elektronischem Geld
29. September 1997- 2. Oktober 1997
Freiburg i. Breisgau
Weitere Informationen: http://www.iig.uni-freiburg.de/gi/vis97

Compsec '97

The 14th World Conference on Computer Security. Audit and Control
5. November 1997 - 7. November 1997
London
Weitere Informationen: a.richardson@elsevier.co.uk

SIS '98

3. Fachtagung Sicherheit in Informationssystemen
26. und 27. März 1998
Stuttgart
Weitere Informationen: http://www.ifi.unzh.ch/events/SIS98

SEC '98

14th International Information Security Conference
31. August 1998 - 4. September 1998
Wien – Budapest
Weitere Informationen: http://www.ocg.at/sec.html
Weitere Informationen: http://www.njszt.iif.hu/sec.html

FIfF e.V. FIfF Überall

FIFF–Vorstand

- **Prof. Dr. Reinhard Keil-Slawik (Vorsitzender)**
  U-GH Paderborn,
  Fürstenallee 11
  33102 Paderborn
- **Ute Bernhardt (stellv. Vorsitzende)**
  Paulstraße 15,
  53111 Bonn
- **Peter Bittner**
  Hochstraße 56,
  64285 Darmstadt
- **Johannes Busse**
  Derendingerstraße 106,
  72072 Tübingen
- **Prof. Friedrich-Lothar Holl**
  Hektorstraße 7,
  10711 Berlin
- **Prof. Dr. Hans-Jörg Kreowski**
  Uni Bremen,
  FB 3,
  Postfach 33 04 40,
  28334 Bremen
- **Werner Moritz**
  Uhlandstraße 17,
  27576 Bremerhaven
- **Ingo Ruhmann**
  Paulstraße 15,
  53111 Bonn
- **Jürgen Ditz Schroer**
  Graf-Schenck-Straße 4a,
  82299 Türkenfeld
- **Dr. Cornelia Teller**
  Kittlerstraße 27,

Beirat

Prof. Dr. Wolfgang Coy (Berlin); **Prof. Dr. Leonie Dreschler-Fischer** (Hamburg); **Prof. Dr. Christiane Floyd** (Hamburg); **Prof. Dr. Klaus Fuchs-Kittowski** (Berlin); **Prof. Dr. Thomas Herrmann** (Dortmund); **Prof. Dr. Wolfgang Hesse** (Marburg); **Prof. Dr. Michael Grütz** (Konstanz); **Dr. Rolf Günther** (München); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Hans-Peter Löhr** (Berlin); **Dipl.-Ing. Werner Mühlmann** (Oppung); **Prof. Dr. Frieder Nake** (Bremen); **Prof. Dr. Rolf Oberliesen** (Hamburg); **Dr. Hermann Rampacher** (Bonn); **Prof. Dr. Arno Rolf** (Hamburg); **Prof. Dr. Alexander Roßnagel** (Kassel); **Prof. Dr. Gerhard Sagerer** (Bielefeld); **Dr. Gabriele Schade** (Ilmenau); **Prof. Dr. Britta Schinzel** (Freiburg); **Prof. Dr. Dirk Siefkes** (Berlin); **Dr. Marie-Theres Tinnefeld** (München); **Prof. Dr. Josef Weizenbaum** (Freiburg/Cambridge, Mass.); **Dr. Gerhard Wohland** (Wankheim)

Regionalgruppe München

Arbeit und Leben, Wintersemester 1997/98, Kursnummer BG 140 E

„Kleine Zwischenbilanz zur Informationsgesellschaft"

Seit nunmehr über zwei Jahren überrollen das Internet und die neuen Medien die alten. Viele Erwartungen sind in dieser Zeit entstanden, wie weit sie sich – im Guten wie im Schlechten – erfüllt haben, ist eine Frage, die wir in den Veranstaltungen dieses Semesters diskutieren wollen. Wir wollen die Kunst und die Arbeit, die Politik und die Wissenschaft betrachten. Dazu haben wir wieder sachkundige Referentinnen und Referenten aus diesen Bereichen eingeladen.

Die Veranstaltungen (bis auf den Wochenend-Workshop) finden statt im Kulturzentrum Gasteig am Rosenheimer Platz (S-Bahn-Anschluß), Anfangszeit: 2000 Uhr. Den Raum erfragen Sie bitte beim VHS Infostand im 1. Stock unter der Kursnummer BG 140 E. Leider ist der Kurs nicht mehr kostenlos, für das Semester kosten die Veranstaltungen 20,- DM, Restkarten 6,- DM am Abend. (Man kann sich übrigens auch telefonisch bei der VHS einschreiben, Telefon 4 80 06-0).

9.10.97 – Kunst im Internet – gibt's das?

Dr. Barbara Becker (angefragt)

Die Kunstszene im Internet füllt nicht die Schlagzeilen. In Zeitungen und Magazinen tauchen bestenfalls spektakuläre Fischzüge des Microsoft-Chefs Bill Gates auf, wenn dieser die Rechte an der elektronischen Wiedergabe von ganzen Gemäldesammlungen erworben hat. – Was treiben die Künstlerinnen und Künstler in den Netzen, welche Formen von Kunst gibt es, und wie erleben wir sie?

Dr. Barbara Becker von der GMD stellt einige interessante Beispiele vor und kommentiert sie.

Termine

11.10.97

Darmstadt, Vorstands- und Beiratssitzung. Infos zu den Terminen bei der FIfF-Geschäftsstelle

14.-16.11.97

Paderborn, Jahrestagung des FIfF (siehe Seite 5)

26.-28.11.97

„Dann hilft mir nur das Internet", unter diesem Titel veranstaltet das Bildungszentrum Heinrich Pesch Haus Ludwigshafen ein Werkstattseminar für Vertreter von Menschenrechtsorganisationen, Journalisten und Referenten der politischen Bildung. Es geht um die Frage, welche Chancen das Internet im Kampf für Menschenrechte und Demokratie bietet. Info und Anmeldung:
Heinrich Pesch Haus, Fax 0621/51 72 25.

10.-12.10.97

Herbsttagung des /CL in Nürnberg

Weltweite Vernetzung: Refarate, Fachvorträge, Präsentationen und Informationen zur Vernetzung mit der 3. und 4. Welt.

Das /CL-Netz: Workshops zu aktuellen Diskussionen und Initiativen in der politischen und Umweltvernetzung.

Infos und Anmeldung unter:
089/1675106 und bei
cl-service@link-m.de

13.11.97 – Die Parteienkonzepte für die Informationsgesellschaft

(N.N.)

Wie reagieren die Parteien auf die Herausforderungen der Informationsgesellschaft? Wir wüßten gern, welche Konzepte wir bei welcher Partei wählen und diskutieren mit Parteienvertreter(-innen) von Bündnis90/Die Grünen, CSU und SPD.

14. -16.11.97 – Frauen im Netz

Wochenend-Workshop am Starnberger See mit der VHS nur für Frauen

Was bietet uns Frauen das Internet, was erhoffen wir uns, was lehnen wir ab? Auf der Basis von Szenarien wollen wir Visionen entwickeln, aus denen wir Gestaltungsforderungen und -ansätze ableiten. (Internet-Erfahrung ist erwünscht, aber nicht Bedingung.)

11.12.97 – Arbeiten mit der Informations- und Kommunikationstechnik, so gesund wie nie?

Ditz Schroer

Die europäische Richtlinie zur Bildschirmarbeit ist jetzt auch deutsches Gesetz, und wir wüßten gern, ob die Arbeitnehmerinnen und Arbeitnehmer davon etwas gemerkt haben.

8.1.98 – Kann verbesserte Kommunikation Verkehr vermeiden?

Ulrike Brüggemann

Das Institut für Klima, Umwelt, Energie in Wuppertal bearbeitet z.Zt ein Forschungs-Projekt zum Verkehr: eine moderne/ökologische vs. traditionelle Verkehrsplanung. Die Fragestellung ist dabei: Wie funktioniert Verkehrsplanung bisher? Warum funktioniert sie eher nicht – sondern erzeugt durch Optimierungskonzepte (z.B. Roadpricing) mehr Verkehr?

Das Modell ist Akteursorientiert und stellt v.a. die Frage nach dem Zusammenhang zwischen der Alltagsorganisation der Menschen und ihren Gewohnheiten bezüglich der Mobilität. Nur wenn diese Zusammenhänge berücksichtigt werden, läßt sich Verkehr vermeiden.

(Dagmar Boedicker)

Regionalgruppe Erlangen/ Fuerth/Nuernberg

Terminänderung:

Die Regionalgruppe Erlangen/Fuerth/Nuernberg trifft sich seit kurzem jeden 2. und 4. Montag (frueher: Dienstags) um 19.30 Uhr. Wir treffen uns abwechselnd in Erlangen, Fuerth oder Nuernberg und freuen uns ueber jedeN, die/der uns einmal besucht und vielleicht auch Lust hat, mitzuarbeiten. Weitere Infos gibt es bei:

Klaus Thielking-Riechert,
Sommerstr.10,
90762 Fuerth,
Tel.: 0911/7499672
e-Mail: k.thielking@link-n.cl.sub.de

Regionalgruppe Bremen

Vernichtungskrieg

> *„Es wird niemand leichter ein Mörder als ein Vaterland. (...) Vaterland nennt sich der Staat immer dann, wenn er sich anschickt, auf Menschenmord auszugehen."*
> *Friedrich Dürrenmatt, Romulus der Große*

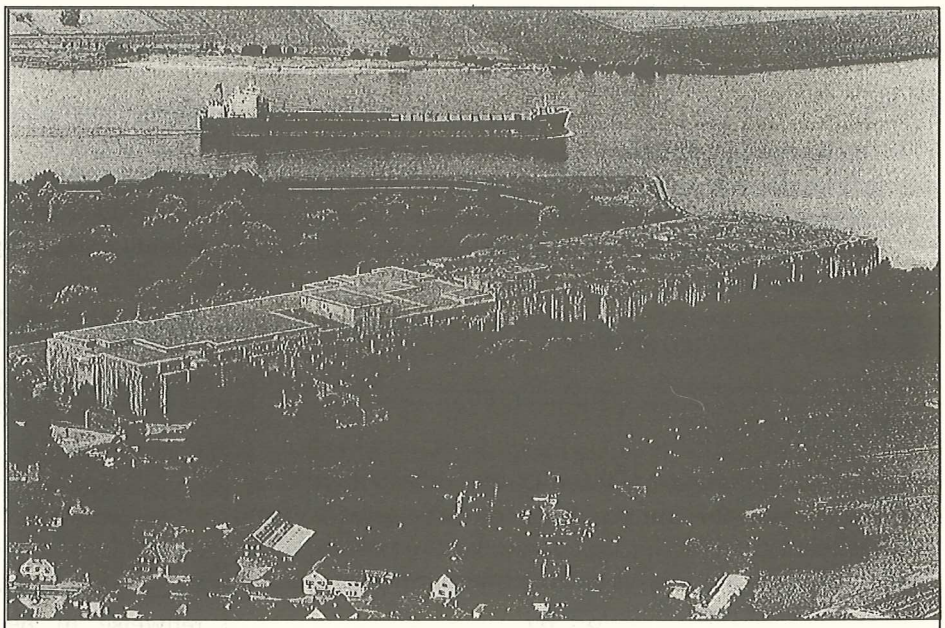
Etwa 20 Mitglieder der FIFF-Regionalgruppe Bremen, teilweise in Begleitung von PartnerIn und Kindern, besuchten im Juni gemeinsam die Ausstellung „Vernichtungskrieg. Verbrechen der Wehrmacht von 1941 bis 1944" des Hamburger Instituts für Sozialforschung und nahmen an einer Führung teil. Über den Aufstellungsort der bekanntlich überall für Aufregung sorgenden Ausstellung – die untere Rathaushalle in Bremen – hatte es im Vorfeld heftigen Diskussionen gegeben (Dank geht z.B. an die CDU, die so sicherlich den hohen Besucherandrang noch gesteigert haben dürfte). In der Ausstellung werden exemplarisch Verbrechen der Wehrmacht in Wort und Bild dokumentiert, wobei gerade das, was der Ausstellung oft vorgeworfen wurde – kollektive Schuldzuweisungen – bewußt vermieden wird. Jedoch wird deutlich auf die systematischen Strukturen hingewiesen, die derartige Verbrechen ermöglicht und gefördert haben. Teilweise drastische Dokumente und Photographien lassen Menschenverachtung und Zynismus deutlich werden. Überaus wichtig und informativ sind jedoch auch die Schautafeln, die sich mit der Nachkriegsauseinandersetzung beschäftigen: Zum einen wird die politische Aufarbeitung in der Bundesrepublik, der DDR und in Österreich dokumentiert. Zum anderen zeigen Beispiele aus Illustrierten und der Medienbranche allgemein (z.B. Film), wie nach dem Krieg die vorher enge Verbindung zwischen nationalsozialistischer Ideologie und Wehrmacht systematisch aufgelöst wurde – ein Indikator hierfür ist z.B. die Verwendung der jeweiligen Symbole. Zukünftige Dokumentationen zu diesem Thema können und müssen zusätzlich den Streit um diese Ausstellung zum Thema machen, der verdeutlicht, wie wenig Auseinandersetzung (und wieviel Verdrängung und Verleugnung) bislang stattgefunden hat. Ansatzweise hat diese Reflexion mit einer Schautafel voller Zeitungsberichte zu den durch die Ausstellung ausgelösten Aufregungen begonnen. Die öffentliche Debatte um die wichtige und eindrückliche Ausstellung wurde in Bremen konstruktiv gewendet und führte zu einem umfangreichen und interessanten Begleitprogramm an Informations- und Diskussionsveranstaltungen.

Einige Literaturhinweise:

- Hamburger Institut für Sozialforschung (Hrsg.) (1996): Vernichtungskrieg. Verbrechen der Wehrmacht 1941-1944. Ausstellungskatalog mit Beiträgen von Bernd Boll, Hannes Heer, Walther Manoschek, Hans Safrian. Verlag Hamburger Ed.. 222 S., 801 Abb., ISBN 3-930908-24-7 Preis 40,- DM
- Thiele, Hans G. (Hrsg.) (1997): Die Wehrmachtsausstellung. Dokumentation einer Kontroverse. Dokumentation der Fachtagung in Bremen am 26. Februar 1997 und der Bundestagsdebatten am 13. März und 24. April 1997. Hrsg. im Auftrag der Landeszentrale für politische Bildung Bremen. Bremen: Temmen. 250 S., ISBN 3-86108-700-6 Preis 14,80 DM
- Donat, Helmut; Strohmeyer, Arn (Hrsg.) (1997): Befreiung von der Wehrmacht: Dokumentation der Auseinandersetzung über die Ausstellung 'Vernichtungskrieg – Verbrechen der Wehrmacht 1941 bis 1944' in Bremen 1996/97. Bremen: Donat. 253 S., ISBN: 3-931737-42-X Preis 24,80 DM
- Manoschek, Walter (Hrsg.) (1996): Die Wehrmacht im Rassenkrieg: Der Vernichtungskrieg hinter der Front. Picus. 223 S., ISBN: 3-85452-295-9 Preis 39,80 DM

Noch drei Literaturhinweise zu einer verwandten Debatte, nämlich der um das Tucholsky-Zitat „Soldaten sind Mörder" und den Ehrenschutz für die Bundeswehr:

- Hepp, Michael; Otto, Viktor (Hrsg.) (1996): Soldaten sind Mörder Dokumentation einer Debatte 1931-1996. Berlin: Links. 392 S., ISBN 3-86153-115-1 Preis 38,- DM
- Hepp, Michael (Hrsg.) (o.J.): „Soldaten sind Mörder" – Zitate aus zwei Jahrtausenden. (Herausgegeben im Auftrag der Kurt-Tucholsky-Gesellschaft). Berlin: Kurt-Tucholsky-Gesellschaft. Preis: 3,- DM
- Internationale Ärzte für die Verhütung des Atomkrieges (IPPMW); Komitee für Grundrechte und Demokratie; Humanistische Union; Verein für Friedenspädagogik Tübingen (Hrsg. (1990): Sind Soldaten Mörder? Analysen und Dokumente zum „Soldatenurteil". Tüningen: Verein für Friedenspädagogik. 224 S., ISBN 3-922833-60-8 Preis 20,- DM



Der U-Boot-Bunker in Bremen-Farge. Deutlich zu erkennen der von der Bundeswehr genutzte, Ende der achtziger Jahre zuletzt sanierte, östliche Teil des Bunkers. (aus: „Fabrik für die Ewigkeit" mit freundlicher Genehmigung des Junius-Verlages)

„UniTranswehr" prüfte Projekte auf militärische Verwendbarkeit

Auf dem jährlichen Projekttag des Studiengangs Informatik am 11. Juli 1997 betätigten sich Mitglieder der FIFF-Regionalgruppe Bremen, ausgerüstet mit einem T-Shirt „UniTranswehr" und einem Klemmbrett, als engagierte BefragerInnen in Sachen militärische Verwendbarkeit der (eigentlich durchwegs zivilen) Projektergebnisse. Unter dem Schlagwort „Freischuß-Diplomarbeiten" informierte „UniTranswehr" über die Möglichkeit, vierwöchige Kurz-Diplomarbeiten anzufertigen, die im Erfolgsfall voll gewertet werden, bei Mißerfolg jedoch keine Konsequenzen haben. Die Diplomarbeitsthemen müßten aus den auf dem Projekttag vorgestellten studentischen Projekten abgeleitet werden und sie sollten auf die Bedürfnisse von Bundeswehr und NATO-Partnern zugeschnitten sein. Eine finanzielle Förderung bis DM 10.000 pro Diplomarbeit sei möglich. Beteiligte der fünf studentischen Projekte und ebenso Gäste und Besucher wurden alsdann interviewt, welche Einsatzmöglichkeiten der Projektergebnisse ihnen für die Bereiche Militär und innere Sicherheit einfielen. Die Ergebnisse wurden ausgehängt. Ziel der Aktion war es, einmal mehr die Reflexion über Mißbrauchsmöglichkeiten von Forschungs- und Entwicklungsarbeiten im Informatikbereich anzustoßen. Was als Satire gedacht war – fragten da schließlich studiengangsbekannte FIFFerlinge nach möglichen Militärkooperationen –, bekam jedoch schnell einen etwas bitteren Beigeschmack, als wir erleben mußten, daß eine gar nicht so geringe Zahl der Befragten das Angebot für echt – und interessant (!) – hielt. So klebten wir – um unsere Intention allgemein klar zu machen – in der nächsten Pause „Satire"-Schilder über die T-Shirts. Einige fühlten sich durch die Aktion ziemlich angefaßt („Schwachsinn!") oder stellten in Frage, ob FIFF auf dem Projekttag überhaut etwas zu suchen hätte. Für manchen Bremer FIFFerling war diese Aktion ein wenig desillusionierend, haben wir doch die Hoffnung, daß unsere regelmäßigen Aktionnen zum Thema „Rüstung und Informatik" innerhalb und außerhalb des Informatik-Studiengangs bewußt-

seinsbildend wirken. Insofern war es natürlich tröstlich, daß viele die Aktion auch als das erkannten, als was sie gedacht war. Doch selbst dann zeigte sich manch einer überrascht: „Ich hätte nicht gedacht, daß man nach kurzem Nachdenken zu jedem der Projekte militärische Verwendungsmöglichkeiten finden kann!", betonte beispielsweise einer der befragten Studenten. Gekoppelt war die Aktion mit einem zentral positionierten Bücher- und Infostand der FIFF-Regionalgruppe, der insgesamt auf positive Resonanz stieß. Am Stand hingen u.a. auch Plakate mit einem Beschluß des Akademischen Senats der Universität Bremen: „Der Akademische Senat lehnt jede Beteiligung von Wissenschaft und Forschung mit militärischer Nutzung bzw. Zielsetzung ab und fordert die Mitglieder der Universität auf, Forschungsthemen und -mittel abzulehnen, die Rüstungszwecken dienen können."

Zensur für Nazis – ja/nein

Am 8. Juni 1997 versandte Wau Holland, einer der Mitbegruender des Chaos Computer Club, über die Mailingliste NETTIME-D einen zur Publikation in einem „Online-Magazin" des MedInform Verlages bestimmten Artikel mit dem Titel „Meinungsfreiheit – das wichtigste Grundrecht. Straffreiheit auch für Nazis im Internet, solange sie gewaltlos Meinungen äussern". Die in dem Text aufgestellten Behauptungen und Thesen erzeugten bei mehreren Mitgliedern der FIFF-Regionalgruppe Bremen nachhaltigen Ärger, der letztendlich in einer ausführlichen Antwort mündete, die sowohl über NETTIME-D als auch über die FIFF-Mailingliste versandt wurde. In der Antwort wurde vor allem herausgestellt, daß das Recht auf Meinungs- und Informationsfreiheit keinesfalls Verbrechen oder die Verletzung der Menschenrechte und Menschenwurde anderer Personen rechtfertigen kann und darf. Nicht eine binäre Frage „Zensur – ja oder nein" ist zu diskutieren, sondern die Frage, wie mit problematischen Inhalten umzugehen ist, welches Spektrum von Regulationsmöglichkeiten es gibt. Die unreflektierte Dichotomisierung von Diskussionsbeiträgern in „Freiheitsverteidiger" und „Zensierer", die sich teilweise auch in den Reaktionen auf unsere Antwort zeigte, verhindert die konstruktive inhaltliche Auseinandersetzung und die Entwicklung sozialer und gesellschaftlicher Reaktionen jenseits staatlicher Reglementierung.

Vernichtung durch Arbeit

Mehrere Mitglieder und Freunde der FIFF-Regionalgruppe Bremen beteiligten sich zum Antikriegstag 1997 an einer von der Internationalen Friedensschule Bremen-Vegesack veranstalteten eine Führung im Bunker Valentin. Dieser Bunker, nördlich von Bremen in Farge direkt an der Weser gelegen, wurde in 18 Monaten zwischen 1943 und 1945 aus dem Boden gestampft. Etwa 10000 bis 12000 Zwangsarbeiter arbeiteten gleichzeitig auf der Baustelle und errichteten ein architektonisches Ungetüm (über 400 Meter lang, 70-100 Meter breit, 25 Meter hoch; für den Bunker wurde soviel Beton verbaut wie für eine Stadt mit 30 000 Einwohnern, allein die Decke besteht aus 7 Meter dickem Beton). In ihm sollte eine komplette U-Boot-Werft entstehen, in der monatlich mehr als ein Dutzend U-Boote hergestellt werden sollten. Die Arbeiter stammten aus verschiedenen Lagern im Umkreis, darunter u.a. das Kriegsgefangenenlager Schwanewede, das Arbeitserziehungslager Farge und zwei Außenlager des KZ Neuengamme. Die Zwangsarbeiter mußten unter katastrophalen Bedingungen und Mißhandlungen Schwerstarbeit leisten – die SS rechnete mit einer „durchschnittlichen Verweildauer" von neun Monaten. Wieviele Menschen dort insgesamt gearbeitet haben und wieviele ums Leben kamen ist bis heute ungeklärt.

Klaas Touber aus Holland – er war Gefangener in dem der Gestapo unterstehenden Arbeitserziehungslager Farge – erzählte im Rahmen der Bunkerführung von dieser Zeit. Seine Rede im Inneren des Bunkers ließ erkennen, welch gravierende Nachwirkungen diese traumatischen Erlebnisse noch Jahrzehnte später auf die betroffenen Menschen haben.

Heute ist im vorderen Teil des Bunkers ein Marinedepot der Bundeswehr untergebracht. Anders als die seit einigen Jahren von der Bundeswehr angebotenen Führungen, stellte die Veranstaltung der Internationalen Friedensschule, an der rund 200 (!) Besucher teilnahmen, nicht das technische Bauwerk, sondern die Menschen in den Mittelpunkt. Abschließend wurde auch über den weiteren Umgang mit dem Gebäude gesprochen: Gerd Meyer von der Internationalen Friedensschule plädiert dafür, den Bunker als Mahnmal zu belassen, jedoch nicht zu nutzen (es gab im Laufe der Jahre einige absurd anmutende Ideen von der Installation von Windkraftanlagen bis hin zu einem Dachcafé). Die Bundesmarine plant das Bunkerdepot noch bis mindestens 2005 zu erhalten.

Im Oktober/November will die Internationale Friedensschule erneut eine Bunkerführung mit einem Zeitzeugen organisieren. Interessierte FIFFerlinge können sich bei der FIFF-Regionalgruppe Bremen melden – wir informieren euch dann über den genauen Termin.

Literaturhinweise:

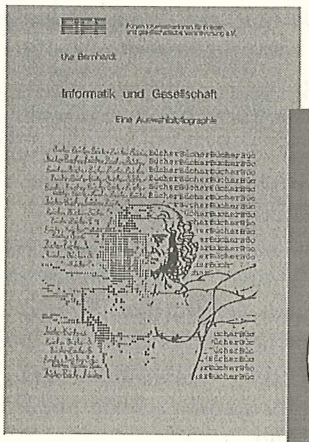
- Aschenbeck, N.; Lubricht, R.; Roder, H. u.a. (1995): Fabrik für die Ewigkeit: Der U-Boot-Bunker in Bremen-Farge. Hamburg: Junius.
- Portefaix, R.; Migdal, A.; Touber, K. (1995): Hortensien in Farge. Überleben im Bunker „Valentin". Bremen: Donat.

„SOFTWEHRTECHNIK – Mit Sicherheit ein gutes Gefühl"

Derzeit beschäftigt sich die Bremer Gruppe u.a. mit der Vorbereitung einer AG zum Themenfeld „Rüstung und Informatik" für die Jahrestagung in Paderborn. Weitere Beitragsanmeldungen sind willkommen.

(Ralf E. Streibl)

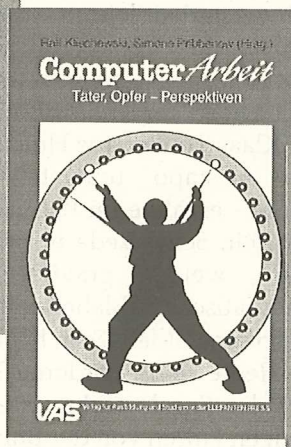
FIFF Bibliothek



Ute Bernhardt: Informatik und Gesellschaft. Eine Auswahlbibliographie

Ein thematisch gegliederter Einstieg in die Literatur zu Informatik und Gesellschaft

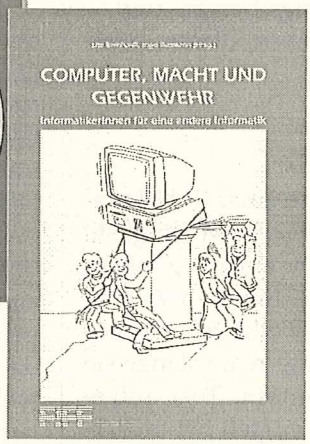
26 Seiten, Bonn 1990, 3,– DM



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 unver-NETZbar.

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**

NEU: „Datendschungelbuch – *Ein pfiffiger Wegweiser für Ihren persönlichen Datenschutz" als elektronische Version unter* **http://www.bawue.de:80/~ernie/index.html** *wieder für alle Interessierte verfügbar.*

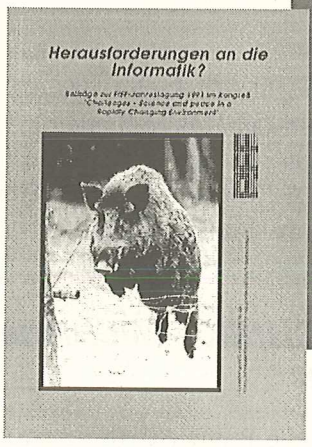
Ute Bernhardt, Ingo Ruhmann (Hrsg.): Ein sauberer Tod: Informatik und Krieg.

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

320 Seiten, Marburg 1991, 20,– DM

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**



Heike 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

Alle Bücher zzgl. Porto zu beziehen bei: FIFF-Geschäftsstelle, Reuterstr. 44, 53113 Bonn

Vielzweck-Schnipsel

Kopieren, ausfüllen und einsenden an: FIFF e.V., Reuterstraße 44, 53113 Bonn

FIFF

Das möchte ich:

- ❒ ***Ich möchte ❒ aktives / ❒ förderndes Mitglied des FIFF werden*** *(Mindestjahresbeitrag ist für Verdienende **100,- DM**, für Studierende und Menschen in vergleichbarer Situation **25,- DM** pro Jahr. Mitglieder in den neuen Bundesländern zahlen **60%** des Beitrags.)*
- ❒ ***Ich möchte die FIFF-Kommunikation zum Preis von 25,- DM jährlich frei Haus abonnieren.***
- ❒ ***Ich überweise den Mitglieds- bzw. Abobeitrag auf das Konto 480 00 798 bei der SPK Bonn, BLZ 380 500 00.***
- ❒ ***Der Mitglieds- bzw. Abobeitrag soll per Lastschriftverfahren von meinem Konto abgebucht werden*** *(siehe unten).*
- ❒ ***Ich möchte meine neue/korrigierte Anschrift mitteilen*** *(siehe unten).* ***Meine alte/falsche Anschrift:***

  Straße: _____ *Wohnort:* _____
- ❒ ***Ich möchte dem FIFF etwas spenden:***
- ❒ *Verrechnungsscheck über* _____ *DM 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:* _____ *DM, 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

Themen-schwerpunkte

für die FIFF-Kommunikation im Jahr 1997:

4/97 »Arbeit«

zuständig: *Ditz Schroer, Friedrich Holl*

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: 6 DM. Der Bezugspreis für die FIFF-Kommunikation ist für FIFF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIFF-Kommunikation für 25 DM/Jahr (inkl. Versand) abonnieren.

Erscheinungsweise: einmal vierteljährlich

Erscheinungsort: Bonn

Auflage: 2000

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

Verlagsadresse: FIFF-Geschäftsstelle, Reuterstr. 44, 53113 Bonn, Tel. (0228) 21 95 48

ISSN 0938 – 3476

Druck: Printwerkstatt Rambow, Auguststr. 10, 53229 Bonn, Tel. (0228) 46 22 14

Layout: Markus Hoff, Harald Selke

Titelfoto: Safe zur Aufbewahrung von Datensicherungsbändern, Harald Selke

Grafik Editorial: erschienen in DuD 4/97, mit freundlicher Genehmigung des Vieweg-Verlags

Redaktionsadresse: FIFF-Kommunikation, Reuterstr. 44, 53113 Bonn, Tel. (0228) 21 95 48, Fax (0228) 21 49 24, 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.biskup@sdm.de

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

Redaktionsschluß für die Ausgabe 4/97: 31.10.1997

Redaktions-Team FIFF-Kommunikation 3/97: Ute Bernhardt, Markus Hoff, Ingo Ruhmann, Claus Stark, Harald Selke (verantwortlich)

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!

Adressen

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

Bonn
Manfred Domke
Am Wildpfad 12
53639 Königswinter
manfred.domke@gmd.de

Braunschweig
TU Braunschweig
Fachschaft Informatik
AStA-Fach
Katharinenstraße 1
38106 Braunschweig

Bremen
Prof. Dr. Hans-Jörg Kreowski
Uni Bremen
FB Informatik/Mathematik
Postfach 330440
28334 Bremen
Tel.: (0421) 218-2956
fiff@informatik.uni-bremen.de
http://www.informatik.uni-bremen.de/~res/fiffhb.html

Darmstadt
Peter Bittner
Jens Woinowski
Hochstr. 56
64285 Darmstadt
Tel.: 06151/41805
bittner@mathematik.th-darmstadt.de
woinowsk@iti.informatik.th-darmstadt.de

Erlangen/Fürth/Nürnberg
Klaus Thielking-Riechert
Sommerstraße 10
90762 Fürth
k.thielking@link-n.cl.sub.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
Brigitte Wolf
Tel.: 07131 / 86505
email: bwolf@jupiter.rz.fh-heilbronn.de

Kaiserslautern
Frank Leidermann
Moltkestraße 58
67655 Kaiserslautern
f_leider@informatik.uni-kl.de

Karlsruhe
Thomas Freytag
Institut AIFB
Universität Karlsruhe
76128 Karlsruhe
Tel.: (0721) 6084063 (d)
(0721) 815416 (p)
E-Mail: 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 Schuchardt
Jungerhalde 78
78464 Konstanz

Leipzig
Dr. Rolf Stranzky
Freiburger Allee 9
04416 Markkleeberg
Tel.: 0341/35879-23
Fax: 0341/35879-26

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

Münster
Werner Ahrens
Hohe Geest 120
48165 Münster
Tel.: (02051) 3054 (p)
(0251) 491-429 (d)

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

Regensburg
Paul Hilmer
Zollerstraße 13
93053 Regensburg
Tel.: (0941) 706542
Fax: (0941) 706540
P.Hilmer@LINK-R.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
http://www-fiff.informatik.uni-tuebingen.de

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

Überregionale Arbeitskreise

AK »RUIN« (Rüstung und Informatik)
Ingo Ruhmann
Paulstraße 15
53111 Bonn
Tel.: (0228) 634816
fiff@fiff.gun.de

AK »FIFF in Europa«
Dagmar Boedicker
Daiserstraße 45
81371 München
Tel.: (089) 7256547

AK »Informationstechnik für eine lebenswerte Welt«
Ralf Klischewski
Universität Hamburg
FB Informatik
Vogt-Kölln-Straße 30
22527 Hamburg
Tel.: (040) 54715-367
Fax: (040) 54715-311
klischew@informatik.uni-hamburg.de

FIFF-Mailingliste
Beiträge an:
fiff-l@dia.informatik.uni-stuttgart.de
An- und Abbestellungen an:
fiff-l-request@dia.informatik.uni-stuttgart.de

FIFF-WWW-Seiten
http://hyperg.uni-paderborn.de/~FIFF

FIFF-Geschäftsstelle

Reuterstraße 44
53113 Bonn

Tel.: (0228) 219548
Fax: (0228) 214924

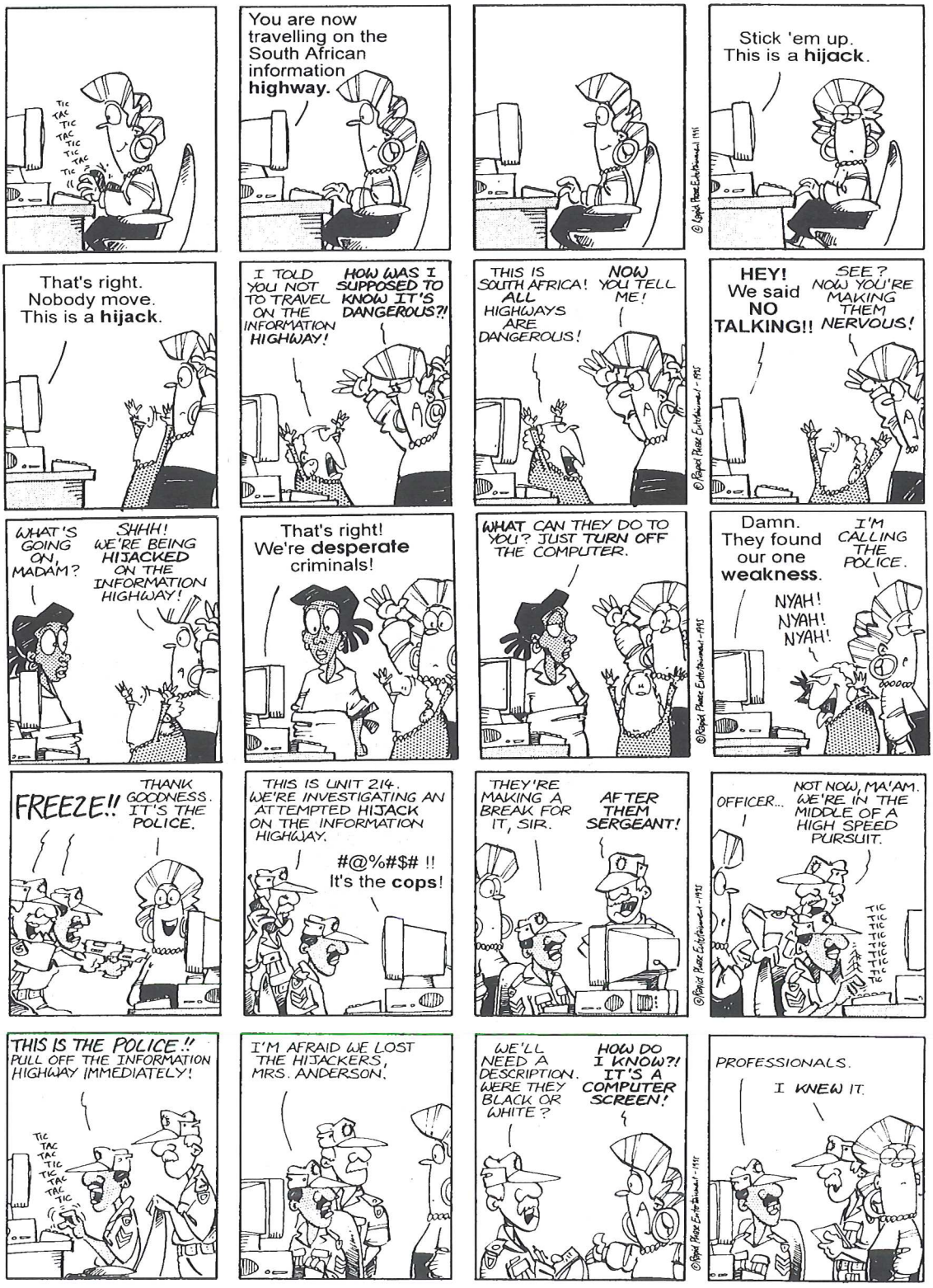
E-Mail: fiff@fiff.gun.de

Dienstags 9 bis 15 Uhr,
Donnerstags 16 bis 19 Uhr

Kontoverbindung: 48000798
Sparkasse Bonn, BLZ 380 500 00

Schluß - PFIFF

WOZU SICHERHEIT AUF DEM DATENHIGHWAY?



"Madam&Eve" ist eine sehr bekannte Comicreihe in Suedafrika, Nachdruck mit freundlicher Genemigung des Cartoonisten Harry Dougmore (Madam&Eve-Homepage: http://www.web.co.za/mg/m&e/index.htm)

Geeignete Texte für den Schluß-PFIFF bitte mit Quellenangabe an Claus Stark (Adresse siehe Adreßverzeichnis) senden.