H 7625

FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

20. Jahrgang 2003 Einzelpreis: 5 EUR **3/2003 - September 2003**

Arbeit und Wissen

- **Neues aus der Arbeitswelt**
- **Nachschlag zur IT-Sicherheit**
- **Datenschutz**

ISSN 0938-3476

• FIfF-Jahrestagung 2003 • Aktuelles • Viele interessante Bücher •

FIfF Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Titelbild „puzzle“
von Matthias Krauss

inhalt

Inhalt

Ausgabe 3/2003

Editorial

Das FIfF e.V. hat viele Mütter und Väter, und eine davon hat dieses Jahr – jetzt darf ichs ja schreiben – ihren sechzigsten Geburtstag gefeiert. Wenn auch mit Verspätung wünschen wir dir, liebe Christiane, alles Gute, viel Glück und weiterhin viel Energie für dein Wirken, besonders natürlich was die FIfF-Themen betrifft. Hoffentlich findest du auch in diesem Heft wieder Dinge, die dich interessieren.

Wir wollten uns wieder einmal dem weiten Feld der *Arbeitswelt* zuwenden, und dazu beleuchten die Autorinnen und Autoren vielfältige Aspekte: Eingriffe in die informationelle Selbstbestimmung von Arbeitnehmern, und ob sie erlaubt sind (Peter Wedde), eine Globalisierungs- und Kapitalismuskritik am Beispiel SAP aus Sicht einer Soziologin (Sabine Pfeiffer) und praktische Tipps für Studierende, die sich auf die Unternehmenswelt einstellen müssen (Cornelia Gschmack). Auch die gewerkschaftliche Sicht: Was können Gewerkschaften den e-workern bieten (Karl-Heinz Brandl)? Wo endet die Regulierung von Arbeitsverhältnissen, wenn die Beschäftigten so in ihrer Rolle von Einhand-Seglern stecken, dass sie sich für Gewerkschaften kaum interessieren (Raphael Menez und Stefanie Springer)? Esther Ruiz Ben und Dietlinde Quack befassen sich mit dem Nachhaltigkeits-Versprechen des *e-work.*

Weil wir im letzten Heft einige Aspekte der IT-Sicherheit nicht abdecken konnten, haben wir diesmal noch ein bisschen Datenschutz dazu gepackt und liefern einen Nachschlag: Es geht um die Risiken der mobilen Arbeit mit PDAs, Laptops u.ä. mit *GPRS, UMTS* und in drahtlosen Netzen (Claudia Eckert), Videoüberwachung und Bürgerrechte (AK Videoüberwachung und Peter Bittner), TCPA (Dagmar Boedicker) und dies und das. Dazu dürfte auch Rubrik *Lesen* nützlich sein: Werner Hülsmann hat eine ganze Reihe von Büchern zu diesem Thema besprochen.

Und dann steht natürlich die Jahrestagung vor der Tür. Wer darüber Genaues wissen will, wie beispielsweise Beschreibungen der AGs oder Vorträge, Anmelde-Information usw., findet es unter *FIfF e.V.,* wie auch die gewohnten Kontakte und Informationen zu unseren Aktivitäten.

Zum Schluss noch ein besonders herzliches Dankeschön an die Autorinnen und Autoren dieser Ausgabe der FIfF-Kommunikation: Ich musste sie diesmal bitten, sehr schnell zu reagieren und ihre Beiträge fast *auf Zuruf* zu schreiben, in fünf Wochen statt mit dem üblichen Vorlauf von etwa drei Monaten. Das haben sie mit Bravour getan. Danke! Schwächen und Fehler in dieser FIfF-Kommunikation sind dagegen mir anzulasten, die lassen sich bei einsamer Wühlerei wohl nicht vermeiden.

Ach ja – noch was: Wie finden Sie/ihr das neue Layout? Ein paar kleine Schwächen hat Carsten Büttemeier inzwischen ausgebügelt, sieht doch nicht schlecht aus, oder?

Eine anregende Lektüre wünscht,
Dagmar Boedicker

Dagmar Boedicker

Dagmar Boedicker ist freiberufliche technische Redakteurin und Mitglied im Vorstand des FIfF e.V. Sie hat Politikwissenschaft studiert.

Peter Wedde

Vertrauen klingt gut - Kontrolle geht gut!

Anmerkungen zur neuen Überwachungskultur in der Arbeitswelt

Die besten Geschichten schreibt das Leben bekanntlich selbst. Diese Feststellung gilt auch für Realsatire aus der Arbeitswelt.

In einem Unternehmen eines großen deutschen Konzerns hatte sich der Arbeitgeber vor einigen Monaten entschlossen, die elektronische Zeiterfassung und das dahinter stehende Gleitzeitmodell ersatzlos abzuschaffen. Stattdessen wurde „Vertrauensarbeitszeit" eingeführt. Der Arbeitgeber verfügte, dass die mündigen Beschäftigten ab sofort selbstbestimmt arbeiten können, wann immer sie dies wollen. Wie viel Zeit sie für die Erledigung einzelner Arbeitsaufgaben aufwenden, sollte ihnen vollständig selbst überlassen werden. Auch die Einhaltung der gesetzlichen Arbeitszeitvorgaben wie etwa zur Höchstarbeitszeit nach den §§ 3ff. Arbeitszeitgesetz sollte in die Verantwortung der Beschäftigten überführt werden. Der Arbeitgeber wollte sich darauf beschränken, vorgelegte Arbeitszeitnachweise vertrauensvoll abzuzeichnen. Der Betriebsrat war mit diesem Vorgehen des Arbeitgebers nicht einverstanden und setzte unter Hinweis auf sein Mitbestimmungsrecht gemäß § 87 Abs. 1 Nr. 2 BetrVG bezüglich des Beginns und des Endes der Arbeitzeit eine Einigungsstelle gegen den erheblichen Widerstand des Arbeitgebers durch.

Praktisch zeitgleich wurde überraschten Mitgliedern des Konzernbetriebsrats in einer anderen Einigungsstelle, die sich mit der konzernweiten Einführung einer umfassenden Kommunikations-Infrastruktur auf Basis des Internets befasste, von Vertretern des Arbeitgebers mitgeteilt, dass mit diesem System auch eine umfassende Inhaltskontrolle der E-Mails und des Internet-Surf-Verhaltens der Beschäftigten sowie eine Auswertung aller weiter anfallenden Informationen (etwa im Termin- und Teamkalender, in *Chats*, in der einheitlichen Wissensdatenbank usw.) erfolgen sollte. Sein Recht zur Kontrolle sah der Arbeitgeber als Bestandteil des geschlossenen Arbeitsvertrags als gegeben an.

Eine Neuerung wurde auch für die Privatnutzung des umfassenden Systems verkündet. Entgegen der vorherigen Übung im Konzern sollte diese vollständig verboten werden. Der Arbeitgeber teilte zur Begründung dieses Schrittes mit, dass zur Sicherung der vollen Arbeitskraft verhindert werden sollte, dass die Beschäftigten während ihrer Arbeitzeit private E-Mails austauschen oder im Internet eigenen Interessen nachgehen.

Diese Aussage galt ausdrücklich für alle Konzernunternehmen - also auch für die, in denen es aufgrund der Vertrauensarbeitzeit keine Unterscheidung zwischen „dienstlicher" und „privater" Zeit mehr gab!

Was folgt aus diesem Beispiel?

Es ist zunächst einmal ein Indiz für die naheliegende Vermutung, dass Arbeitgeber die Kontrolle über ihre Beschäftigten und deren Arbeitsleistung auch nach Einführung von *Vertrauensarbeitzeit* nicht aus der Hand geben wollen. Von einer *neuen Freiheit* für Arbeitnehmer kann wirklich nicht die Rede sein. Es bleibt eigentlich alles beim Alten. Neu ist, dass die IT-Technik es Arbeitgebern ermöglicht, auf die antiquierte Kontrollmethode der summierenden Zeiterfassung zu verzichten. Sie können die Zeitautonomie deshalb ohne Probleme mit großzügiger Geste und verpackt in schöne Worte an ihre Arbeitnehmer übergeben - wohl wissend, dass ihnen auf Basis der Daten, die bei der Arbeitserledigung in den elektronischen Systemen und Netzen anfallen, viel effizientere Kontrollwerkzeuge zur Verfügung stehen.

Zudem wird mit Einführung der Vertrauensarbeitszeit ein Teil des Betriebsrisikos auf die Beschäftigten verlagert. Wer seine Arbeit nicht in der geplanten Zeit schafft, kann sie zu anderer Zeit getrost und freiwillig nachholen. Ob dies am Abend oder in der Nacht bzw. am Wochenende passiert, bleibt den autonomen Arbeitnehmern überlassen. Dass sie selbst, und nicht der Arbeitgeber, dabei auch für die Einhaltung der gesetzlichen Höchstarbeitszeiten verantwortlich sein sollen, versteht sich schon fast von selbst. Für Arbeitnehmer, die dies nicht verstehen, fügen die Arbeitgeber freundlicherweise Formulierungen wie „für die Einhaltung der Vorgaben des Arbeitszeitgesetzes sind die Arbeitnehmer verantwortlich" in Arbeitsverträge oder Betriebsvereinbarungsentwürfe ein. Auch die mit einem solchen Vorgehen verbundene bewusste Umgehung gesetzlicher Schutzbestimmungen wird den Betroffenen positiv als „neue Form der Autonomie im Angesicht einer den Einzelnen ungebührlich beschränkenden Gesetzgebung" verkauft. Dieses Argument fällt gerade bei Beschäftigten der IT-Branche oft auf fruchtbaren Boden. Wer dann völlig autonom rund um die Uhr, nachts und an Wochenenden arbeitet, vergisst schon einmal, dass gesetzliche Arbeitszeitbegrenzungen sich historisch aus der Erkenntnis ableiten, dass zu viel Arbeit auf Dauer krank macht.

Informationelle Selbstbestimmung?

Kommen wir nach diesem kurzen Exkurs in das Arbeitszeitrecht zurück in die Welt der gläsernen Arbeitnehmer. Das oben angesprochene Beispiel ist stellvertretend für einen Trend, den es in Deutschland in einer zunehmenden Zahl von Betrieben und Unternehmen gibt: Die mächtigen Erfassungsmöglichkeiten, die der Einsatz von Informationstechnik mit sich bringt, werden in einer immer größeren Zahl von Fällen von Arbeitgebern genutzt, um das Arbeitsverhalten der Beschäftigten detailliert zu erfassen und zu bewerten. Dem Umfang der Datenerhebung sowie den Formen der Auswertungen sind praktisch keine Grenzen mehr gesetzt. Bisher war ein solches Vorgehen vorwiegend aus dem Ausland und hier insbesondere aus den USA bekannt. Dort sol-

len etwa in High-Tech-Unternehmen bereits zwischen 1/3 und 3/4 aller E-Mails auf bestimmte *Reizworte* hin gescannt und ab einer bestimmten *Trefferquote* von Beauftragten des Arbeitgebers gelesen werden. Das zu den indizierten Reizworten auch solche wie „Gewerkschaften", „Streik", „Gehaltserhöhung" oder „Jobsuche" gehören, lässt sich mit einer hohen Wahrscheinlichkeit vermuten. Indes ist diese neue Form der Kontrolle in den USA längst nicht mehr auf Bildschirmarbeitsplätze in den Büros beschränkt. Sie erfasst inzwischen praktisch alle Bereiche der Arbeitswelt, in denen Daten in irgendeiner Form anfallen. So soll es beispielsweise bei großen Supermarktketten in den USA üblich sein, dass das *Kassierverhalten* permanent erfasst und ausgewertet wird. Öffnet eine Kassiererin die Kassenschublade zu oft oder abweichend von der *üblichen* Verhaltensnorm, macht sie sich damit aus Sicht des eingesetzten Computerprogramms ebenso als mögliche Diebin verdächtig wie diejenige, die die Korrekturtaste zu häufig betätigt. Und selbst bei korrekter (sprich: programmkonformer) Bedienung der Kasse kann es passieren, dass eine Kündigung erfolgt, weil eine Beschäftigte im Vergleich zu anderen Kolleginnen und Kollegen zu langsam kassiert - was das Programm anhand von Parametern wie *Scan-Geschwindigkeit* in Relation zum Gewicht der Ware permanent und automatisch bewertet. Ergebnis der Bewertung kann sowohl die Identifikation der „Kassiererinnen des Monats" als auch die der „zu kündigenden Beschäftigten" sein.

Wer nun sagt, in der BRD bestehe ja eine andere Rechtssituation und deshalb könne es so etwas hier nicht geben, der sei darauf hingewiesen, dass auch bei uns große Unternehmen (dem Vernehmen nach beispielsweise *Infineon*) laut darüber nachdenken, durch ein jährliches *Scoring* auf der Basis von in den IT-Systemen erfassten Leistungsdaten einerseits die leistungsstärksten Beschäftigten zu identifizieren und zu belohnen. Andererseits sollen mit der gleichen Methode die 5% *leistungsschwächsten* Arbeitnehmer entdeckt und vermutlich ebenfalls *belohnt* werden - mit einem Ausflug zum Arbeitsamt.

Informationen über das Arbeitsverhalten fallen in vielen IT-Systemen eher zufällig an. Sie können aber durch den Einsatz spezieller Software gezielt erhoben werden. Geeignete Programme finden sich auf dem kaum noch zu überschauenden Markt der Filter-, Content-Search- und Spy-Software.[1] Sie können je nach Ausgestaltung den Zugriff von Arbeitnehmern auf bestimmte Angebote verhindern, den Nachrichtenaustausch über das Internet regeln und beschränken, das konkrete Arbeitsverhalten einzelner Mitarbeiter überwachen usw. So unterschiedlich sie in ihrer technischen Konfiguration auch sind: Schmackhaft gemacht werden die Programme Arbeitgebern mit dem immer gleichen Argument. Die Verkäufer der Software rechnen ihnen immer wieder vor, dass nach (eigenen) wissenschaftlichen Untersuchungen der durchschnittliche Arbeitnehmer zwischen einem und zwei Drittel seiner gesamten Arbeitszeit am Arbeitsplatz mit privaten Aktivitäten beschäftigt ist.

Wird die entsprechende Software angeschafft, kann der Arbeitgeber beispielsweise den Zugriff auf bestimmte Internet-Seiten und -Inhalte verhindern. Gleichzeitig kann er protokollieren, was die Beschäftigten in *erlaubten* Bereichen tun. Damit lässt sich dann etwa erkennen, welche Arbeitnehmer E-Mails an den Betriebsrat geschickt haben oder welche die Seiten der zuständigen Datenschutzaufsichtsbehörde aufgerufen haben bzw. die der für den Betrieb zuständigen Gewerkschaft.

Mit Blick auf die zur Verfügung stehenden technischen Möglichkeiten ist es sicher kein Zufall, wenn die Zahl der Fälle zunimmt, in denen Arbeitnehmer von ihren Arbeitgebern ermahnt oder abgemahnt werden, weil sie sich etwa per E-Mail negativ über einen Chef und positiv über gewerkschaftliche Aktivitäten geäußert haben, oder weil sie im Internet zu lange auf den Seiten eines Ferienortes verweilten. Diese Tatsache führt unmittelbar zu einer juristischen Bewertung des Sachverhalts, bei der naturgemäß arbeitsrechtliche Aspekte im Vordergrund stehen.

Die juristische Sicht

Die vorstehenden Beispiele legen eine simple Frage nahe: Darf ein Arbeitgeber in der BRD dies alles eigentlich? - Will man die Frage juristisch beantworten, kommt man nicht an der grundlegenden Erkenntnis vorbei, dass es in der BRD nach wie vor keine speziellen Datenschutzregeln gibt, die den Besonderheiten des Arbeitslebens gerecht werden und die die mit umfassenden Leistungs- und Verhaltenskontrollen verbundenen Eingriffe in die Persönlichkeitsrechte der Beschäftigen ausschließen oder zumindest sinnvoll begrenzen. Insbesondere das lange versprochene *Arbeitnehmerdatenschutzgesetz* lässt weiter auf sich warten.[2] Gleiches gilt für entsprechende Aktivitäten auf Ebene der Europäischen Union, die bisher ebenfalls nicht zu einem Abschluss gekommen sind.

Auch der Blick auf die Rechtsprechung hilft nicht unmittelbar weiter. Höchstrichterliche Entscheidungen, die sich mit den individuellen Aspekten und der generellen Zulässigkeit der angesprochenen geschilderten Verhaltens- und Leistungskontrolle bei der Nutzung von IT-Systemen und E-Mail-Systemen bzw. des Internets befassen, stehen noch aus. Gleiches gilt bezüglich des Einsatzes von Spyware unterschiedlicher Couleur. Von Instanzgerichten liegen lediglich Urteile zu konkreten Einzelthemen wie etwa zur Zulässigkeit des Öffnens von passwortgeschützten Dateien eines erkrankten Arbeitnehmers vor.[3] Damit lässt sich die Zulässigkeit der Verhaltens- und Leistungskontrollen neuer Art nur unter Rückgriff auf vergleichbare juristische Fallgestaltungen wie etwa die Frage der Zulässigkeit des Mithörens von dienstlichen Telefongesprächen oder die Installation von Videokameras durch Arbeitgeber bewerten.

Aufschlussreich für den hier zu diskutierenden Sachverhalt ist insbesondere die einschlägige Rechtsprechung des Bundesarbeitsgerichts und des Bundesverfassungsgerichts. Beide Gerichte vertreten seit Jahren zum Themenfeld „Überwachung von Arbeitnehmern durch technische Einrichtungen" eine relativ klare Linie: Grundsätzlich sind Maßnahmen zur Verhaltens- und Leistungskontrolle auch im Arbeitsverhältnis nicht ausgeschlossen. Sobald mit Kontrollen aber in Grundrechte der betroffenen Arbeitnehmer eingegriffen wird (etwa in das Recht auf infor-

mationelle Selbstbestimmung, das Recht am eigenen Bild bzw. am eigenen Wort oder in das allgemeine Persönlichkeitsrecht), sind dem Handeln von Arbeitgebern aus verfassungsrechtlicher Sicht enge Grenzen gesetzt. Mit Blick auf den hohen Stellenwert verfassungsrechtlicher Garantien sind Eingriffe in Grundrechte der Arbeitnehmer immer nur als Ergebnis einer umfassenden Interessenabwägung zulässig, deren Maßstäbe *Erforderlichkeit* und *Verhältnismäßigkeit* sind. Nur wenn beide Aspekte für eine Kontrolle sprechen, darf sie erfolgen.

Erforderlichkeit kann gegeben sein, wenn eine Maßnahme notwendig ist, um den ungestörten Arbeitsablauf zu gewährleisten oder wenn sich nur durch eine Kontrollmaßnahme Warenverluste begrenzen lassen. Damit kann als Ergebnis einer Abwägung beispielsweise die Kameraüberwachung im Kassenbereich einer Bank oder in Warenhäusern zulässig sein. Kommen Kontrollmaßnahmen zum Einsatz, müssen die betroffenen Arbeitnehmer aber über die eingesetzten technischen Einrichtungen und deren Wirkungsweise umfassend unterrichtet werden. Als nicht erforderlich werden hingegen von der Rechtsprechung Überwachungsmaßnahmen angesehen, die nur dem Zweck der kostengünstigen und schnellen Information des Arbeitgebers dienen[4] oder eine sorgfältigere Arbeitserbringung bewirken sollen.

Ist die Erforderlichkeit eines Eingriffs festgestellt, kann seine Zulässigkeit durch den Grundsatz der **Verhältnismäßigkeit** begrenzt werden. Es sind nur solche erforderlichen Maßnahmen zulässig, die das schonendste Mittel zur Erreichung eines vom Arbeitgeber gewollten und rechtlich zu billigenden Zweckes sind.[5] Stehen dem Arbeitgeber zur Erreichen eines Zweckes verschiedene Handlungsalternativen zur Verfügung, muss er diejenige auswählen, die mit den geringsten Eingriffen in Grundrechte der Arbeitnehmer verbunden ist.[6] Hieraus folgt beispielsweise, dass eine persönlichen Kontrolle durch Vorgesetzte der Vorrang vor technischen Überwachungsmaßnahmen einzuräumen ist, wenn hierdurch der Eingriff in Grundrechte der Arbeitnehmer reduziert oder ausgeschlossen wird.

Ist der Einsatz technischer Einrichtungen unumgänglich, muss eine grundrechtswahrende Ausgestaltung gewählt werden. Für die Praxis bedeutet dies etwa, dass eine Überwachungskamera in der Kassenhalle einer Bank so angebracht sein muss, dass sie vorrangig Personen vor dem Schalter filmt und dass die Bänder nur nach einem Überfall ausgewertet, ansonsten aber automatisch überschrieben werden.

Wendet man die verfassungsrechtlich geprägten Grundsätze der Rechtsprechung auf die hier zu diskutierenden Konstellationen an, kommt man zu eindeutigen Ergebnissen: Zunächst einmal ist festzustellen, dass es Arbeitgebern für den Regelfall verwehrt bleibt, Kontroll- und Auswertungsmaßnahmen heimlich einzusetzen. Die verdeckte Installation von Content-Searchern oder Spy-Ware-Programmen ist damit ebenso unzulässig wie die Konfiguration einer Firewall in der Art und Weise, dass das Verhalten einzelner Arbeitnehmer geloggt und ausgewertet wird. Dies gilt selbst dann, wenn Arbeitgeber meinen, nur auf diese Art und Weise strafbares Handeln ihrer Mitarbeiter aufdecken zu können (etwa Geheimnisverrat per E-Mail). Sie müssen sich insoweit wie Arbeitnehmer an Recht und Gesetz halten - und ggf. Staatsanwaltschaft und Polizei mit Ermittlungen betrauen.

Will der Arbeitgeber in IT-Systemen vorhandene Daten zu Kontrollzwecken auswerten, oder will er spezielle Kontrollsoftware einführen, muss er dies seinen Arbeitnehmern vorab konkret ankündigen. Allerdings macht auch eine solche Ankündigung nicht jede Form der Kontrolle zulässig. Es sind vielmehr auch hier Grundrechte der Betroffenen zu wahren und geltende Gesetze zu beachten. Zunächst einmal muss die schon angesprochene verfassungsrechtlich geprägte Rechtsgüterabwägung erfolgen. Zudem sind die Vorgaben zu beachten, die das BDSG enthält. Von Bedeutung ist hier insbesondere die grundlegende Norm des § 4 Abs. 1 BDSG, nach der entsprechende Kontrollmaßnahmen nur zulässig sind, wenn sie eine gesetzliche Grundlage haben oder wenn eine Einwilligung der betroffenen Arbeitnehmer vorliegt.

Als gesetzliche Erlaubnisnorm kommt im Arbeitsverhältnis insbesondere § 28 Abs. 2 Nr. 1 BDSG in Betracht. Hiernach ist die Verarbeitung personenbezogener Daten im Rahmen der *Zweckbestimmung* eines Vertragsverhältnisses zulässig. Allerdings sind dem Umfang der zulässigen Verarbeitung durch das Gesetz enge Grenzen gesetzt. So sind gemäß § 28 Abs. Abs. 1 Satz 3 BDSG schon bei der Erhebung die Zwecke konkret festzulegen, für die die Daten verarbeitet oder genutzt werden sollen. Weiterhin ist das in § 4 BDSG enthaltene Gebot der Datenvermeidung und Datensparsamkeit zu beachten, nach dem Gestaltung und Auswahl von Datenverarbeitungssystemen stets mit dem Ziel erfolgen müssen, keine oder so wenig Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Schließlich muss der Arbeitgeber das in § 4 Abs. 2 BDSG enthaltene Gebot der Direkterhebung beim Betroffenen berücksichtigen. Will er den Inhalt einer dienstlichen E-Mail erfahren, muss er sich deshalb zuallererst an seinen Mitarbeiter wenden und diesen um einen Ausdruck oder um die Übersendung einer Kopie bitten. Erst wenn dieser die Einsicht in den Inhalt unberechtigt verweigert, kann er versuchen, sich den Einblick anderweitig zu verschaffen.

Ergebnis der Anwendung dieser beispielhaft angeführten normativen Vorgaben ist, dass Arbeitgeber ihren Arbeitnehmern schon vor der Erhebung von Daten mitteilen müssen, welche Überwachungs- und Kontrollmaßnahmen sie konkret durchführen wollen. Eine spätere *Umwidmung* vorhandener Daten zu diesen Zwecken ist hingegen sowohl datenschutzrechtlich als auch (aus den vorstehend dargelegten Gründen) in den meisten Fällen verfassungsrechtlich unzulässig.

An dieser Situation ändert sich auch nichts, wenn der Arbeitgeber die private Nutzung der im Betrieb eingesetzten Systeme verbietet. Auch in diesen Fällen hat er nicht das Recht, jegliche *dienstliche* Kommunikation zu kontrollieren. Es ist vielmehr zu beachten, dass es auch im Arbeitsleben *persönliche* oder *vertrauliche* Kommunikationsvorgänge gibt (etwa im Kontakt mit

dem Datenschutzbeauftragten oder mit dem Betriebsrat), deren Kenntnis dem Vorgesetzen oder dem Arbeitgeber verschlossen bleiben muss.

Private Einwilligung - keine Lösung

Als Zwischenergebnis kann an dieser Stelle festgestellt werden, dass auch im Arbeitsleben kein Raum für umfassende und unbegrenzte Verhaltens- und Leistungskontrollen ist. Will der Arbeitgeber diese durchführen, muss er nachweisen, dass dies die für ihn die *ultima ratio* ist und dass er sein Ziel nicht auf einem anderen, weniger grundrechtsschädlichen Weg erreichen kann. Vor dem Hintergrund dieser Feststellung meinen einige Arbeitgeber, einen Königsweg gefunden zu haben, der von ihnen gewollte umfassende Auswertungen möglich macht: Sie versuchen, die bestehende Rechtssituation dadurch zu ihren Gunsten zu beeinflussen, dass sie ihre Beschäftigten vertraglich zur Einwilligung in entsprechende Kontrollen verpflichten. Teilweise wird eine entsprechende Einwilligung direkt bei Abschluss des Arbeitsvertrags eingefordert - insbesondere in Call-Centern bezüglich des Mithörens von Telefongesprächen, teilweise erst später im Verlauf des Arbeitsverhältnisses - etwa in einem großen deutschen Unternehmen bezüglich des umfassenden Datentransfers in ein datenschutzfreies Drittland.

Der Umgang mit individuellen Einwilligungen ist in diesem Zusammenhang kritisch zu bewerten. Geht es doch schließlich um die Aufgabe von individuellen Grundrechten. Grundsätzlich spricht zwar nichts dagegen, dass im Rahmen eines Arbeitsverhältnisses auf Grundrechte verzichtet werden darf, und dass Arbeitnehmer in Kontrollmaßnahmen des Arbeitgebers einwilligen können. Allerdings muss ein solcher Verzicht, damit er aus verfassungsrechtlicher Sicht Wirkung entfalten kann, aus freien Stücken und ohne Zwang erfolgen.

Diese verfassungsrechtlich begründeten Anforderungen an die Freiwilligkeit wurden in der aktuellen Fassung des BDSG abgebildet. Eine nach § 4 Abs. 1 BDSG mögliche Einwilligung in Überwachungs- und Kontrollmaßnahmen des Arbeitgebers ist gemäß § 4a Abs. 1 BDSG nur dann wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht.

Wann eine *freie Entscheidung* vorliegt, hat das Bundesverfassungsgericht 1981 in seiner sog. „Lügendetektorentscheidung" festgestellt.[7] Freiwilligkeit ist nur dann anzunehmen, wenn eine Entscheidung nicht unter Druck oder in einer Zwangslage getroffen wird. Diese Voraussetzung wird gerade im Arbeitsverhältnis regelmäßig nicht vorliegen. Dazu ist das Macht- und Kräfteverhältnis zwischen Arbeitgebern und Arbeitnehmern zu ungleich - gerade auch vor dem Hintergrund einer hohen Arbeitslosigkeit: Wer etwa die bei Vertragsabschluss geforderte Einwilligung nicht erteilt, wird nach der allgemeinen Lebenserfahrung gar nicht erst eingestellt. Wer sie während des Verlaufs des Arbeitsverhältnisses nicht erteilt oder eine erteilte Einwilligung zurücknimmt, wird zum EDEKA-Mitarbeiter (= **E**nde **de**r **Ka**rriere).

An die Wirksamkeit einer *freiwilligen Entscheidung* als Voraussetzung für umfassende Leistungs- und Verhaltenskontrollen sowie für Inhaltskontrollen von E-Mails sind damit hohe Anforderungen zu stellen. Ihr Vorliegen wird im Arbeitsverhältnis aufgrund der zumeist bestehenden Drucksituation die Ausnahme bleiben. Im Streitfall wird der Arbeitgeber nach allgemeinen zivilrechtlichen Beweisregeln („wer etwas will, muss seinen Anspruch substantiiert darlegen") den Nachweis erbringen müssen, dass die Voraussetzungen der Freiwilligkeit ausnahmsweise vorgelegen haben. Kann er dies nicht, darf er die illegal erhobenen Verhaltens- und Leistungsdaten nicht verwenden (etwa zur Begründung einer Kündigung).

Zulässigkeit von Inhaltskontrollen - ein enger Rahmen

Fasst man diese juristischen Ausführungen zusammen, ergibt sich ein relativ klares Bild: Arbeitgebern ist zwar grundsätzlich das Recht zuzugestehen, die Arbeitserbringung ihrer Mitarbeiter zu kontrollieren. Dies bedeutet aber nicht zugleich, dass sie Kontrollformen wählen dürfen, die in Persönlichkeitsrechte der Beschäftigten eingreifen. Insbesondere die Zulässigkeit der Auswertung der in IT-Systemen vorhandener Leistungs- und Verhaltensdaten hat enge Grenzen. Will der Arbeitgeber seine Beschäftigten anhand dieser Daten kontrollieren und stehen ihm tatsächlich keine anderen, weniger grundrechtsschädlichen Möglichkeiten zur Verfügung, muss er dies offen tun. Umfassende Persönlichkeitsprofile darf der Arbeitgeber dabei ebenso wenig erzeugen wie die E-Mails seiner Beschäftigten lesen oder deren Internet-Aktivitäten detailliert verfolgen.

Soweit entsprechende Kontrollmaßnahmen als Ergebnis einer verfassungsrechtlich orientierten Rechtsgüterabwägung ausnahmsweise überhaupt zulässig sind (etwa für E-Mail-Kontakte von Mitarbeitern einer geheimen Forschungsabteilung), müssen sie konkret für den Einzelfall und nicht nur abstrakt zu Beginn des Arbeitsverhältnisses angekündigt werden. Dies bedeutet aber in der Umkehrung, dass das standardisierte Mitlesen des E-Mail-Verkehrs, das Scannen auf bestimmte Suchworte oder die Protokollierung und personenbezogene Auswertung des Internet-Verkehrs im Regelfall selbst dann unzulässig sind, wenn die private Nutzung verboten wird. Dies ergibt sich aus der Überlegung, dass es auch im Rahmen der ausschließlich betrieblichen oder dienstlichen Nutzung Bereiche persönlicher Kommunikation gibt, die datenschutzrechtlich besonders geschützt ist. Hierzu zählen mit Blick auf § 3 Abs. 9 BDSG beispielsweise

Prof. Dr. Peter Wedde

Dr. Peter Wedde ist Professor für Arbeitsrecht und Recht der Informationsgesellschaft an der Fachhochschule Frankfurt am Main, seit 1999 behördlicher Datenschutzbeauftragter der Fachhochschule und seit 2001 ehrenamtlicher Richter am Arbeitsgericht Frankfurt.

herausragend geschützte besondere Daten, wie sie etwa beim dienstliche Kontakt zur Gewerkschaft und zum Betriebsrat, zum Betriebsarzt oder zum Betriebspsychologen, zur Frauenbeauftragten oder zum Ausländerbeauftragten usw. anfallen. Darüber hinaus unterliegen auch vertrauliche und persönliche Kontakte zur Personalabteilung im Zusammenhang mit einer gewollten Versetzung einem besonderen Vertrauensschutz, der einer Kenntnisnahme der Inhalte von E-Mails durch Vorgesetzte entgegensteht.

Die Macht über die Kommunikation

Aus den vorstehenden juristischen Ausführungen lässt sich unschwer ableiten, dass die Debatte um Kontrollen im Arbeitsverhältnis trotz der juristisch weitgehend eindeutigen Situation erst am Anfang steht. Diese Aussage gilt ausdrücklich auch vor dem Hintergrund, dass in einer Reihe von Unternehmen für den Umgang mit personenbezogenen Daten, die im Bereich E-Mail/Internet sowie bei neuen umfassenden Kommunikationsoberflächen anfallen, sinnvolle und ausgewogene Regeln existieren, die auf Kontrollen verzichten oder diese auf ein Minimum begrenzen. Fragt man hier nach, erhält man von Arbeitgebern die Auskunft, dass mit dem Verzicht ein positiver Umgang mit den neuen Medien gefördert werden soll. Die weitere Begründungslinie ist einfach: Wer keine Angst hat, dass ihm aus seinem persönlichen Umgang mit IT-Systemen Nachteile erwachsen, der wird unbefangen alle Vorzüge erproben und benutzen. Wer hingegen fürchten muss, dass ein falscher Tastendruck arbeitsrechtliche Konsequenzen nach sich zieht, wird den Umgang mit den IT-Systemen auf das Notwendigste beschränken.

Nun ist es aber ja nicht so, dass die Protagonisten von *mehr Kontrolle im Betrieb* diese Argumente nicht kennen. Auch sie würden wahrscheinlich sogar zugestehen, dass sie sich im Zeitalter von preisgünstigen *Unternehmens-Flaterates* und von *Vertrauensarbeitszeit* keine ernsthafte Sorge machen müssen, dass ihre Arbeitnehmer sie mit dem gelegentlichen Schreiben oder Empfangen privater E-Mails oder dem privaten Surfen im Internet während der Arbeitszeit betriebswirtschaftlich schädigen. Gerade weil dies eine nicht zu übersehende Tatsache ist, liegt der Verdacht nah, dass es in Wirklichkeit um etwas ganz anderes geht: Die Macht über die Kommunikation.

Könnte es sein, dass es den Arbeitgebern, die mehr Verhaltens- und Leistungskontrollen fordern, eigentlich nur darum geht, die Vorzüge, die sich mit modernen IT-Systemen und mit ihren interaktiven Kommunikationsmöglichkeiten verbinden, ausschließlich für ihre Interessen optimal nutzen wollen? Den Beschäftigten und deren Interessenvertretern soll hingegen genau dieses Potenzial verschlossen bleiben. Wenn dieser Verdacht zutrifft – und hierfür spricht, dass es Rechtsstreitigkeiten über die Nutzung von IT-Systemen durch Betriebsräte schon seit fast zwanzig Jahren gibt – dann wird die Intensität der von einzelnen Arbeitgebern geführten Debatte plausibel. Wo kämen wir da auch hin, wenn Arbeitnehmer das ihnen entgegen gebrachte *Arbeitszeitvertrauen* dazu nutzen würden, in ihrer freien Zeit über die betrieblichen IT-Systeme einen Austausch mit Kolleginnen und Kollegen zu beginnen und über unterschiedliche Arbeitsbedingungen zu reden…?

Der Verdacht, dass es nur vordergründig um den Arbeitszeitaufwand für private Interessen geht, wird durch ein weiteres Indiz gestützt: In dem im Anfangsbeispiel angesprochenen Konzern wurde inzwischen zwar mit Duldung des Betriebsrats die einheitliche Internet-Oberfläche mit vielfältigen Einzelanwendungen wie Termin-, Aufgaben und Dokumentenmanagement, *Schwarzen Brettern*, *Chat*-Gruppen usw. konzernweit eingeführt - einschließlich des dem System innewohnenden immensen Kontrollpotenzials. Der Arbeitgeber hat aber seinerseits dem Konzernbetriebsrat ohne nähere Begründung erklärt, dass die kollektiven Interessenvertreter das System für ihre Arbeit nicht nutzen dürfen.

Aus dem juristischen Blickwinkel ist diese Aussage mit Blick auf § 40 BetrVG zwar eindeutig als Wunschrecht und nicht als Arbeitsrecht zu qualifizieren. Steht der Zugriff auf im Betrieb eingeführte Systeme dem Betriebrat doch nach der ständigen Rechtsprechung des zuständigen 7. Senats des Bundesarbeitsgerichts nach eigener Entscheidung eigenständig zu.[8] Die Position des Arbeitgebers ist aber ein deutliches Signal dafür, dass eine Verbesserung der Arbeitsbedingungen von Betriebsräten gerade *nicht* gewollt ist.

Fazit

Im Ergebnis bleibt zu hoffen, dass Entscheidungen der Arbeitsgerichte und das längst überfällige Arbeitnehmerdatenschutzgesetz das Thema „Verhaltens- und Leistungskontrolle in der Internet-Welt" bald umfassend zu Gunsten des Grundrechtsschutzes der Arbeitnehmer klären. Bis dahin bleibt nur die Hoffnung, dass mehr Arbeitgeber zu der Erkenntnis gelangen, dass eine Abkehr vom restriktiven Kontrollkurs ihren Unternehmen selbst unmittelbar zugute käme: Nur wenn nämlich Arbeitnehmer keine Angst mehr vor übermäßigen oder heimlichen Verhaltens- und Leistungskontrollen haben müssen, werden sie bereit sein, mit ihren Arbeitgebern gemeinsam die Vorzüge der neuen IT-Welt zu erschließen - etwa im Bereich des Wissensmanagements.

Den Arbeitgeber, die bisher mehr und umfassendere Verhaltens- und Leistungskontrollen fordern, ist vor diesem Hintergrund anzuraten, sich schnell vom antiquierten Denken zu verabschieden und stattdessen eine neue Formel für den Umgang mit ihren Arbeitnehmern zu lernen:[1] „Kontrolle ist out - Vertrauen hat Zukunft!"

1 *Vgl. Wedde, Auf dem Weg zu einem Arbeitnehmerdatenschutzgesetz, in: Sommer/Brandt/Schröder (Hrsg.), Im Netz@work, Hamburg 2003, S. 42 ff.; Wiegand/Friedel, Der Chef surft mit, elektronisches Dokument, www.onlinerechte-fuer-beschäftigte.de.*

2 *Vgl. zur aktuellen Situation Wedde, a.a.O, S. 43.*

3 *Vgl. ArbG Frankfurt, AiB 2003, 271 mit Anm. Wedde.*

4 *Vgl. etwa BAG v. 7.10.1987, AP Nr. 15 zu § 611 BGB Persönlichkeitsrechte.*

5 *Vgl. insgesamt Hirschberg, Der Grundsatz der Verhältnismäßigkeit, Göttingen 1981; Wiese, ZfA 1971, 273 (283).*

6 *Vgl. BAG v. 19.1.1999, NZA 1999, 547.*

7 *BVerfG v. 18.8.1981, NJW 82, 375.*

8 *Vgl. Wedde in Däubler/Kittner/Klebe, Betriebsverfassungsgesetz, Kommentar, 8. Aufl. Frankfurt 2002, § 40 Rn. 97 ff.*

Sabine Pfeiffer

SAP R/3 & Co.

Integrierte Betriebswirtschaftliche Systeme als stille Helferlein des Lego-Kapitalismus

„Submit and Pray" *ist eine von unzähligen, meist spöttischen Nachbildungen des Firmenkürzels SAP, die im Internet ausgetauscht werden. Der Spott richtet sich meist gegen die veraltete Architektur und Philosophie* („Senil, alt, prähistorisch"), *die hierarchische Struktur oder die Trägheit des Systems* („Sanduhr-Anzeige-Programm"). *Nun gibt es in der Technikgeschichte genügend populäre Beispiele für den offensichtlich nicht monokausalen Zusammenhang zwischen der – wie auch immer zu definierenden – Güte einer Technik und ihrem Diffusionserfolg bzw. -misserfolg.*

Der Diffusionserfolg von SAP allerdings ist so unbestritten wie beeindruckend: Die Anzahl der Installationen weltweit wird auf über 20.000 geschätzt und allein in Deutschland setzen 80 der 100 größten Firmen SAP im Produktivbetrieb ein (Trittmann u.a. 2000). Die Erfolgsstory von SAP verlief kometenhaft: Seit der Gründung 1972 mit anfangs neun Mitarbeiterinnen und Mitarbeitern hat sich das Unternehmen mit einem durchschnittlichen jährlichen Umsatzwachstum von 44 Prozent zum Weltmarktführer auf dem Gebiet betriebswirtschaftlicher Anwendungssoftware entwickelt (Meissner 2001). Der Marktanteil in Deutschland lag 1999 bei 55 Prozent, der nächstgrößte Konkurrent kann nur einen Marktanteil im einstelligen Bereich vorweisen (IT.Services 07/2000). Trotz dieser hegemonialen Marktstellung ist SAP nur das prominenteste Beispiel für eine bestimmte Art von Softwaresystemen, die als Integrierte Betriebswirtschaftliche Systeme (IBS) bezeichnet werden können – versuchen sie doch *alle* Unternehmensprozesse in betriebswirtschaftliche Logik gemäß unterstellter best-way-Lösungen zu integrieren. Es geht hier also nicht um das Unternehmen oder das Produkt SAP, sondern vielmehr um den Erfolg einer bestimmten IT-vermittelten Logik.

IBS, das soll nachfolgend gezeigt werden, stehen in besonderem Maße für ein Ineinanderfallen von ökonomischer Logik und technischer Repräsentation. SAP und Co. sind in diesem Sinne symptomatische Prototypen für einen vorläufigen Höhepunkt des historischen Prozesses der Informatisierung. Sie verleihen der kapitalistischen Verwertungsperspektive eine Repräsentationsmacht, wie sie Managementsysteme (Kennzahlensteuerung, Zielvereinbarung etc.) ohne diese Flankierung durch scheinbar neutrale, technische Systeme kaum erzeugen könnten. Diese These lässt sich mit den innerbetrieblichen Auswirkungen belegen: Die betriebswirtschaftliche Ausrichtung und das Paradigma eines *one best way*, wie sie für alle IBS charakteristisch sind, gehen mit einer bisher unbekannten enormen Abstrahierung von realen betrieblichen Prozessen einher. In einem zweiten Schritt wird diese These anhand aktueller überbetrieblicher Prozesse und globaler ökonomischer Entwicklungen untermauert: Der Erfolg von SAP und Co. erklärt sich aus ihrer logischen Kongruenz mit den ökonomischen Entwicklungen, die mit Hilfe von IBS von den globalen Finanzströmen bis hinein in kleinste betriebliche Einheiten wirken. Mit ihrer Öffnung hin zu webbasierten und Plattform-unabhängigen Systemen sowie offenen Schnittstellen läuten SAP und Co. nicht nur einen neuen Trend in der Informatisierung von Arbeit ein, sondern verstärken und erleichtern als stille Helferlein die Ausbreitung des Lego-Kapitalismus.

IBS als symptomatischer Prototyp von Informatisierung

Die Soziologie verstand in Unternehmen eingesetzte Informationstechnologien traditionell vor allem als Organisationstechnologien (Benz-Overhage u.a. 1981). Eine Erklärung, über welches Scharnier der unterstellte Zusammenhang vermittelt wird, lieferte schlüssig jedoch erst das Konzept der Informatisierung von Arbeit (Schmiede 1996): Informatisierung als Durchsetzungsinstanz und Reproduktionsmechanismus kapitalistischer Verwertungslogik ist demnach ein historischer Prozess, in welchem die gesellschaftliche Dominanz des Kapitals in Form der Informationstechnologien eine materiale Gestalt annimmt. Informationssysteme werden damit zu einem wesentlichen Vermittlungsglied zwischen „dem anonymen Imperativ der Kapitalverwertung" und den realen Produktionsprozessen (ebd., S. 43). Nicht die Informatisierung ist das Ergebnis der Potenziale heutiger Informationstechnologien, sondern umgekehrt sind diese selbst eingebettet in einen historischen Prozess der Erzeugung und Nutzung von Informationen – beginnend mit der Buchführung seit dem 13. Jahrhundert bis hin zur wissenschaftlichen Betriebsführung des Taylorismus (Baukrowitz u.a. 2001). Dabei hat schon immer die Abstraktion vom Gebrauchswert der Ware und die Reduktion auf ihren in den Büchern abgebildeten Wert eine zentrale Rolle gespielt. In Kopplung mit den Potenzialen heutiger Informationstechnologien erreicht dieser Prozess eine neue Qualität, es kommt zu einer neuen Dimension der „Herrschaft des Formellen", bei der die Informationstechnik selbst die Rolle einer „Verkörperung der Herrschaft der Form" übernimmt (Schmiede 1996, S. 27 ff.).

Auch wenn das Konzept der Informatisierung gerade im Hinblick auf seine verkürzende Gleichsetzung von ökonomischen Abstraktifizierungs- und konkreten Abstrahierungsprozessen einer kritischen Erweiterung bedarf (Pfeiffer 2003), liegt sein Charme unbestritten in der historischen Perspektive und dem Sichtbarmachen der strukturellen und immanenten Verschränkung von Informatisierung und kapitalistischen Verwertungs-

strukturen und -logiken. IBS sind das bislang eindeutigste und umfassendste Phänomen dieser Verschränkung. So beziehen sich die offensiv vermarkteten Nutzeneffekte von SAP und Co. in erster Linie auf die Optimierung des Geschäftsprozess-Managements und damit vor allem auf kürzere Durchlaufzeiten und die Verbesserung von Planung, Steuerung und Kontrolle. IBS sind nicht nur wegen ihrer betriebswirtschaftlichen Ausrichtung als symptomatischer Prototyp von Informatisierung zu deuten. Bei ihnen ist die Herrschaft von Wert über Produkt, von abstraktem Abbild über Prozess und von Tausch- über Gebrauchswert beabsichtigt. Betriebliche Abläufe werden ex ante im Sinne eines *best way* aus rein betriebswirtschaftlicher Perspektive definiert und dieser abstrakten Vorgabe wird die betriebliche Wirklichkeit so lange angenähert, bis sie passgenau an die Logik der Systeme angedockt werden kann. Die hierarchische Architektur und die Komplexität der Systeme tun ein Übriges: Im Bestreben, den Pflege- und Update-Aufwand zu minimieren, wird die Dominanz des *best way* über die realen Erfordernisse noch verstärkt und oft über Jahre hinweg zementiert. Der Prozess des *Customizing* ist also als Anpassung der Realprozesse des Unternehmens an die Logik des Systems zu interpretieren und weniger als Anpassung der Software an die konkreten Unternehmenserfordernisse. Von diesem selten bruchlos verlaufenden Abstraktionsprozess lebt zu einem nicht unerheblichen Teil eine ganze Gilde von Consultants. So wurden im Jahre 1995 allein in Deutschland 1,2 Milliarden DM für SAP-bezogene Dienstleistungen ausgegeben (Meissner 2001). Die informationstechnisch vermittelte betriebswirtschaftliche Logik, wie IBS sie repräsentieren, hat nicht nur innerbetrieblich eine mehrdimensional prägende Wirkung, sondern erklärt sich als Erfolgsmodell nur im Rahmen jüngster Informatisierungstrends und aktueller global-ökonomischer Strategien. Dies soll nachfolgend skizziert werden.

Die Standardisierung des Realen und die Folgen

Nicht nur der beeindruckende Verbreitungsgrad rechtfertigt einen kritischen Blick auf IBS, sondern vor allem ihre Zugriffsintensität auf die Gestaltung organisatorischer Abläufe und betrieblicher Prozesse. SAP ist ein funktionales System mit einem hierarchischen Datenmodell nach dem *Top-down-Prinzip.* Sein erklärter Anspruch ist es, Abläufe weitestgehend zu automatisieren und Verlässlichkeit dadurch zu garantieren, dass Eingabeformen und -abfolgen den Benutzern zwanghaft bis ins Letzte vorgeschrieben werden können (Schmitz 1995). Damit wird die organisatorische Vorgabe und Standardisierung von Prozessen auf einer neuen Stufe der Informatisierung weiter geführt, mit dem Ziel transparente und prognostizierbare Abläufe (Altmann, Bechtle 1971) zu schaffen. IBS erlauben Kontrolle schon aus ihren Strukturen heraus: Je differenzierter und detaillierter sie aufgebaut sind, umso mehr überwachungsgeeignete Betriebsdaten fallen an. Wegen der hohen Integriertheit der Systeme sind diese Daten nicht auf den Ort ihrer Entstehung begrenzt, sondern nahezu überall zugänglich und bei Realtime-Zugriff (z.B. bei SAP seit dem Sprung von R/2 auf R/3) zeitnah abrufbar.

Als informationstechnologisch vermittelte Standardisierungsinstanz prägen IBS den jeweiligen Anwendungskontext und die in ihm Agierenden in einem bislang ungekannten Ausmaß nach dem Muster der durch diese Systeme repräsentierten betriebswirtschaftlichen Logik. Ihre Logik und damit auch die Struktur der Softwaremodule – bis in die Gestaltung der *User Interfaces* hinein – orientiert sich am eigentlichen Zweck der Systeme: der zentralen Lenkung, Transparenz und Steuerung von Unternehmen, weitgehend abstrahiert von stofflichen und realen Erfordernissen und reduziert auf betriebswirtschaftliche Kenngrößen, Bewertungs- und Entscheidungskriterien. IBS sind keine *Arbeits*-Support-Systeme sondern *Management*-Support-Systeme – sie fordern den Beschäftigten auf der operativen Geschäftsebene mehr ab als sie ihnen nützen. So kommt es durch einen gesteigerten Datenpflegeaufwand bei qualifizierten Fachkräften oft zu einem zusätzlichen, aber nicht explizierten Arbeitsanfall, der weder bei der Formulierung von Stellenbeschreibungen noch bei Projektplanungszeiten eine Rolle spielt. Dies führt auf der Seite (hoch-)qualifizierter Fachkräfte zu einer oft erheblichen Leistungsverdichtung *durch die Hintertür*, auf der Seite weniger qualifizierter administrativer Beschäftigter zu Rationalisierung: So kann die Implementierung von IBS nach der Einführungsphase Personalabbau in Größenordnungen von 20-30% nach sich ziehen (Doleschal 1998, S. 24) und Bürohilfskräfte werden bei Einführung von SAP schnell zur *bedrohten Art* (AFOS 1996).

Nicht nur die operativen Geschäftsebenen sind betroffen. Schon wenn es um die Ausweitung und Relevanz von integrierten Standardsoftwarepaketen in Zusammenhang mit entsprechender Hardware und Client/Server-Strukturen geht sowie die Verbindung zu Software für *MRP (Manufacturing Resource Planning)* und *ERP (Enterprise Resource Planning)*, wird festgestellt:

> *„Die Freiheitsgrade menschlicher Entscheidungen und menschlichen Handelns schrumpfen in dem Maße, wie DV-Systeme das betriebliche Geschehen bestimmen. Was bisher noch in der Hand der unmittelbaren Vorgesetzten lag, wenn es um Auftragsabwicklung oder um Personalstärke ging, wird nunmehr von Systemen erledigt" (Doleschal 1998, S. 24).*

Diese Tendenz wird durch IBS auf die Spitze getrieben. SAP und Co. fungieren nicht nur als Management-Support-Systeme, sondern zunehmend als ein Management-Substitut – sie entheben partiell selbst den Manager zunehmend seiner gesellschaftlich zugestandenen Entscheiderrolle: Führen und Entscheiden *gegen* die Zahlen des Systems wird stark legitimierungsbedürftig, wenn nicht undenkbar; Führen und Entscheiden *entlang* der vom System generierten Zahlen wird zunehmend zu einem kaum hinterfragbaren Automatismus.

Die Symbiose von IBS und Internet: Bedingung und Folge der kapitalistischen Lego-Logik

Der vorherrschende Blick der Industriesoziologie – gerade auch was die Bewertung der Folgen informatisierter Technik betrifft – war lange Zeit auf den Betrieb als System fokussiert, als Einzelkapital mit autonomen Interessen. Der *Betriebsansatz* (Altmann, Bechtle 1971; Bechtle 1980) deutete *Betrieb* als organisierte Herrschaft und als Bewältigungsstrategie des Kapitals angesichts der gesellschaftlichen Grundprobleme von

- Macht (Reproduktion der asymmetrischen Machtverhältnisse von Kapital und Arbeit),
- Markt (erweiterte Vermarktung bei wachsender Produktivität)

- und Konkurrenz (Absatz auf konkurrierenden Märkten).

In diesem Zusammenhang wurden auch Technisierung und Organisierung als betriebliche Strategien zur Beherrschung des unmittelbaren Produktionsprozesses verstanden.

Nun ist der Kapitalismus aber jüngst in einer neuen Qualität global geworden. Ob globales Empire (Hardt, Negri 2002), informationeller Kapitalismus (Lash 2002) oder Netzwerkgesellschaft (Castells 2001): Die Dynamik globaler Finanzströme einerseits und moderner Informationstechnologien andererseits scheint die Bedeutung des Nationalstaats ebenso zu untergraben wie die des Einzelbetriebs. Mit dieser Entwicklung verliert jedoch weder der Betrieb seine strategische Bedeutung zur Beherrschung der unmittelbaren, also der Mehrwertproduktion, noch lösen sich die Koordinaten von Macht, Markt und Konkurrenz in einer unbestimmbaren virtuellen Weltgesellschaft auf – im Gegenteil: Macht, Markt und Konkurrenz bekommen eine verstärkte globale Bedeutung und müssen nun auch global bewältigt werden. Zum Betrieb als Herrschaft über den unmittelbaren Produktionsprozess und damit über die Mehrwert*produktion* kommt nun (additiv, nicht substitutiv) das Netzwerk als Strategie der Herrschaft über den Zirkulations- bzw. Verwertungsprozess und damit über die Mehrwert*realisierung* hinzu. Diese Prozesse sind Phänomene spezifischer ökonomischer Veränderungen wie des von Marx prognostizierten tendenziellen Falls der Profitrate und äußern sich u.a. auch in der steigenden Bedeutung lebendiger Arbeit für die Verwertung gegenüber ihrer abnehmenden Bedeutung für den unmittelbaren Produktionsprozess. Die Strategie einer zunehmend globalen Beherrschung von Macht, Markt und Konkurrenz findet ihren empirischen Ausdruck u.a. in einer zunehmenden Automatisierung von Finanzprozessen. *Online Analytical Processing (OLAP)* oder *Business Intelligence* sind nur zwei Stichworte, die für Konzepte einer strategischen Integration von eBusiness und Finanzwesen stehen. Traditionelle, an materiellen Gütern orientierte Controlling-Konzepte werden zunehmend durch Strategien abgelöst, die *Shareholder Value*, Kundennutzen und den Realoptionswert (aktiver Unternehmenswert, der zukünftige Entwicklungen zu fassen sucht) in die Finanzmanagementprozesse des Unternehmens einbinden. Der *CFO (Chief Financial Officer)* braucht zunehmend widerspruchsfreie und global durchgängige Zahlen. Dafür müssen – so die Empfehlung einer SAP-Publikation (SAP 2002) – die Bedürfnisse lokaler Gegebenheiten bei der Auswahl neuer Prozesse und Tools eben zurückstehen.

Es handelt sich hier also um eine ökonomie- und nicht um eine technikgetriebene Entwicklung, bei der jedoch Informationstechnologien und insbesondere IBS eine spezifische Rolle spielen. Die Diffusion von IBS über ganze Wertschöpfungsketten und nationale Grenzen hinweg ist einerseits die Folge und schafft andererseits die stoffliche Grundlage für das, was als *Lego-Logik* der kapitalistischen Netzwerkgesellschaft bezeichnet werden kann. Im Zuge der Shareholder-Value-Orientierung wird das Outsourcing und Filettieren von Unternehmensbereichen und das Fusionieren und Übernehmen von Unternehmen zum Alltag. *Mergers and Acquisitions* sind selbst zur Quelle des Profits geworden und liegen – auch wenn die Zahlen gegenüber den Ausnahmewerten von 2001 heute als rückläufig gelten – nach einer Studie der Wirtschaftsprüfungsgesellschaft KPMG mit über 7.300 globalen Unternehmenstransaktionen und einem Volumen von 464 Milliarden US$ allein im ersten Halbjahr 2003 in einer Schwindel erregenden Höhe (Financial Times Deutschland, 30.06.2003). Und es sind IBS mit ihrer betriebswirtschaftlichen Ausrichtung und ihrem Primat des *best way*, die es zusehends erleichtern, Unternehmenseinheiten wie Legosteine beliebig auseinander zu nehmen, neu zu schneiden und wieder zu gruppieren. Die Rolle von IBS ist dabei nicht nur, die Gleichheit der Schnittstellen (der Lego-Steckverbindungen) herzustellen, sondern gleichzeitig spezifische Methoden (des Lego-Bauens, der Lego-Architektur) normierend zu verbreiten. Zudem lassen sich An- und Zukäufe von Unternehmen, Übernahmen und Fusionen leichter und damit kostengünstiger abwickeln, wenn die einzelnen Elemente der neu zu konfigurierenden Unternehmenseinheiten kompatibel zueinander sind. Mit Kompatibilität sind dabei nicht nur kompatible IT-Strukturen oder die diese Kompatibilität gewährleistenden technischen Schnittstellen angesprochen, sondern auch die Kompatibilität der jeweiligen Unternehmensabläufe, Geschäftsprozesse und organisatorischen Strukturen selbst. Auch deren möglichst reibungsloses Ineinandergreifen wird wesentlich erleichtert, wenn sie dank IBS schon vor dem Merging nach einem einheitlichen *best way* strukturiert waren. Die Fragen, welches IBS bei den neu zu fusionierenden Unternehmen eingesetzt wird und welche Kosten durch die Anpassung eventuell inkompatibler Systeme entstehen, spielen daher auch eine nicht unbedeutende Rolle in der Kalkulation von *Mergers and Acquisitions*-Prozessen. Ja mehr noch: Der ganze Prozess von Firmenzusammenschlüssen selbst wird wiederum durch IBS abgebildet, um ihn kalkulier-, plan- und steuerbar zu machen. So bietet SAP seit kurzem das Modul „SAP xApp MA" an, das „speziell für Unternehmen entworfen [wurde], die andere Unternehmen aufkaufen wollen" und das „Methoden, Technologien und Services [...] für die Durchführung von Fusionen oder Übernahmen" bietet – so zumindest die vollmundigen Ankündigungen der Marketingabteilung[1].

Vor dem Hintergrund der weltweiten Verbreitung webbasierter, Plattform-unabhängiger Technologien zeichnen sich derzeit drei – durchaus widersprüchlich, ungleichzeitig und in unterschiedlicher Dynamik verlaufende – *neue Trends in der Informatisierung von Arbeit* ab (Pfeiffer 2001). Neben der *Virtualisierung des*

Sabine Pfeiffer

Sabine Pfeiffer, Soz. (M.A.) studierte nach mehrjähriger Tätigkeit als Werkzeugmacherin und im technischen Support (CNC und CAD/CAM) Soziologie, Philosophie und Psychologie. Im Rahmen ihrer wissenschaftlichen Forschungstätigkeit am *ISF Institut für Sozialwissenschaftliche Forschung e.V.* beschäftigt sie sich mit soziologischen Auswirkungen neuer Trends in der Informatisierung von Arbeit – derzeit mit dem Schwerpunkt auf agentenbasierten Systemen, Multimedia-Technologien, Open Source und Teleservice.

Arbeitsvermögens (z.B. durch neue Metaphern bei Nutzungsoberflächen und agentenbasierte Softwarearchitekturen) und der *Mediatisierung der Arbeitskraft* (z.B. durch *Tracking, Profiling* und *Online Recruiting)* kann von einer qualitativ neuen Stufe der Verschränkung von Organisation und Informationstechnologien gesprochen werden. Diese *Technologisierung der Arbeitsorganisation* vollzieht sich auf der Ebene von IBS in Form einer strategischen Öffnung in Richtung webbasierter Anwendungen und offener Systeme. Das zeigt sich empirisch beispielsweise in den im SAP R/3-Release 3.1 enthaltenen mehr als zwanzig unterschiedlichen Internet-*Szenarien* oder in der offenen Java-basierten Schnittstelle *BAPI (Business Application Programming Interface)* von SAP. Die angestrebte Symbiose dieser Systeme ist gerade angesichts ihrer bekannt hierarchischen Architektur und ihrer bislang prorietären Geschäfts- und Produktphilosphie kaum immanent aus dem Potenzial webbasierter Technologien selbst zu erklären. IBS erfassen damit nicht mehr nur innerbetriebliche Abläufe, sondern zielen in einer bislang unerreichten Zugriffsintensität zunehmend auf die Gestaltung organisatorischer Abläufe auch im Sinne zwischen- und überbetrieblicher Prozesse. Dies zeigt sich besonders augenfällig an den beiden *äußeren Enden* von Unternehmen hinsichtlich ihrer Wertschöpfungsketten, nämlich *eProcurement* (Beschaffung) einerseits und *eService* bzw. *eCRM (Customer Relationship Management)* andererseits – übrigens jeweils mit erstaunlich vergleichbaren Stoßrichtungen und Implementationsproblemen.

IBS machen sich sozusagen ihren Herrn – das Unternehmen – selbst zum Gegenstand, wirken als technisch repräsentierte Charaktermaske. Dass sie dies tun, und dass sie dies zunehmend unhinterfragt und Verwertungsketten übergreifend tun – darin liegt die neue Qualität. Informatisierung überwindet hier die Logik einer „Rationalisierung im Quadrat" (Deutschmann 1989, S. 378), d.h. einer Rationalisierung bereits rationalisierter, objektivierter Strukturen: IBS bilden zunehmend die informatisierte Basis für eine Rationalisierung der bislang *rationalisierenden* Strukturen selbst und damit sozusagen für eine *Rationalisierung hoch drei*. Die Ziele klassischer Rationalisierung werden also erweitert um die Rationalisierung *der* Managementprinzipien und um die Rationalisierung der Art und Weise von Unternehmensinteraktionen und -kooperationen. In der Lego-Logik der kapitalistischen Netzwerkgesellschaft ist der Betrieb nicht mehr der alleinige strategische Herrscher über innerbetriebliche Rationalisierungsprozesse, sondern diese Prozesse werden Objekte einer externen Rationalisierungsstrategie. SAP und Co. fungieren dabei als stille, aber willfährige Helferlein.

Skepsis – Analyse – Politik

Absicht der bisherigen Argumentation war es, die bislang von der Soziologie kaum beachteten IBS in ihren Auswirkungen auf Arbeit, Betrieb und Organisation in einem ersten Entwurf zu skizzieren und den Zusammenhang zwischen dem Erfolg von IBS und globalen Entwicklungen im Finanzwesen aufzuzeigen. SAP und Co. sind ein Phänomen von Informatisierung, das für eine beispiellose Verschränkung von ökonomischem Kalkül und Informationstechnologie steht, aus der sich eine erschreckende Prägungsdominanz der Systeme auf die betriebliche Organisation, die Beschäftigten und das Management ableiten lässt. Diese Prägungsdominanz ist allerdings nicht im Sinne eines einseitigen Oktroyierens technischer Logik auf Realprozesse zu verstehen – hier soll die Argumentation nicht hinter das von der Industriesoziologie heftig debattierte „Ende des Technikdeterminismus" zurückfallen (Lutz 1987; zu den Debattenverläufen auch Dörner 1989 und Degele 2002). Vielmehr wird auch hier an den schon erwähnten Betriebsansatz angeknüpft, der die Formen von Techniknutzung ebenso wie die Entwicklung industrieller Arbeit als Resultat betrieblicher Rationalisierungsstrategien deutete. Das Beispiel IBS zeigt, dass Techniknutzung darüber hinaus auch als Resultat global-ökonomischer Prozesse zu deuten ist, die wiederum auf die betrieblichen Rationalisierungsstrategien selbst wirken. Keine Entwicklung jedoch verläuft einseitig, ohne innere Widersprüche. Gerade für IBS gilt aufgrund ihrer Logik und Struktur mehr als für andere IT-basierte Systeme, dass sie Produzenten ihrer eigenen Widersprüche sind: Die gewollte Abstraktion von Realprozessen und lokalen Gegebenheiten kann nicht vollständig durchgesetzt werden, ohne zu höchst dysfunktionalen Effekten zu führen. Beim Einsatz von IBS potenzieren sich die neuen Spannungsfelder zwischen zunehmender technologischer Systemisierung und erhöhter Kontingenz (Behr u.a. 1991), zwischen technischer Rationalität und *anderen* Wissensformen, zwischen formaler Organisation und informeller Kooperation (Böhle, Bolte 2002), zwischen Subjektivierung von Arbeit (Moldaschl, Voß 2002) und einer neuen (Selbst-)Objektivierung des Arbeitshandelns (Böhle 2002) sowie zwischen den formalen Regeln der Koordination und den situativen Erfordernissen der Kooperation (Kumbruck 1998). Die Intention der Systeme in Zusammenhang mit global-ökonomischen Prozessen ist relativ klar nachzuzeichnen, ihre Durchsetzungspotenz jedoch ist kein unveränderbar vorgezeichneter Weg: Auch IBS mit hoher Prägungsdominanz wirken weder als monokausal prägender *Akteur* noch als reiner *Erfüllungsgehilfe* der dahinter stehenden Verwertungslogik. Die mit IBS versuchte Standardisierung von betrieblichen Organisationsabläufen und überbetrieblichen Unternehmensbeziehungen vollzieht sich gleichzeitig mit und in Interdependenz zu Prozessen der Entgrenzung tayloristischer Arbeitsorganisation (Bechtle, Sauer 2002; Kratzer 2003) und einer damit einhergehenden zunehmenden Subjektivierung von Arbeit (Moldaschl, Voß 2002).

Die betrieblichen Organisationen ebenso wie die arbeitenden Subjekte bewegen sich somit in einem Spannungsfeld der – informationstechnologisch vermittelten – gegenläufigen Tendenzen von Standardisierung und Präformation einerseits sowie Autonomisierung und Offenheit andererseits. Umso mehr gilt angesichts von SAP und Co. die Devise „Skepsis, Analyse, Politik", d.h. ein skeptischer Blick auf die Entwicklungen ist erforderlich, gekoppelt mit einer umfassenden und kritischen Analyse der Auswirkungen von IBS, um politisch gestaltend und verändernd gegenzuwirken. Hier haben die Techniksoziologie ebenso wie die kritische Informatik, insbesondere aber die Arbeits- und Industriesoziologie erst noch ihre Hausaufgaben zu machen.

1 http://www.sap-ag.de/germany/solutions/xapps/xma/index.asp

Literatur

Altmann, N., Bechtle, G. (1971): Betriebliche Herrschaftsstruktur und industrielle Gesellschaft, Frankfurt/M.

AFOS (Hg.) (1996): SAP Arbeit Management. Durch systematische Arbeitsgestaltung zum Projekterfolg, Wiesbaden

Baukrowitz, A.; Boes, A.; Schmiede, R. (2001): Die Entwicklung von Arbeit aus der Perspektive ihrer Informatisierung. In: Matuschek u.a., 217-235
Bechtle, G. (1980): Betrieb als Strategie. Theoretische Vorarbeiten zu einem industriesoziologischen Konzept, Frankfurt/M.
Bechtle, G.; Sauer, D. (2002): Kapitalismus als Übergang - Heterogenität und Ambivalenz. In: Jahrbuch Arbeit Bildung Kultur, Bd. 19/20, 49-61
Behr, M.; Heidenreich, M.; Schmidt, G.; Schwerin, H.-A. (1991): Neue Technologien in der Industrieverwaltung, Wiesbaden
Benz-Overhage, K.; Brumlop, E.; Freyberg, T.; Papadimitriou, Z. (1981): Computereinsatz und Reorganisation von Produktionsprozessen. In: Leviathan SH4. Opladen, 100-117
Böhle, F. (2002): Vom Objekt zum gespaltenen Subjekt. In: Moldaschl/Voß, 101-133
Böhle, F.; Bolte, A. (2002): Die Entdeckung des Informellen, Frankfurt/M., New York
Castells, M. (2001): Der Aufstieg der Netzwerkgesellschaft, Opladen
Degele, N. (2002): Einführung in die Techniksoziologie, München
Deutschmann, C. (1989): Reflexive Verwissenschaftlichung und kultureller ‚Imperialismus' des Managements. In: Soziale Welt, 40. Jg., H3, 374-396
Doleschal, R. (1998): Die IT-Revolution umfaßt die Unternehmen. In: Die Mitbestimmung, 44. Jg., H12, 23-26
Dörner, C. (1989): Die Hypostasierung des Computers. Soziologische Schriften, Bd. 51, Berlin
Hardt, M.; Negri, A. (2002): Empire. Die neue Weltordnung, Frankfurt/M., New York
Kratzer, N. (2003): Arbeitskraft in Entgrenzung - Grenzenlose Anforderungen, erweiterte Spielräume, begrenzte Ressourcen, Berlin
Kumbruck, C. (1998): Tele-Kooperation und Hintergrundkooperation. In: Spieß, E. (Hg.): Formen der Kooperation: Bedingungen und Perspektiven. Göttingen: Verlag für angewandte Psychologie, S. 231-246
Lash, S. (2002): Critique of Information, London, Thousand Oaks, New Delhi
Lutz, B. (1987): Das Ende des Technikdeterminismus und die Folgen. Soziologische Technikforschung vor neuen Aufgaben und Problemen. In: ders. (Hg.): Technik und sozialer Wandel. Verhandlungen des 23. Deutschen Soziologentages in Hamburg 1986. Frankfurt/M., New York, 34-52
Matuschek, I.; Henninger, A.; Kleemann, F. (Hg.) (2001) : Neue Medien im Arbeitsalltag. Empirische Befunde – Gestaltungskonzepte – Theoretische Perspektiven, Wiesbaden
Meissner, G.: (2001): SAP – die heimliche Software-Macht, München
Moldaschl, M.; Voß, G. G. (Hg.) (2002): Subjektivierung von Arbeit, München, Mering
Pfeiffer, S. (2001): information@WORK. Neue Tendenzen in der Informatisierung von Arbeit und vorläufige Überlegungen zu einer Typologie informatisierter Arbeit. In: Matuschek u.a., 237-255
Pfeiffer, S. (2003): Arbeit und ihr Vermögen. Arbeitsvermögen als Schlüssel zur Analyse von (reflexiver) Informatisierung. Diss. FeU Hagen, Inst. f. Soziologie
SAP (2002): Veränderungen in der Finanzwelt. In: SAP-Info 92 v. 28.02.2002
Schmiede, R. (Hg.) (1996): Virtuelle Arbeitswelten. Arbeit, Produktion und Subjekt in der ‚Informationsgesellschaft', Berlin
Schmitz, K. (1995): Warum die Zukunft von SAP schon aufgehört hat. In: Computerwoche Nr. 7/95 vom 17. Februar 1995, 56
Trittmann, R.; Stelzer, D.; Hierholzer, A.; Mellis, W. (2000): Managing Motivation bei der Softwareentwicklung. Eine Fallstudie in der SAP AG. In: Frey, B. S.; Osterloh, M. (Hg.): Managing Motivation, Wiesbaden, 271-294

Karl-Heinz Brandl

Elektronische Arbeit

Elektronische Arbeit, e-work, *ist die umfassende Beschreibung von zeit- und ortsunabhängiger Arbeit. Betroffen sind Arbeiter und Angestellte der Betriebe ebenso wie* out-gesourcte *Unterauftragnehmer, TelearbeiterInnen, Freelancer, virtuelle Teams sowie virtuelle Unternehmen. Es gilt, in diesen neuen Arbeitsformen Autonomie und Flexibilität mit Sicherheit zu verknüpfen. Die Betrachtung der Telearbeit in diesem Beitrag öffnet uns ein Schaufenster in die mögliche Zukunft des* e-work.

Der Abschlussbericht der Enquete-Kommission des deutschen Bundestages zum Thema „Multimedia" zeigt die Dimension der Veränderung von Arbeit durch neue Techniken auf: „Immer leistungsfähigere informations- und kommunikationstechnische Infrastrukturen erlauben es, weltweit fast ohne Zeitverzögerung, zu geringen Kosten und in stetig verbessernder Qualität zu kommunizieren und arbeitsteilige Leistungsprozesse zu koordinieren. Wenn Koordination zu beliebigen Zeiten von beliebigen Standorten aus erfolgen kann, verlieren auch Arbeitsplätze zunehmend ihre räumliche Bindung. [...] Durch die Möglichkeit einer räumlichen Verteilung von Wertschöpfungsaktivitäten werden aber nicht nur Standortrestriktionen aufgelöst, auch Zeitgrenzen können überwunden werden. [...] Setzt sich dieser Trend fort, dann wird der Betrieb als klassisches Gravitationszentrum der Arbeitswelt erheblich an Bedeutung und prägender Kraft einbüßen."

Was ist e-work – eine Definition

„Viele Begriffe beschreiben eine neue Erscheinungsform von Arbeit: Alternierende, heimbasierte und mobile Telearbeit (teleworking), distant oder remote work (Fernarbeit), Nachbarschafts- oder Satellitenbüros sowie Telearbeitszentren (center-based telework), On-Site-Telearbeit, Outworking. e-work ist eine Arbeitsform, bei der mittels Nutzung von Informations- und Kommunikationstechniken Arbeit zeit- und ortsunabhängig geleistet wird. Als Sammelbegriff entwickelt sich zunehmend der

Begriff e-work für diese Variante des *anytime, anyplace*–Konzeptes (Input 2000).

Diese Definition von e-work umfasst Angestellte der Unternehmen ebenso wie *out-gesourcte* Unterauftragnehmer, schließt somit *klassische* Telearbeiter und Telearbeiterinnen, Freelancer, virtuelle Teams sowie virtuelle Unternehmen ein. (vgl. auch Reichwald 1998)

Die bekannteste Form der elektronischen Arbeit ist Telearbeit. Das Bundeswirtschaftsministerium definierte sie wie folgt: „Telearbeit ist jede auf Informations- und Kommunikationstechniken gestützte Tätigkeit, die ausschließlich oder alternierend an einem außerhalb des Betriebs liegenden Arbeitsplatz verrichtet wird (z. B. Privatwohnung, Nachbarschaftsbüro, Satellitenbüro, Telehaus, mobiler Arbeitsplatz), der mit der zentralen Betriebsstätte durch elektronische Kommunikationsmittel verbunden ist.". Vielfach ist die Telearbeit durch Tarifverträge, Betriebsvereinbarungen und Zusatzverträge zum Arbeitsvertrag schon geregelt. Es wurden Standards zur Einführung und Durchführung von Telearbeitsprojekten entwickelt.

Telearbeit wird inzwischen in Deutschland von einer Vielzahl von Betrieben und Unternehmen durchgeführt. Pionierunternehmen wie Siemens oder IBM verfügten schon zu Beginn der 1980er Jahre über die technische Voraussetzungen zur Telearbeit. Inzwischen spielen die technischen Aspekte keine entscheidende Rolle mehr. Telearbeit findet im Versicherungs- und Bankenbereich, bei Automobilunternehmen, im Logistik- und im Telekommunikationsbereich sowie immer öfter auch in der öffentlichen Verwaltung statt.

Eine repräsentative Studie (vgl. Freudenreich, Klein, Wedde, 1997) stellte fest, dass 1997 rund eine Million Telearbeitsplätze in rund 135.000 Betrieben bestanden (siehe Abbildung 1).

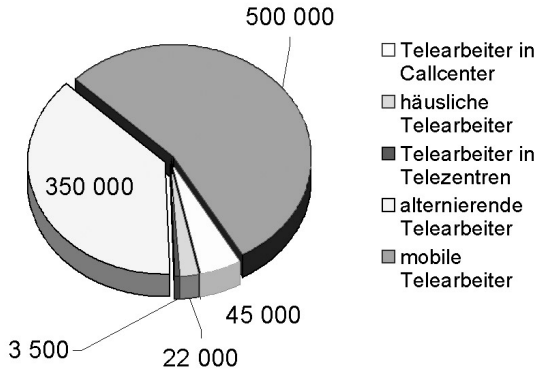


Abbildung 1: Gesellschaftliche Dimension der Telearbeit

Die Abbildung macht nicht nur die Vielfalt von Telearbeit deutlich, sondern zeigt zugleich die Definitionsprobleme. So wird in der Studie von Freudenreich u.a. die Arbeit in in Call Centern sowie in Telezentren ebenfalls als Telearbeit definiert, in der bereits zitierten Definition des Bundeswirtschaftsministeriums gehören sie aber nicht zur Telearbeit.

Die neueste Erhebung - der sogenannte EcaTT-Report (empirica 2000) – stellt fest, dass es 1999 in zehn untersuchten EU-Mitgliedstaaten insgesamt neun Millionen Telearbeitsplätze gibt. In Deutschland werden zwei Millionen Telearbeitsplätze gezählt, das entspricht 6 % der Beschäftigten. Dabei stellt sich heraus, dass vor allem Großbetriebe Telearbeit praktizieren – zwei Drittel der europäischen Großunternehmer bieten regelmäßig Telearbeitsplätze an.

Vor allem die Beschäftigten selbst sind der Telearbeit gegenüber aufgeschlossen: 66 % der arbeitenden Bevölkerung in Deutschland hat Interesse an Telearbeit.

Trotz unterschiedlicher Untersuchungsansätze und Definitionen zeigen die verschiedenen Studien die rasante Weiterentwicklung im Bereich von e-Work, in der Telearbeit die bedeutendste Vertreterin ist. Ein weiteres Sich-Ausbreiten von e-Work-Formen wird die Arbeit generell verändern.

e-Work und die Fixpunkte sozialer Sicherung

Durch die technischen Möglichkeiten und die Anforderungen einer Dienstleistungsorientierung entkoppelt sich Arbeit immer stärker von herkömmlichen Betrieben, sie wird zeitlich flexibler und räumlich mobil (siehe Abbildung 2).

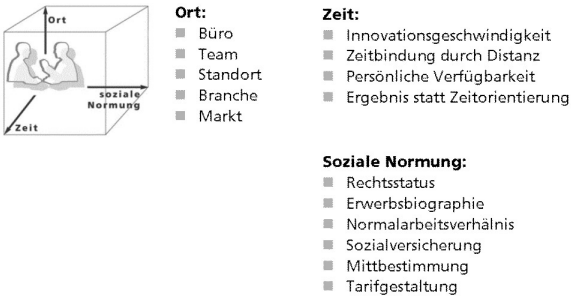


Abbildung 2: Geänderte Bestimmungsfaktoren der Arbeit (1)

Die elektronische Arbeit entfernt sich aus dem Einflussbereich der Betriebe und entzieht sich damit der sozialen Normgebung. Die herkömmlichen Instrumente der sozialen Normung geraten unter Anpassungsdruck:

- Immer mehr Beschäftigte verrichten ihre Tätigkeit außerhalb der Betriebe, beim Kunden, unterwegs in Flugzeugen, Zügen und Autos oder in häuslicher Umgebung;
- Immer häufiger werden Arbeitnehmer-/Arbeitgeberbeziehungen durch Auftragnehmer-/Auftraggeberbeziehungen abgelöst. Herkömmliche Betriebs- und Arbeitnehmerbegriffe sind nicht mehr anwendbar oder Mitbestimmung verflüchtigt sich in virtuellen Betriebsstrukturen. Die Anzahl der freiberuflichen Beschäftigten wächst. Sie verstehen sich häufig als *abhängige Selbständige*, während die im Betrieb beschäftigten Arbeitnehmerinnen und Arbeitnehmer sich durch Zielvereinbarungen und ergebnisorientiertes Arbeiten immer häufiger als *selbständige Abhängige* definieren.
- Je schneller die Wirtschaft versucht, sich auf rasch wechselnde Markttrends einzustellen, desto häufiger werden

virtuelle Teams mittels moderner Kommunikationstechniken über räumliche Entfernungen hinweg flexibel zusammengesetzt. Die unmittelbare zwischenmenschliche Beziehung, der „Teamgeist" wird nicht mehr in dem Maß wie in der Vergangenheit unserer Arbeitswelt prägen.

- Betriebstore verlieren ihre Bedeutung für Streikposten. Standorte werden verändert oder aufgegeben, Branchengrenzen verschwinden. Auf Branchen und auf regional fixierte Betriebe sind aber die heutigen normsetzenden Instrumente der Tarifpolitik von Gewerkschaften und der Mitbestimmung der Betriebsräte ausgerichtet.

- Märkte werden globalisiert. Nach den Finanz- und Gütermärkten werden auch nationale Arbeitsmärkte insbesondere für Informationsarbeit *entgrenzt*.

- Technische Entwicklungen haben in der Geschichte häufig unsere Zeitbeziehungen verändert. Wir können eine derartige Veränderung auch von E-Work-Techniken, z.B. durch die unmittelbare Erreichbarkeit über Handy und Laptop erwarten. Sie werden die ohnehin schon hohen Innovationsgeschwindigkeiten weiter steigern.

- Virtuelle *Schichtbetriebe* über alle Zeitzonen der Erde hinweg sind heute bereits keine Utopie mehr. Die Anforderung an die persönliche und zeitliche Verfügbarkeit von Erwerbstätigen steigt. Eine Ergebnis- löst eine Zeitorientierung in der Arbeitswelt ab.

Für die Zukunft der Arbeitswelt lassen sich verschiedene Szenarien entwerfen. Ein optimistisches Szenarium beschreibt das mit dem Leitbild „Arbeite wo und wann du willst unter deinen Bedingungen". Die pessimistische Betrachtung könnte lauten: „Arbeite immer, wenn du Arbeit bekommst, egal unter welchen Bedingungen" (siehe Abbildung 3).

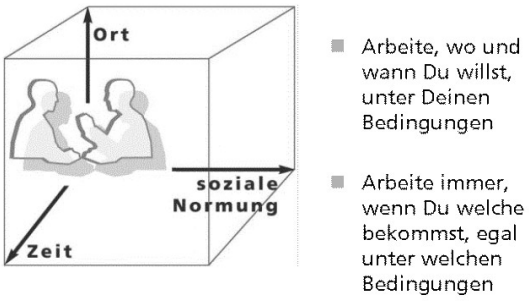


Abbildung 3: Geänderte Bestimmungsfaktoren der Arbeit (2)

Wir brauchen Zukunftsentwürfe, nach denen die Normen der Arbeit in neuen Sphären in der Informationsgesellschaft ausgerichtet werden.

Leitbilder für E-Work

Arbeitnehmerorientierte Leitbilder sollen eine soziale, demokratische und ökologische Informationsgesellschaft gestalten helfen und nicht nur auf Kommerz und Technik ausgerichtet sein. Nach wie vor besteht Bedarf, die arbeitenden Menschen auch in neuen Wirtschaftsbranchen vor existenzieller Not zu schützen und die bewährten Grundrechte zu bewahren, die die Arbeiterbewegung erstritten hat. Ihre Teilhabe am gesellschaftlichen Fortschritt gilt es sicherzustellen, humane Arbeit zu verwirklichen und für soziale Gerechtigkeit und Chancenzuwachs einzutreten.

Teilhabe zu organisieren, bedeutet z.B. für Beschäftigte den realen Nutzen zu erschließen, den die neuen Techniken und Arbeitsprinzipien hervorbringen - beispielsweise im Sinne erweiterter Autonomie zur besseren Vereinbarkeit persönlicher Lebensumstände und beruflicher Pflichten. Viele Regelungen zur alternierenden Telearbeit geben hierzu Gestaltungsbeispiele.

Integration zu organisieren, bedeutet dafür einzutreten, dass keine neue Trennlinie zwischen den Generationen entsteht - zwischen denjenigen, die den Umgang mit moderner Technik von Kindesbeinen an erleben und denjenigen, die den Umgang nicht gewohnt sind.

Die **Chancen** aus der Verbreitung neuer Techniken zu erschließen, bedeutet beispielsweise, Belastungen durch Pendeln abzubauen und Beiträge zum Umweltschutz durch Telearbeit zu leisten. Chancen können dadurch erhöht werden, dass Arbeit zu den Menschen gebracht wird und nicht umgekehrt.

Eher defensiv, aber völlig unabdingbar ist das Leitbild des **Schutzes** der einzelnen Menschen angesichts der Dimension des Veränderungsprozesses. Es gilt, Arbeitnehmerinnen und Arbeitnehmer in ihren sozialen und beruflichen Standards zu schützen. Arbeitsbedingungen müssen so organisiert sein, dass sie den Schutz der Privatsphäre am Arbeitsplatz, der persönlichen Daten wie auch der Gesundheit der Beschäftigten umfassen.

Die Verwirklichung des Leitbilds der **Humanen Arbeit** in der Informationsgesellschaft setzt voraus

- eine sorgfältige und umsichtige Technikfolgenabschätzung,

- keine euphorischen Beschäftigungsprognosen, sondern gezielte Förderung gesellschaftlich nützlicher Produkte und Dienstleistungen zur Schaffung von Arbeitsplätzen,

- neue Impulse für die Debatte um eine Humanisierung der Arbeit,

- zugleich Bemühungen, soziale Gestaltung in jene Bereiche hineinzutragen, in denen Sozialstandards bisher nicht existierten.

Karl-Heinz Brandl

Karl-Heinz Brandl ist Geschäftsführer der ver.di-innotec gGmbH sowie selbstständiger Technologie- und Datenschutzberater für Betriebs- und Personalräte, Experte bei OnForTe, Frankfurt a.M.

Praktische Erfahrungen zur Gestaltung von E-Work gibt es vor allem mit der Telearbeit. Zwei historische Abschnitte kennzeichnen die Erfahrungen:

In den frühen 1980er Jahren stand die noch nicht ausgereifte, kostenintensive Technik einer Ausbreitung der Telearbeit entgegen. Zehn Jahre später waren die technischen Voraussetzungen für Telearbeit günstiger, weil verbesserte und verbilligte Hard- und Software sowie vereinfachte, kostengünstigere und universell verfügbare Übertragungsmöglichkeiten geschaffen worden waren. Darüber hinaus fügte sich diese Arbeitsform optimal ein in neue Organisationskonzepte und komplexe Anwendungszusammenhänge dezentraler Aufgabenerledigung, deren Realisierung in Betrieben und Unternehmen zu diesem Zeitpunkt fortschritt.

Die Telearbeit hat sich mit dem Wegfall der technischen Hemmnisse etabliert, wenn auch anders als in der ersten Phase prognostiziert wurde. Nicht die ausschließliche Tele*heim*arbeit mit nur häuslicher Beschäftigung ist der Regelfall geworden, sondern die Ergänzung betrieblicher und mobiler Tätigkeiten durch alternierende oder mobile Telearbeit. Arbeit außerhalb des Betriebes am häuslichen PC oder am Notebook ist für Beschäftigte zur ständigen Arbeitsform geworden beispielsweise im Vertrieb, in Verkaufs- und Beratungsbereichen und in den Bereichen technischer Kundendienst, Service und Wartung sowie in vielen anderen Berufsfeldern mit hohem Reiseanteil und/oder direkten Kundenkontakten, wie etwa in der Software-Entwicklung.

Die Gestaltung von Telearbeit am Beispiel der Telekom AG

Im Mittelpunkt der Arbeitswelt – im Betrieb – konnten bisher Arbeitszeit- und Arbeitsschutzvorschriften, Mitbestimmungsregelungen, Tarifverträge und andere soziale Normen ein stabiles Gleichgewicht für die unterschiedlichen Interessen von Arbeit und Kapital herstellen. Darauf richten sich die meisten Gestaltungsinstrumente.

Als Beispiel einer sozialen Gestaltung von e-Work soll hier der von ver.di und der Telekom AG abgeschlossene Tarifvertrag zur alternierenden und mobilen Telearbeit dienen. Der seit dem 1.1.1999 geltende Tarifvertrag bestimmt diesen Bereich und wurde in der Praxis erprobt.

Hier die wesentlichen Prinzipien, die mit diesem Tarifvertrag verwirklicht wurden:

- Der Rückgriff auf die häusliche Umgebung folgt dem Prinzip der Freiwilligkeit. Arbeitgeber, Beschäftigte und der zuständige Betriebsrat müssen im Einzelfall zustimmen.

- Es wurde ein Diskriminierungsverbot festgeschrieben. Niemand darf wegen der Aufnahme der Telearbeit oder der Ablehnung dieser Arbeitsform benachteiligt werden.

- Der Arbeitgeber stellt die kompletten Arbeitsmittel kostenfrei zur Verfügung, die für die Telearbeit erforderlich sind.

- Der Arbeitgeber oder von ihm beauftragte Personen, die aufgrund gesetzlicher Verpflichtung Zugang zur häuslichen Arbeitsstätte haben müssen, müssen ihren Besuch vorher mit der Arbeitnehmerin oder dem Arbeitnehmer abstimmen.

- Es ist klargestellt, dass die Bereitstellung geeigneter Mechanismen zum Schutz personenbezogener Daten dem Arbeitgeber obliegt - auch für die häusliche Sphäre.

- Haftungs- und Unfallversicherungsfragen wurden im Tarifvertrag geklärt.

- Wer in alternierende Telearbeit wechselt, muss zuvor mindestens sechs Monate ununterbrochen im Betrieb beschäftigt gewesen sein, damit eine Anbindung an das Unternehmen und das betriebliche Leben gewährleistet ist.

- Der Tarifvertrag enthält zwei Gestaltungsvorgaben zur Arbeitszeitgestaltung, die in jedem Einzelfall vor Ort ausgestaltet werden müssen: Der soziale Kontakt zum Betrieb muss aufrecht erhalten bleiben, und der Anteil der selbstbestimmten Arbeitszeit soll so groß wie möglich gestaltet werden. Es erfolgt eine schriftliche Aufteilung der Arbeitszeit. Die häusliche Arbeitszeit wird aufgeteilt in eine betriebsbestimmte und eine selbstbestimmte Arbeitszeit.

- Bei den im Betrieb zu leistenden Arbeitszeiten wird den Arbeitnehmern ein für die Aufgabenerledigung geeigneter Arbeitsplatz zur Verfügung gestellt.

- Auch Rückkehrrechte in den Betrieb existieren. Die Vereinbarung über die Einrichtung von Telearbeitsplätzen kann mit einer Frist von drei Monaten zum Monatsende ohne Angabe von Gründen widerrufen werden. Ausnahmen bestehen für Fälle der Kündigung der Wohnung, einen Stellenwechsel des Arbeitnehmers oder aus triftigen Gründen für den Arbeitgeber.

Die ver.di-Gründungsgewerkschaft Deutsche Postgewerkschaft hat an einem Punkt einen Quantensprung in den Vereinbarungen zwischen Arbeitgeber und Arbeitnehmer geschafft. Es ist in der Bundesrepublik Deutschland erstmalig gelungen, in einem Tarifvertrag ein elektronisches Zugangsrecht zur gewerkschaftlichen Betreuung von Telearbeitern durchzusetzen. Es gibt ein elektronisches „Schwarzes Brett" der Gewerkschaft beim Telekom-Konzern. Per E-Mail können *Flugblätter* verteilt werden, mit denen auf die Inhalte des „Schwarzes Brettes" aufmerksam gemacht wird.

Damit hat ver.di die Möglichkeit, die verminderten Chancen der Telearbeiter, gewerkschaftliche Informationsangebote in den Betrieben zu nutzen, durch ein elektronisches Medium auszugleichen. In autonomer, inhaltlicher Verantwortung können künftig gewerkschaftliche Informationen im Intranet der Telekom hinterlegt und die Telearbeiterinnen und Telearbeiter darauf hingewiesen werden.

Die Vereinbarung geht zurück auf Anregungen aus der Kampagne der UNI (Union Network International) „Online Rights for Online Workers", die in Deutschland durch ver.di als „Online-Rechte für Online-Beschäftigte" umgesetzt wird und umfasst im Wesentlichen die Sicherstellung des Rechts auf informationelle Selbstbestimmung, den Ausschluss elektronischer Überwachung sowie den Zugang zu Intranets der Unternehmen und zum In-

ternet – inklusive gewerkschaftlicher und betriebsrätlicher Informationen und Angebote (siehe Abbildung 4).

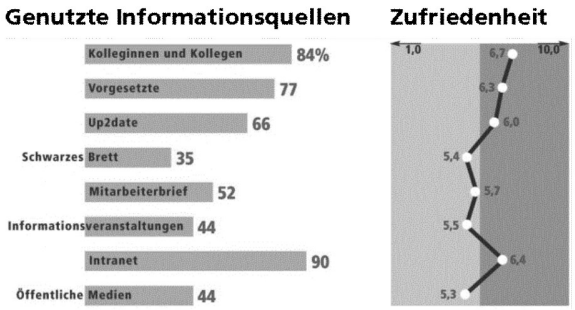


Abbildung 4: Informationsquellen

Wie notwendig dies ist, zeigt eine Befragung in einer Computerfirma über den Umgang mit den neuen Informationsquellen. In dieser *Mitarbeiterbefragung* steht das Intranet an erster Stelle der Informationsquellen – noch vor dem persönlichen Gespräch mit den Kolleginnen und Kollegen. Ein Beleg, wie wichtig es für Gewerkschaften ist, auch elektronisch in den Betrieben präsent zu sein.

Der vorgestellte Tarifvertrag zur Telearbeit ist ein Beitrag zur Gestaltung von elektronischer Arbeit und eine Zukunftssicherung für die Beschäftigten.

Die *klassische*, geregelte Telearbeit breitet sich nicht in dem in den 1980er und 1990er Jahren erwarteten Maße aus. Hemmnisse sind nicht nur die befürchteten Kosten von Telearbeit und Bedenken der Unternehmen hinsichtlich Kontrolle und Datenschutz, sondern auch die Sorge der Beschäftigten, sich mit dieser Arbeitsform ins berufliche Abseits zu begeben. Diese Variante von e-Work wird damit wohl auch in Zukunft nur für bestimmte Tätigkeiten durchsetzbar und gewünscht sein. Gestaltungselemente sind jedoch sicher auf viele e-Work-Formen übertragbar. Auch die Erfahrungen eines seit 1997 tätigen virtuellen Beratungsteams von ver.di bestätigt diese Entwicklung.

OnForTe – ein virtuelles ver.di-Beratungsteam

Das Projekt Online-Forum-Telearbeit (OnForTe) geht auf die Erfahrungen der DPG zurück und wurde gemeinsam von den Gewerkschaften HBV, DAG und IG Medien getragen.

Das Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie sowie die Deutsche Telekom AG unterstützten das Projekt bis zum 30.06.2001.

OnForTe schafft Transparenz in Fragen der Telearbeit, der virtuellen Teamarbeit, berät bei der Einführung von e-Learning sowie Intranet und Internet. Von sechs verschiedenen Standorten in der Bundesrepublik Deutschland aus berät das arbeitnehmerorientierte Expertennetzwerk, um die Risiken neuer Arbeitsformen zu minimieren und die Chancen zu nutzen. OnForTe wendet sich primär an Arbeitnehmerinnen und Arbeitnehmer, übrigens völlig unabhängig von ihrer Gewerkschaftszugehörigkeit. Das Projekt ist offen für Selbstständige, für freie Mitarbeiter und natürlich für Betriebs- und Personalräte und Gewerkschaften.

Jede/r im OnForTe-Team arbeitet selbst als Telearbeiterin bzw. Telearbeiter. Im virtuellen Expertennetzwerk helfen ein freier Journalist, eine Rechtsanwältin, eine Betriebswirtin, eine Tarifexpertin und ein Betriebsrat am Telefon, per Fax und per Mail Ratsuchenden weiter. Neben der Einzelberatung referieren die Kolleginnen und Kollegen bei Veranstaltungen und beraten Betriebe. Sie kümmern sich um die rechtlichen, ökonomischen, tariflichen und betriebspraktischen Fragen der Telearbeit. Das Projekt ist im Internet präsent (www.onforte.de), ein Call Center dient als erste Anlaufstelle für Interessierte.

Darüber hinaus hat OnForTe Basisinformationen mit praktischen Tipps, Checklisten etc. in Broschürenform zur Verfügung gestellt: Telearbeit 1 + 2, E-Learning, Intranet/Internet und Wissensmanagement.

Eine Begleitforschung zu OnForTe belegt, dass zwei Drittel der Anrufer hoch zufrieden mit der Hilfe des Projektes sind und die Verständlichkeit der Information begrüßen. Die Struktur des Projektes mit einer Call-Center-Lösung und einem virtuellen Expertennetzwerk wurden als wichtige Voraussetzung für eine kompetente Fachberatung identifiziert. (vgl. OnForTe 1999). Eine derartige Virtualisierung der Beratung kann herkömmliche branchen-, betriebs- oder regionalbezogene Gewerkschaftsarbeit unterstützen und Chancen für neuartige flexible Kooperation im Sinne der Ratsuchenden bieten. Eine virtuelle Beratungsstruktur wie OnForTe ist *eine* mögliche Antwort auf die Ausbreitung von e-Work-Prinzipien, die sich nicht mehr auf betriebliche Strukturen fixieren.

Abbildung 5: OnForTe - Das virtuelle Büro

Trendsetter, nicht Brechstange

e-Work in den verschiedenen Formen Telearbeit, virtuelle Teamarbeit, Telekooperationen, virtuelle Betriebe und Wissensarbeit werden zunehmend zu Kennzeichen einer Arbeitswelt, die von einer wachsenden Dienstleistungsorientierung geprägt ist und uns zugleich mehr Flexibilität abverlangt und bietet. Die starren Hierarchien und streng arbeitsteiligen Prozesse der *Fließband-Ära* passen dazu nicht mehr. Arbeitstechniken, Arbeitsformen und Arbeitsbeziehungen verändern sich grundlegend. Betriebe werden mehr und mehr zu virtuellen Gebilden, in denen konventionelle Strukturen durch digitalisierte Formen und elektronische Netze ersetzt werden. Das Qualifikationsniveau ist ebenso wenig ausschlaggebend wie das individuelle Interesse an dieser

Form der Arbeit. Die Entscheidung für oder gegen e-Work kann sich damit für jede und jeden stellen.

Es gilt, in neuen Arbeitsformen Flexibilität mit Sicherheit zu verknüpfen. Existenzielle Anliegen der Beschäftigten bleiben Schutz, Teilhabe, humane Arbeitsbedingungen, gerechte Entlohnung und Mitbestimmung. Größere Autonomie in der Wahl der Arbeitszeit und des Arbeitsortes durch elektronische Arbeitsformen (E-Work) muss mit adäquatem Schutz verbunden werden.

Die bisherigen Erfahrungen vor allem auf dem Feld der Telearbeit belegen: Wenn die Risiken eingedämmt sind und ein ausreichender Schutzrahmen verankert ist, steigt das Vertrauen in die neuen Arbeitsformen rapide.

e-Worker sind Informationsarbeiterinnen und Informationsarbeiter, deren Wissen das Wesen der Informationsgesellschaft ausmacht. Warum sollen sie eine Verschlechterung ihrer Arbeitsbedingungen hinnehmen, obwohl sie den wesentlichsten Produktionsfaktor der Informationsgesellschaft in ihren Köpfen tragen?

Literatur:

empirica (2000) EcaTT Final Report. Benchmarking Prozess on New Ways of Working and New Forms of Business across Europe, Bonn 2000

EU (1999) Europäische Kommission: Status Report on European Telework. New Methods of Work 1999 (www.eto.org.uk/twork/tw99/index.htm)

Freudenreich, Klein, Wedde (1997): Entwicklung der Telearbeit – Arbeitsrechtliche Rahmenbedingungen, Abschlußbericht, Bundesministerium für Arbeit und Sozialordnung (Hrsg), Bonn 1997

Giarini, Orio/Liedtke, Patrick M.(1998): Wie wir arbeiten werden – Der neue Bericht an den Club of Rome, Hamburg 1998

Input Consulting GmbH (2002): „Anytime, anyplace…" Befunde zur elektronischen Internationalisierung von Arbeit, Stuttgart 2000

Input Consulting GmbH (2002): „Mobile Telearbeit – Problemfelder und Gestaltungsideen (MOTAP)" im Auftrag von ver.di – Vereinte Dienstleistungsgewerkschaft e.V., Stuttgart, 2002

OnForTe (1997) Online Forum Telearbeit: „Basisinformation Telearbeit", Frankfurt 1997

OnForTe (1999) Online Forum Telearbeit: „Basisinformation II Telearbeit", Frankfurt 1999

Reichwald, Ralf (1998): Telekooperation – Verteilte Arbeits- und Organisationsformen, Berlin 1998

Raphael Menez/Stefanie Springer

Kollektive Regulierung von subjektivierten Arbeitsverhältnissen in der IT-Branche

Gewerkschaften haben bei der Organisation junger, überwiegend wissensbasierter Branchen und Tätigkeitsfelder mit enormen Zugangsproblemen zu kämpfen. Am Beispiel der IT-Branche lässt sich zeigen, dass tradierte Organisationsstrategien wie Interessenkollektivierung und Schutzpolitiken bei hochqualifizierten Experten weitgehend ins Leere gehen. Zumindest bei jungen, expandierenden Unternehmen dominiert bislang ein Typus der Arbeitsregulation, in dem hochqualifizierte Beschäftigte ihre Arbeitsbedingungen weitgehend selbst aushandeln.

Von gewerkschaftlicher Seite wurde bisher davon ausgegangen, dass mit sich verschlechternder Arbeitsmarktlage auch die „Sympathien für die gute alte gewerkschaftliche Interessenvertretung" (so IG Metall-Vize Jürgen Peters) von selbst steigen werden. Infolge der Wachstumsschwäche der Wirtschaft und der damit verbundenen Krise der IT-Branche kam es zwar zur vermehrten Gründung von Betriebsräten, aber ein signifikanter Mitgliederzuwachs bei den Gewerkschaften und eine Ausweitung ihrer Organisationsdomäne konnte nicht verzeichnet werden. Vor diesem Hintergrund stellt sich die Frage, unter welchen Voraussetzungen Gewerkschaften eine kollektive Interessenvertretung in der IT-Branche implementieren können. Um diese Frage zu beantworten, werden zunächst die Arbeitsformen und Beschäftigungsbedingungen der IT-Branche analysiert, um sie den Regulationsmustern gewerkschaftlicher Interessenvertretung gegenüber zu stellen. Wir gehen dabei von der These aus, dass eine auf Kollektivierung abzielende Interessenvertretung, wie sie traditionell von den Gewerkschaften verfolgt wird, unter neuen heterogenen Beschäftigungsbedingungen mit auseinander strebenden Interessenlagen nur wenig Erfolg haben wird.

Arbeitsformen und Beschäftigungsbedingungen in der IT-Branche

Grundsätzlich ist es schwierig, von *den* IT-Fachkräften bzw. *der* IT-Branche zu sprechen. Die Informationstechnik ist eine Querschnittstechnologie, die in fast allen Branchen sowohl

Anwendung findet als auch – an die jeweiligen Erfordernisse angepasst – weiterentwickelt wird. Entsprechend ist die IT-Branche als solche in keiner Wirtschaftssystematik verzeichnet, sondern nur durch die Bündelung verschiedener Wirtschaftszweige (re)konstruierbar. Die IT-Branche ist gekennzeichnet durch einen hohen Angestelltenanteil, hohe Anteile an Hoch- und Fachhochschulabgängern sowie eine Zunahme junger hochqualifizierter Beschäftigter in den Dienstleistungsbereichen bei gleichzeitiger Abnahme von Beschäftigtengruppen in hardwarenahen, produzierenden Bereichen (Trautwein Kalms 1995¸ Menez/Munder/Töpsch 2001; Boes/Baukrowitz 2002, Bitkom 2002). Ungeachtet der Abgrenzungsprobleme gilt die IT-Branche als Vorreiter für die Entstehung neuer Beschäftigtentypen und Arbeitsformen (Töpsch/Menez/Malanowski 2001; Heidenreich/Töpsch 1998; Braczyk u.a. 2000). Die heterogenen Beschäftigungsbedingungen variieren je nach Größe, Geschäftsbereichen und Produkten des Unternehmens, den Einsatzbereichen und Tätigkeitsfeldern der Mitarbeiter sowie nicht zuletzt in Abhängigkeit von der individuellen beruflichen Qualifikation. Als Ergebnis zeigen sich hier Arbeitsformen und Arbeitsbedingungen, die oftmals vom klassischen Normalarbeitsverhältnis abweichen, was in der sozialwissenschaftlichen Diskussion als „Entgrenzung von Arbeit" (Voß 1998) bezeichnet wird.

Entgrenzung und Pluralisierung von Arbeit

Ein Blick in die spärlich vorhandene Empirie zeigt: Bezogen auf die kontraktuelle Seite sind vor allem in den kreativen Arbeitsbereichen auf Selbständigkeit beruhende Vertrags- und Kooperationsformen erkennbar. Der Anteil von Freiberuflern ist im Bereich Grafik und Multimedia-Design am höchsten, weniger verbreitet ist der Einsatz von freien Mitarbeitern dagegen bei den überwiegend großen Unternehmen des Telekommunikationssektors sowie bei den Hardwareproduzenten (Menez/Munder/Töpsch 2001).

Der überwiegende Anteil der IT-Beschäftigten befindet sich dennoch weiterhin in Angestelltenverhältnissen (Trautwein-Kalms 1995), wobei *selbstorganisierte Arbeitsformen* einen immer höheren Stellenwert erhalten. Viele der wissensintensiven Tätigkeiten finden projektförmig statt – meist mit starkem Kunden- und Dienstleistungsbezug – und lassen hierarchische Anweisungsstrukturen in den Hintergrund treten. Fallstudien der TA-Akademie in Unternehmen der IT-Branche zeigen, dass in diesen Unternehmen vorwiegend Koordinationsmechanismen zum Einsatz kommen, die wesentlich auf dem Organisationsmodus der „Problemlösung" (Braczyk 2001) beruhen und als *diskursive bzw. ergebnisbezogene Koordinations- und Steuerungsformen* (Braczyk u.a. 2000) bezeichnet werden können. Kontrolliert wird hierbei das Endergebnis und nicht mehr der Weg dorthin.

Bezogen auf die Arbeitszeit sind oft weder die Dauer noch die Lage der Arbeitszeit einer expliziten Regelung unterworfen. Eine Zeiterfassung wird allenfalls vorgenommen, um Bearbeitungszeiten bestimmten Projekten und Kunden zuordnen zu können. Dementsprechend gibt es – insbesondere in Unternehmen ohne betriebliche Interessenvertretung und tarifvertragliche Bindung – keinen einklagbaren Arbeitszeitausgleich und meist auch keine Vergütung von Überstunden. De facto bedeutet dies, dass die Mitarbeiter mit ihrer tatsächlichen Arbeitszeit deutlich über dem vereinbarten Soll liegen. In den untersuchten Unternehmen lag die effektive wöchentliche Arbeitszeit durchschnittlich ca. 3 Stunden über der vereinbarten Arbeitszeit (Menez/Munder/Töpsch 2001).

Insgesamt wird in dienstleistungs- und wissensintensiven Unternehmen die Relation von Leistung und Gratifikation in vergleichsweise hohem Maße individualisiert (Töpsch/Menez/Malanowski 2001). Die Gehälter der Mitarbeiter setzen sich aus festen und variablen Gehaltsbestandteilen zusammen, die nach der (aktuellen) individuellen Leistung bemessen werden. Individuelle Verhandlungen und anschließende Zielvereinbarungen zwischen Mitarbeitern und Vorgesetzten bzw. Projektleitern sind die Grundlage für die Kalkulation der variablen Entgeltbestandteile. Dies führt zu einer starken Einkommensdifferenzierung sowohl zwischen Einstiegs- und Topmanagement-Gehältern als auch zwischen verschiedenen Tätigkeiten bzw. Berufen im IT-Bereich (IG Metall 2000; Menez/Munder/Töpsch 2001).

Die Zunahme von Projektarbeit, selbständigen Vertragsformen, ergebnisbezogener Koordinierung, individuellen Arbeitszeitregimes und Vergütungsformen sind Indikatoren eines weitreichenden Deinstitutionalisierungs-Prozesses, mit dem vormalige Grenzen der Produktion und des Arbeitens verschwimmen. Diese *Entgrenzung von Arbeit* ist dabei „Ausdruck neuer arbeitskraftorientierter Rationalisierungsstrategien, die sich darauf richten, bislang weniger zugängliche Leistungspotentiale der Arbeitskräfte auszuschöpfen" (Döhl u.a. 2000: 10). Damit verbunden ist eine schleichende Auflösung des industriegesellschaftlich verfassten Normalarbeitsverhältnisses[1] und der an ihm ausgerichteten industriegesellschaftlichen Institutionen.

Ihren Fluchtpunkt hat diese Entwicklung im Individuum (Wolf/Mayer-Ahuja 2002). Denn wenn kollektive Institutionen und Grenzen aufweichen, ergibt sich für die Beschäftigten selbst die Notwendigkeit und Möglichkeit, die Arbeit zu strukturieren sowie entstehende Unsicherheitszonen subjektiv zu interpretieren und zu bewältigen. Entgrenzt werden damit auch die Ansprüche an die Beschäftigten, die nicht mehr an formalfachlichen Anforderungen halt machen und nunmehr die ganze Person und ihre Subjektivität in den Arbeitsprozess einbinden sollen. Arbeit in der IT-Branche kann daher als „subjektivierte Arbeit" (Moldaschl/Voß 2002, vgl. auch Schönberger/Springer 2003) bezeichnet werden.

Die sich dahinter verbergende veränderte Logik der Nutzung von Arbeitskraft (Moldaschl 2002) wird um so klarer, je mehr man sich verdeutlicht, dass der tayloristisch-industrielle Organisationsmodus gerade auf *die Ausschaltung von Subjektivität* in Arbeitsprozessen setzt. Die starke Zergliederung und Standardisierung von Arbeitsabläufen in hierarchischen Anweisungsstrukturen soll die frei gestaltbaren Handlungsräume reduzieren, die aus der Managementperspektive immer auch eine unbeherrschte Unsicherheitszone bedeuten. Kritisiert wurden aus sozialwissenschaftlicher, aber auch aus gewerkschaftlicher Sicht immer wieder die mangelnden Identifikations- und Selbstentfaltungsmöglichkeiten für die Beschäftigten, die aus dem fehlenden Bezug zum gesamten Produktionsprozess und zum Endprodukt resultieren. Wird von betrieblicher Seite nun explizit auf eine subjektiv kontrollierte Leistungserstellung in entgrenzten Arbeitsstrukturen gesetzt, könnten auch neue Möglichkeiten entstehen, sich in und durch die Arbeit zu entfalten. Und diese individuellen Selbstentfaltungsmöglichkeiten

erschweren die Zusammenführung individueller Interessen zu kollektiven Forderungen, zumal die subjektiven Interessenlagen der Beschäftigten in ausdifferenzierten Arbeitsbedingungen auseinanderdriften.

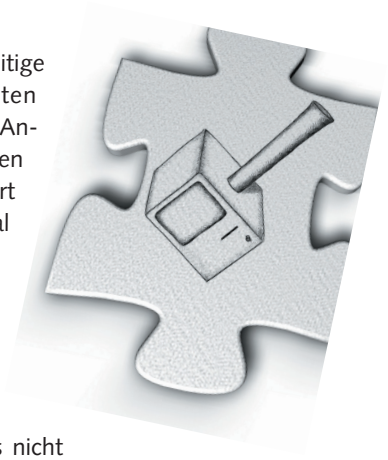
Selbstverständnis, Arbeitsorientierungen und Interessenstrukturen der IT-Fachkräfte

Neben der Entgrenzung von Arbeit ist das gewandelte Selbstverständnis der Arbeitskräfte eine weitere Barriere für eine kollektive Interessenvertretung. IT-Experten stellen eine sehr selbstbewusste Klientel dar, die eigene Ansprüche an die Arbeit formuliert. Vor allem bei jungen, gut ausgebildeten Angestellten in qualifizierten Berufspositionen ist ein hohes „individualistisches Interessen- und Handlungskonzept" (Baethge 1994: 720) beobachtbar, das sich auf eine starke inhaltliche Berufsorientierung mit hoher Wissens- und Fachkompetenz stützt. Formuliert werden dezidiert Ansprüche an Selbstentfaltung in der Arbeit und im Privatleben. Demgegenüber haben rigide Organisationsstrukturen mit geringen Freiheitsgraden Akzeptanzprobleme unter den Beschäftigten (Heidenreich 1996). Für berufliche Freiheiten sind sie bereit, *Opfer* in Form eines intensiven Arbeitseinsatzes zu bringen. Kotthoff (2001) z.B. kommt für hochqualifizierte Angestellte zu dem Ergebnis, dass sie ihre vermarktlichten Arbeitsbedingungen nicht als Selbstausbeutung empfinden, da sie damit eine besondere und privilegierte Art der Lebensführung verbinden. Pongratz/Voß (2003) weisen in ihrer jüngsten Studie darauf hin, dass Angestellte sich in Projektteams als „Teil einer gesellschaftlichen Dynamik" (ebd.: 141) verstehen. Belastungen in Form von langen Arbeitszeiten und Stress-Symptomen werden in Kauf genommen, „weil sie [die Angestellten] ein höheres Ziel vor Augen haben". Betont wird zudem eine emotionale Spaß- und Erlebenskomponente, die sich mit einem ausgeprägten Leistungsanspruch verknüpft und auch bei Angestellten mit geringerem Qualifikationsniveau bemerkbar ist (ebd.: 139).

Verbunden ist mit diesem Arbeitsverständnis auch ein bewusster Verzicht auf kollektive Regulierungsformen. Das distanzierte Verhältnis von hochqualifizierten Angestellten und Gewerkschaften ergibt sich laut Kotthoff,

> *„weil sie die Organisation der Arbeiter und unteren Angestellten ist, und deshalb nicht die Identität der beitragsorientierten firmenloyalen, unternehmerisch eingestellten Leistungsträger und Intrapreneure verkörpert. Die Gewerkschaft verkörpert für sie ein Milieu, in dem die Identität des arbeitenden Menschen mit Entfremdung, Verelendung, mangelnder Anerkennung und mit darauf basierendem Protest und Gegenmacht in Verbindung gebracht wird. In einer solchen Verbindung möchten sich die HQA [hochqualifizierte Angestellte, d.V.] nicht wiederfinden" (Kotthoff 2001: 13).*

Der Standpunkt, die eigenen Interessen selbst am besten vertreten zu können, beruht natürlich auch auf einer von den Wissensarbeitern empfundenen Marktmacht, die insbesondere in der IT-Branche aufgrund des bislang diagnostizieren Fachkräftemangels galt (Menez/Munder/Töpsch 2001). Ob sich durch die aktuell rückläufige Beschäftigungsentwicklung in der IT-Branche (Bitkom 2002) Ansatzpunkte für kollektives Interessenhandeln ergeben, bleibt offen, da Arbeitsplatzverluste in dieser Branche durch anderweitige Beschäftigungsmöglichkeiten für IT-Fachkräfte bei IT-Anwendern in anderen Branchen teilweise gut kompensiert werden können, wie Dostal (2002) bemerkt.



Von den Beschäftigten formulierte Spannungsverhältnisse deuten aber darauf hin, dass das neue selbstbewusste Arbeitsethos nicht konfliktfrei ist. So konnten Baethge u.a. (1995) nachweisen, dass auch Führungskräfte wahrnehmen, dass die „betriebliche Realität (...) das im zivilen Leben genährte Bedürfnis nach mehr Transparenz und Einfluss bei wichtigen Entscheidungen" (Baethge u.a. 1995: 359) enttäuscht. Die Untersuchungen von Voß/Pongratz weisen – neben einer emotionsgeladenen Leistungsorientierung am Arbeitsplatz – für die persönliche Lebensführung und berufliche Entwicklung über die Betriebsgrenzen hinaus auch bei höher qualifizierten Angestellten eine starke Absicherungsmentalität nach (Pongratz/Voß 2003).

Typen der Arbeitsbeziehungen in der IT-Branche

Wir haben bisher gezeigt, dass die IT-Branche nicht nur durch eine Vielfalt an Arbeitsformen, Beschäftigungsbedingungen und Interessenstrukturen gekennzeichnet ist, sondern die Beschäftigten auch ein verändertes, inhaltlich orientiertes Selbstbewusstsein an den Tag legen. Nun wollen wir der Frage nachgehen, wie Arbeit in der IT-Branche reguliert wird, wie also die „Verkaufs- und Anwendungsbedingungen der Arbeitskraft" (Müller-Jentsch 1997) zwischen den Beschäftigten, Betriebsrat, Management, Gewerkschaften und Arbeitgeberverbänden ausgehandelt werden. In Anlehnung an eigene empirische Untersuchungen unterscheiden wir dabei drei Typen der Arbeitsregulation in der IT-Branche (Töpsch/Menez/Malanowski 2001; Menez/Töpsch 2003), die vor allem die verschiedenen Interessenvertretungs-Strukturen, die jeweils dominierenden Akteure sowie die bevorzugten Regulationsgegenstände, Regelungsebenen und Regelungsinstrumente beschreiben.

Tarifliche Arbeitsregulation

Die „tariflich-unternehmensbezogene Arbeitsregulation" hat ihren Ursprung im Flächentarifvertrags-System. Hier sind die verbandlichen und betrieblichen Akteure bemüht, die wichtigsten Variablen der Arbeitsbedingungen wie Arbeitszeit, Entgelt, Qualifizierung, Belastungen usw. zu standardisieren und möglichst flächendeckend einer Regulierung zu unterwerfen. In der IT-Branche finden wir den *reinen* Typus der kollektiven tariflichen Arbeitsregulation kaum, statt dessen gelten für einige Unternehmen sog. Ergänzungs-Tarifverträge, in denen mit Zustimmung der Gewerkschaften von wichtigen tarifvertraglichen Regelungen abgewichen werden kann, beispielsweise in Fragen der Arbeitszeit. Meist handelt es sich bei Unternehmen dieses Typs um solche, die eine historische Bindung an das Flächentarifvertragssystem und die damit verbundene Kultur der Arbeitsbeziehungen haben. Es sind in der Regel Unternehmen, die aus dem Organisationsbereich des Flächentarif-Systems

durch Ausgründung oder die Entwicklung neuer Geschäftsfelder herausgewachsen sind und in denen teilweise eine heterogene Gemengelage von Regulationsformen vorherrscht, bedingt etwa durch den Zukauf von oder die Fusion mit nicht tarifgebundenen Unternehmen.

Unternehmensbezogene Arbeitsregulation

Dieser Regulationstypus unterscheidet sich insofern von der tariflichen (kollektiven) Arbeitsregulation, als die hier zugeordneten Unternehmen keiner tariflichen Regulation unterliegen, auch nicht in Form eines Haus- oder Unternehmenstarifvertrags. Meist handelt es sich um Unternehmen, die keine historische Bindung an das Flächentarifvertrag-System aufweisen oder sich schon vor langer Zeit für die Exit-Option entschieden haben (wie etwa Hewlett Packard). Dominante Regelungsinstrumente sind bei diesem Typus Betriebsvereinbarungen bzw. Zielvereinbarungen zwischen Mitarbeitern und Vorgesetzten sowie die individuellen Arbeitsverträge. Bei diesem Regulationstypus zeigt sich auch, dass die betriebliche Interessenvertretung nicht mit gewerkschaftlicher Interessenvertretung Hand in Hand gehen muss, in einigen Unternehmen existierten sogar ausgesprochen *gewerkschaftsferne* Betriebsräte. Sie beziehen Beratungs- und Unterstützungsleistungen, die in anderen Fällen die Gewerkschaft bereitstellt, bereits von externen Dienstleistern, etwa Rechtsanwälten.

Individualisierte Arbeitsregulation

Der dritte Typ, den wir als individualisierte Arbeitsregulation bezeichnen, unterscheidet sich grundlegend von den in den industriellen Kernbereichen verbreiteten Regulationsformen. Die hier zugeordneten Unternehmen und ihre Mitarbeiter kommen nicht nur ohne Tarifvertrag und auch ohne Mitbestimmung und Betriebsverfassung aus, sondern praktizieren den bewussten Verzicht auf diese Regulationsformen. Wichtigste Regelungsinstrumente sind Arbeitsvertrag und Zielvereinbarung. Gewerkschaften und Arbeitgeberverbände treten bei diesem Regulationstypus als Akteure der Interessenaushandlung in den Hintergrund. Weder sind die Beschäftigten gewerkschaftlich organisiert, noch sind die Unternehmen einem Arbeitgeberverband angeschlossen. Auftretende Probleme werden in der direkten Aussprache zwischen Beschäftigten und Führungskräften thematisiert und zu lösen versucht. Die Kontrolle des Arbeitgebers bezieht sich nur noch auf die Zielerreichung, den Weg zum Ziel müssen die Beschäftigten weitgehend selbst verantworten. *Commitment* gegenüber der Firma und dem Team sowie das Ethos des professionellen Spezialisten kennzeichnen das Selbstverständnis der Mitarbeiter. Diese verstehen sich daher auch kaum mehr als Arbeitnehmer im hergebrachten Sinn.

Möglichkeiten und Grenzen einer gewerkschaftlichen Interessenvertretung in der IT-Branche

Um zu verdeutlichen, welche Auswirkungen die beschriebenen Regulationsmuster auf die gewerkschaftliche Interessenpolitik haben, soll kurz die klassische gewerkschaftliche Strategie beschrieben werden, das Fernziel flächen- oder unternehmensbezogener Tarifbindung über einzelne Etappen zu erreichen: Über die Beratung von Beschäftigten sollen Betriebsräte in den Unternehmen aufgebaut werden, die dann aktiv Mitglieder rekrutieren und betriebliche Vereinbarungen abschließen, um Regelungskompetenz zu beweisen. Diese betrieblichen Erfahrungen sollen dann in einem weiteren Schritt in kollektive Regelungen überführt werden, sobald eine kritische Größe an Gewerkschaftsmitgliedern in den Betrieben aufgebaut wurde und zur Durchsetzung von kollektiven Regelungen mobilisiert werden kann. Allerdings zeigt sich nach unseren bisherigen Beobachtungen, dass die oben vorgestellten Typen der Arbeitsregulation in sich relativ stark verriegelt sind, mit anderen Worten: In Unternehmen, in denen sich ein bestimmter Regulationsmodus etabliert hat, haben es die betrieblichen und überbetrieblichen Akteure der industriellen Beziehungen nicht leicht, diesen Regulationsmodus zu verändern, weil damit eine Änderung der Regelungsebenen, Regelungsgegenstände und Regelungsinstrumente verbunden ist. Aus gewerkschaftlicher Sicht sind stabilisierte Formen der unternehmensbezogenen und individualisierten Arbeitsregulation damit langfristig bestandsgefährdend, da sich beide Typen der Arbeitsregulation durch die Abwesenheit kollektiver überbetrieblicher Akteure ausweisen. Offenbar ist das Vorhandensein einer institutionalisierten betrieblichen Interessenvertretung zwar eine notwendige, aber keine hinreichende Voraussetzung für gewerkschaftliche Einflussnahme. Als Fazit lässt sich an dieser Stelle festhalten: Die Entgrenzung von Arbeit führt nicht zwingend zur Auflösung der institutionellen Regulierungsmuster, es kommt allerdings zu einem Bedeutungsverlust der überbetrieblichen Ebene der industriellen Beziehungen und damit zu einem Bedeutungsverlust der Gewerkschaften in dieser Branche, weil betriebliche und individuelle Vereinbarungen bisherige tarifliche Regulationsmuster ersetzen.

Ein wesentlicher Faktor für den Bedeutungsverlust von Gewerkschaften im IT-Bereich liegt in der Heterogenität der Beschäftigteninteressen. Die klassische gewerkschaftliche In-

Die Autoren

Stefanie Springer, Dipl.Sozialwirtin, ist wissenschaftliche Mitarbeiterin im Projekt „Wandel der Erwerbsarbeit im Übergang zur Wissensgesellschaft“ der Akademie für Technikfolgenabschätzung, Stuttgart. Arbeitsschwerpunkte: Informatisierte und subjektivierte Arbeit, organisationaler Wandel, Wissensökonomie. Kontakt: stefanie.springer@ta-akademie.de

Raphael Menez, Soz. M.A., ist wissenschaftlicher Mitarbeiter im Projekt „Interessenverbände in der IT-Branche“ am Institut für Politikwissenschaft der Universität Tübingen. Arbeitsschwerpunkte: Industrielle Beziehungen, Verbändeforschung, Arbeits- und Industriesoziologie. Kontakt: raphael.menez@uni-tuebingen.de

teressenpolitik, die auf die Vereinheitlichung der Lebens- und Arbeitsbedingungen ihrer spezifischen Klientel setzt, verliert so ihre Bezugspunkte. Die Klientel wandelt sich, und einheitliche Interessenlagen sind nur noch schwer zu identifizieren. Die Heterogenität der Interessen spiegelt sich in der ganzen Bandbreite zwischen Autonomie und Schutz und ist nicht mehr nur an einzelnen Beschäftigtengruppen festzumachen, so dass individualisierte Interessenlagen zunehmend schwerer zu aggregieren sind. Je nach individueller Arbeitssituation und Lebenslage entstehen Bedürfnisse nach mehr Freiraum oder nach mehr Regulierung, und Gewerkschaften stehen damit vor einem Spagat zwischen Schutz- und Gestaltungsmacht der Beschäftigten, auf den sie bisher nur unzureichend vorbereitet sind. Zenke (1999) beschreibt pointiert, dass sich erst in den letzten Jahren auf Seiten der Gewerkschaften die Bedeutung von Interessenpolitik auch für hochqualifizierte Dienstleistungsarbeiter durchgesetzt habe. Allerdings erschweren unklare Zuständigkeitsbereiche und Kommunikations-Barrieren eine erfolgreiche Angestelltenpolitik für Hochqualifizierte. Und auch Schumann argumentiert, dass sich die Gewerkschaften in ihrer Interessenpolitik auf ein pluralisiertes Solidaritätsverständnis einstellen sollten:

> *„innerhalb der „Arbeiter" und „Angestellten" sind die Unterschiede manchmal größer als das Gemeinsame. Der Anspruch auf Solidarität trifft damit auf ausdifferenzierte Interessen- und Problemlagen. Für die traditionelle Arbeitersolidarität gilt: Die Interessendifferenzen von Kapital und Arbeit lassen sich zwar noch bündeln und können solidarisches Verhalten begründen. Aber: Diese Solidarität steht in Konkurrenz mit vielen anderen „Gemeinschafts"-Bezügen und Verpflichtungen; die Solidarität der abhängig Beschäftigten ist in Gefahr, ihre normativ überhöhte, emotional gestützte sozialmoralische Selbstverständlichkeit zu verlieren" (Schumann 2001: 532).*

Hinzu kommt, wie Anke Hassel konstatiert, dass die „mangelhafte Organisation der Angestellten die Achillesferse der Organisationsentwicklung" (Hassel 1999: 231) bleibe, während Ulrich Mückenberger (2002) in diesem Zusammenhang sogar von einer „Rekrutierungsfalle" spricht: die Politik der Gewerkschaften wird von den dominierenden Teilgruppen innerhalb der Organisation bestimmt, wobei die unterlegenen Teilgruppen sich nicht ausreichend repräsentiert sehen und als Konsequenz austreten oder gar nicht erst eintreten. Die Bestätigung der dominanten Interessenorientierung wird dann zum Problem, wenn die innerorganisatorische Dominanz zur Umwelt in Widerspruch gerät und neue Umweltanforderungen intern blockiert werden. Auch Wiesenthal und Clasen (2002) gehen von einer zunehmenden Diskrepanz zwischen Selbstbild und Handlungsprämissen von Gewerkschaften auf der einen Seite und der differenzierter gewordenen Handlungswirklichkeit auf der anderen Seite aus, die eine Neuausrichtung von Gewerkschaftspolitik erforderlich mache.

Schlussfolgerungen und Ausblick

Die Zukunftsfähigkeit der Gewerkschaften hängt entscheidend von ihrer Fähigkeit ab, organisationspolitische Antworten auf diese Herausforderungen zu finden. Als intermediäre Organisation müssen sie den Spagat zwischen der Integration möglichst vieler unterschiedlicher Interessen und der gleichzeitigen Aufrechterhaltung ihrer Handlungsfähigkeit meistern (vgl. Streeck 1987). Eine zentrale Frage lautet, wie es Gewerkschaften gelingen kann, ihre Organisationsfähigkeit – also die Chance, Mitglieder zu rekrutieren, zu binden und zu mobilisieren – auch unter veränderten gesellschaftlichen Arbeits- und Lebensbedingungen sicherzustellen. Um in der IT-Branche eine flächendeckende kollektive Interessenvertretung (also eine tariflich-verbandliche Ordnung) zu implementieren, sind Anpassungsleistungen nötig, die auf einen gewerkschaftlichen Organisationswandel in drei zentralen Dimensionen hinauslaufen:

1. gewerkschaftliche Regelungsinstrumente und –ziele,
2. das gewerkschaftliche Selbstverständnis als Gegenmacht und Dienstleister,
3. die gewerkschaftliche Organisationsstruktur zwischen bürokratischer Massenorganisation und Netzwerkstruktur (Menez/Töpsch 2003).

Zu den *Instrumenten und Zielen gewerkschaftlicher Politik*: Gewerkschaftliche Organisationsdomänen beschränken sich bisher noch auf große Unternehmen mit einer Tradition institutionalisierter Arbeitsbeziehungen. Hier konnten Gewerkschaften über den Abschluss zumeist unternehmens- oder konzernbezogener Regelungen ihre Position sichern oder sogar ausbauen. Überall dort, wo bereits gewerkschaftliche Strukturen bestehen, gelingt es den Interessenvertretungen auch, über Maßnahmen gegen Stellenabbau oder für die Sicherung von Arbeitsplätzen vermehrt Mitglieder zu rekrutieren. Anders ist die Lage in Unternehmen, die der unternehmensbezogenen Arbeitsregulation unterliegen. Hier gelingt es den Gewerkschaften trotz der Krise nur selten, tarifvertragliche Standards zu implementieren, da die Organisationsmacht gemessen an den Mitgliederzahlen im jeweiligen Unternehmen zu schwach ausgeprägt ist. Infolge der wirtschaftlichen Krise gelingt es den Gewerkschaften demgegenüber verstärkt, Unternehmen, die bisher der individualisierten Arbeitsregulation zugeordnet werden konnten, über Beratungsdienstleistungen und Einrichtung von Betriebsräten in den Modus der unternehmensbezogenen Arbeitsregulation zu überführen. Allerdings ist noch nicht abzusehen, inwieweit es sich dabei um stabile Formen der institutionalisierten Interessenvertretung handelt, da auch hier vorrangig kurzfristige Abwehrmaßnahmen gegen Stellenabbau sowie Sozialpläne verhandelt werden.

Das *gewerkschaftliche Selbstverständnis* orientiert sich im IT-Bereich nicht mehr nur an der Herstellung von Gegenmacht, sondern wird ergänzt durch eine verstärkte Kundenorientierung der gewerkschaftlichen Akteure, um so die heterogenen Bedürfnisse der IT-Beschäftigten differenzierter berücksichtigen zu können. Damit verbunden ist eine Ausweitung ökonomischer Kompetenz, um in den entsprechenden Gremien und bei den Beschäftigten vor Ort auch als qualifizierte Beratungs- und Entscheidungsinstanz auftreten zu können. Dies beinhaltet eine Ausweitung der klassischen gewerkschaftlichen Themen, da nicht mehr nur die Verkaufs- und Anwendungsbedingungen der Arbeitskraft, sondern auch Management-Funktionen und Fragen nach der Unternehmens- und Leistungskultur in den Fokus gewerkschaftlicher Politik treten müssen. Diese Dienstleistungsorientierung stößt aber dort an ihre Grenzen, wo das

gewerkschaftliche Selbstverständnis als politisch-moralische Massenorganisation in Frage gestellt wird. Eine reine Dienstleistungsorientierung nach dem Vorbild des ADAC wird nachhaltig abgelehnt, und auch eine stärkere Beitragsdifferenzierung ist zur Zeit noch ein Tabu-Thema innerhalb der gewerkschaftlichen Organisation.

Ein weiterer Faktor bei der Etablierung einer gewerkschaftlichen Interessenvertretung betrifft die Einrichtung von *Projekt- und Netzwerkstrukturen* im IT-Bereich. Die gewerkschaftliche Diskussion über die Vor- und Nachteile dieser Organisationsformen zur Erschließung der IT-Branche ist gerade in vollem Gange, und die zur Zeit laufenden Pilotprojekte (z. B. *connexx.av* von *Ver.di* oder das Siemens-Projekt der IG Metall) sind hinsichtlich ihrer Erfolge bei der Erschließung von Mitgliedern und Unternehmen sehr unterschiedlich zu bewerten. Die Vorteile von gewerkschaftlichen IT-Projekten und –Netzwerken liegen aber darin, dass so die Kompetenzen und die Aktivitäten der unterschiedlichen Zuständigkeitsbereiche besser gebündelt werden können. Zudem gelingt hier eine bessere Einbindung von Gewerkschaftsaktivisten und eine differenziertere Berücksichtigung der Interessen der IT-Beschäftigten vor Ort. Die Nachteile werden in einer Gefahr von Verselbständigungs-Tendenzen innerhalb der gewerkschaftlichen Organisation gesehen, die letztlich die ehernen Prinzipien als Branchen- und Einheitsgewerkschaft in Frage stellen könne. Die daraus resultierenden Organisationswiderstände schlagen daher noch in einer begrenzten Ressourcenausstattung und fehlenden personellen Kapazitäten zu Buche, die dazu führen, dass neue Unternehmen und neue Mitglieder im IT-Bereich bisher nur schwer zu organisieren sind.

1 *Unter Normalarbeitsverhältnis (NAV) versteht Mückenberger (1985: 429) „Arbeitsverhältnisse, die idealiter dauerhaft und kontinuierlich, im (möglichst groß-)betrieblichen Zusammenhang auf Vollzeitbasis erfolgen und Qualifikationen voraussetzen". Das NAV war also strukturiert durch den Betrieb als festen Ort der Leistungserbringung, einer an Vollzeitbeschäftigung orientierten Regelarbeitszeit von unbefristeter Dauer sowie die Abhängigkeit und Weisungsgebundenheit des Arbeitnehmers gegenüber dem Arbeitgeber. Flankiert wurde es durch institutionelle Rahmenbedingungen wie z. B. die duale Berufsausbildung und das System der industriellen Beziehungen sowie durch die sozialen Sicherungssysteme.*

Literatur

Baethge, Martin/Denkinger, Joachim/Kadritzke, Ulf (1995): Das Führungskräfte-Dilemma. Manager und industrielle Experten zwischen Unternehmen und Lebenswelt. Frankfurt: Campus.

Baethge, Martin (1994): Arbeit 2000. Wie Erwerbsarbeit Spaß macht – Arbeitsansprüche der Beschäftigten als Herausforderung für die Gewerkschaften. Gewerkschaftliche Monatshefte (45) 12: 711-733.

Boes, Andreas/Baukrowitz, Andrea (2002): Arbeitsbeziehungen in der IT-Industrie. Berlin: edition sigma.

BITKOM 2002: Arbeitsmarkt der Informations- und Kommunikationsbranche schrumpft. Pressemitteilung und Charts vom 29.07.2002.

Braczyk, Hans-Joachim (2001): Wandel des Unternehmensregimes. S. 39–61. In: Fuchs, Gerhard/Töpsch, Karin (Hg.): Baden-Württemberg – Erneuerung einer Industrieregion. Kolloquium zum Andenken an Prof. Dr. Hans-Joachim Braczyk. Stuttgart: TA-Akademie.

Braczyk, Hans-Joachim/Franzpötter, Reiner/Renz, Christian/Töpsch, Karin (2000): Wandel der Arbeit durch neue Formen der Koordination und Steuerung. Forschungsbericht für die Deutsche Forschungsgemeinschaft. Stuttgart.

Döhl, Volker/Kratzer, Nick/Sauer, Dieter (2000): Krise der NormalArbeit(s)Politik. Entgrenzung von Arbeit – neue Anforderungen an Arbeitspolitik. WSI – Mitteilungen (53) 1: 5-17.

Dostal, Werner (2002): IT-Arbeitsmarkt. Chancen am Ende des Booms. IAB-Kurzbericht Nr. 19/2002.

Faust, Michael/Jauch, Peter/Notz, Petra (2000): befreit und entwurzelt: Führungskräfte auf dem Weg zum internen Unternehmer. München/Mering: Hampp.

Franzpötter, Reiner (2000): Der unternehmerische Angestellte – ein neuer Typus der Führungskraft in entgrenzten Interorganisationsbeziehunge n. S. 163-176 In: Minssen, Heiner (Hrsg.), Begrenzte Entgrenzungen: Wandlungen von Organisation und Arbeit. Berlin: edition sigma.

Hassel, Anke 1999: Gewerkschaften und sozialer Wandel. Baden-Baden: Nomos.

Heidenreich, Martin (1996): Die subjektive Modernisierung fortgeschrittener Arbeitsgesellschaften. Soziale Welt (47) 1: 25-43.

Heidenreich, Martin/Töpsch, Karin (1998): Die Organisation von Arbeit in der Wissensgesellschaft. Industrielle Beziehungen (5) 1: 13-44.

IG Metall (2000): IT-Magazin. Informationen der IG Metall für die Beschäftigten der IT-Industrie 1/2000. Frankfurt: IG Metall.

Kleemann, Frank/Matuschek, Ingo/Voß, G. Günter (2002): Subjektivierung von Arbeit. Ein Überblick zum Stand der Diskussion. S. 53-100 In: Moldaschl, Manfred/Voß, G. Günter (Hrsg.), Subjektivierung von Arbeit. München/Mering: Hampp.

Kotthoff, Hermann (2001): Zwischen Selbstausbeutung und Selbstverwirklichung. Wandlungen im Arbeitsmodell Hochqualifizierter Angestellter. Arbeitspapier Nr. 44. Universität Bremen.

Menez, Raphael/Munder, Irmtraud/Töpsch, Karin (2001): Qualifizierung und Personaleinsatz in der IT-Branche. Arbeitsbericht Nr. 200. Stuttgart: TA-Akademie.

Menez, Raphael/Töpsch, Karin 2003: Arbeitsregulation in der IT-Branche – Organisationsbedarf und Organisationsfähigkeit aus gewerkschaftlicher Sicht. Arbeitsbericht Nr. 231. Stuttgart: TA-Akademie.

Moldaschl, Manfred/Voß, G. Günther (Hrsg.) (2002): Subjektivierung von Arbeit. München/Mering: Hampp.

Moldaschl, Manfred (2002): Ökonomien des Selbst. Subjektivität in der Unternehmergesellschaft. S. 29-62. In: Klages, Johanna/Timpf, Siegfried (Hrsg.), Facetten einer Cybergesellschaft. Subjektivität der Eliten, Netzwerke, Arbeit, Ökonomie. Hamburg: VSA.

Mückenberger, Ulrich (2002): Gesellschaftliche Strukturveränderungen erfordern veränderte Konzepte der Gewerkschaften. Vortrag auf der Jahrestagung der Kooperationsstelle Hochschule - Gewerkschaften Oldenburg „Gewerkschaften im Veränderungssog" am 25. 01. 2002.

Mückenberger, Ulrich (1985): Die Krise des Normalarbeitsverhältnisses (1. Teil). Zeitschrift für Sozialreform (31) 7: 415-434.

Müller-Jentsch, Walter (1997): Soziologie der industriellen Beziehungen. Eine Einführung. Frankfurt: Campus.

Pongratz, Hans/Voß, G. Günter (2003): Arbeitskraftunternehmer. Erwerbsorientierungen in entgrenzten Arbeitsformen. Berlin: edition sigma.

Schönberger, Klaus/Springer, Stefanie (2003): Handlungsräume subjektivierter Arbeit in der Wissensökonomie. Eine Einführung. In: diess. (Hrsg.): Subjektivierte Arbeit, Mensch, Organisation und Technik in einer entgrenzten Arbeitswelt. Frankfurt: Campus [Im Druck].

Schumann, Michael (2001): Sozialstrukturelle Ausdifferenzierung und Pluralisierung der Solidarität. WSI-Mitteilungen (54) 9: 531-537.

Streeck, Wolfgang (1987): Vielfalt und Interdependenz. Überlegungen zur Rolle von intermediären Organisationen in sich ändernden Umwelten.

Kölner Zeitschrift für Soziologie und Sozialpsychologie (39), 3: 471-495.
Töpsch, Karin/Menez, Raphael/Malanowski, Norbert (2001): Ist Wissensarbeit regulierbar? Arbeitsregulation und Arbeitsbeziehungen am Beispiel der IT-Branche. Industrielle Beziehungen (8) 3: 306-332.
Trautwein-Kalms, Gudrun (1995): Ein Kollektiv von Individualisten? Interessenvertretung neuer Beschäftigtengruppen, Berlin: edition sigma.
Voß, G. Günter (1998): Die Entgrenzung von Arbeit und Arbeitskraft. Eine subjektorientierte Interpretation des Wandels von Arbeit, in: Mitteilungen aus der Arbeitsmarkt- und Berufsforschung 3: 473-487.
Wiesenthal, Helmut/Clasen, Lothar (2002): Gewerkschaften in Politik und Gesellschaft: Von der Gestaltungsmacht zum Traditionswächter? Erscheint in: Schroeder, Wolfgang/Weßels, Bernhard (Hrsg.): Gewerkschaften in Politik und Gesellschaft. Opladen: Westdeutscher Verlag.
Wolf, Harald/Mayer-Ahuja, Nicole (2002): „Grenzen der Entgrenzung von Arbeit" – Perspektiven der Arbeitsforschung. SOFI-Mitteilungen Nr. 30: 197- 205.
Zenke, Ulrike (1999): Qualifizierte Dienstleistungsarbeit und die Organisat ionsperspektiven der Gewerkschaften. Arbeitsbericht Nr. 132. Stuttgart: TA-Akademie.

Esther Ruiz Ben und Dietlinde Quack

Ökologische Aspekte von mobiler Arbeit und e-learning

Die Basisinnovationen im Informations- und Kommunikationsbereich (IuK Bereich) zählen zu den wichtigsten Entwicklungsfaktoren post-industrieller Gesellschaften, dennoch werden auch der Grenznutzen des Wohlstands in westlichen Gesellschaften sowie die ökologischen Nebenwirkungen immer sichtbarer (vgl. Anders 1980, Beck 1986, Joas 1988, Beck et al. 1996). Wie bei anderen Technologien vorheriger Innovationszyklen ist auch die Entwicklung zur Informationsgesellschaft im wesentlichen von wirtschaftlichen Zielen angetrieben.

Soziale und ökologische Aspekte treten daneben stark zurück bzw. werden nur mit zeitlicher Verzögerung wahrgenommen. Die Informationsgesellschaft wird durch implizite Risiken gekennzeichnet, denn die Innovationen der IuK-Technologien (IKT) bringen nicht intendierte und methodisch schwer analysierbare Nebenwirkungen nicht nur sozialer, sondern auch ökologischer Natur mit sich (z. B. Rebound Effekte[1]). Glotz (2001) identifiziert in seiner Charakterisierung der digitalen Gesellschaft vier Haupttendenzen: Dematerialisierung, Beschleunigung, Dezentralisierung (Just in time, Outsourcing) sowie Globalisierung. Diese werden wiederum in den verschiedenen Teilsystemen der Gesellschaft (Arbeitsmarkt, Bildungssystem, Politik, Rechtssystem, Handelssystem, Sozialsicherungssystem, Konsumsystem) mit ihren jeweiligen unterschiedlichen Grundlogiken erweitert. Die konkreten Auswirkungen lassen sich auf zwei Ebenen betrachten: Zum einen spricht man von direkten Effekten, wenn diese direkt an die Produktion, den Betrieb und die Entsorgung von Computern, Mobilfunktelefonen oder der Netzinfrastruktur, also an die IuK-Technologien und deren Nutzung gebunden sind. Indirekte Effekte, zum anderen, sind beispielsweise der Transport per Internet bestellter Bücher oder das Nutzerverhalten bei Online-Buchungen.

In unseren Beitrag wollen wir anhand verschiedener Studien über soziale, ökonomische und ökologische Aspekte von e-learning in verschiedenen Kontexten und mobiler Arbeit den Stand der Diskussion über die Nachhaltigkeit in diesen Bereichen zeigen.

Einleitung

Insbesondere im IuK-Bereich werden zunehmend technische Innovationen bzw. Telematikanwendungen umgesetzt, um Telekooperation und Telearbeit innerhalb der Organisationen zu ermöglichen. Die Unternehmen möchten dadurch ihre Produktivität erhöhen und eine dynamische effektive Positionierung im Konkurrenzfeld sicherstellen. Damit werden eine ständige Erreichbarkeit, der Zugriff auf Informationen, Datenaustausch und EDV-gestützte Zusammenarbeit ermöglicht, von den Mitarbeiterinnen und Mitarbeitern wird aber auch eine erhöhte Flexibilität erwartet (s. dazu Baukrowitz und Boes 2000; Sennett 1998; Voß 2001). Bezogen auf soziale sowie Umweltaspekte werden große Hoffnungen mit der Anwendung von IuK-Technologien im Bereich Telearbeit verknüpft (vgl. z. B. Gesi 2002, Irani et al. 1999). Insbesondere handelt es sich um

die Erwartung von Dematerialisierungs-Effekten[2], Verkehrsreduktion, die Ermöglichung selbstbestimmter Arbeits- und Lebensformen, eine bessere Integration von Arbeit und Leben und die Vereinbarkeit von Familie und Beruf. Allerdings wird in verschiedenen Studien auch auf die Risiken hingewiesen (vgl. z. B. Griesshammer et al. 1997, OECD 2001, Di Martino 2001, Brandl und Hildebrandt 2001): Erhöhte Umweltbelastungen infolge von Rebound-Effekten durch Überkompensation der Umwelteffizienz, Desintegration, Segmentierung, Arbeitsintensivierung und Risiko erhöhter Kontrollintensität stehen hier im Vordergrund. Brandl und Hildebrandt (2002) weisen noch darauf hin[3], dass die Erfordernis, Arbeitstätigkeit, Qualifikation und auch Arbeitszeiten selbst zu steuern, tendenziell den zeitlichen und mentalen Freiraum verringert für ein hinsichtlich sozial-ökologischer Folgen reflektiertes Verhalten. Andererseits verändern sich auch die Qualifikationsanforderungen an Mitarbeiterinnen und Mitarbeiter: Die neue Arbeitskultur erfordert Akteure, die neben ihren fachlichen Fähigkeiten vermehrt auch über soziale Kompetenzen wie Kommunikationsfähigkeit, Empathie und ein Verständnis zwischenmenschlicher Interaktionen verfügen. Insbesondere aber die Bereitschaft zum lebenslangen Lernen, die durch IuK Innovationen bzw. durch e-learning Entwicklungen unterstützt wird. Betrachtet man die e-learning Angebote in Unternehmen und Betrieben, so ergibt sich ein widersprüchliches Bild: Viele große und international tätige Unternehmen nutzen Multimedia und Internet, um ihre Mitarbeiterinnen und Mitarbeiter ganz gezielt und *on-demand* mit Wissen und Informationen zu versorgen[4]. Anstatt umständlicher Fortbildungsmaßnahmen in Schulungszentren soll die Weiterbildung direkt am Arbeitsplatz und just-in-time stattfinden. In den kleineren Unternehmen haben dagegen die neuen Lern-Technologien noch kaum Einzug gehalten (Unicmind 2002).

Direkte Auswirkungen von IuK-Technologien und deren Anwendungen

Mittlerweile wird zunehmend deutlich, dass die Innovationen der IKT nicht intendierte und methodisch schwer analysierbare Nebenwirkungen mit sich bringen. Gesellschaft, Wirtschaft und Umwelt – kein Bereich ist von Wirkungen der IKT und ihrer Anwendungen ausgenommen. Zu den direkten Effekten gehören beispielsweise

- als Teil der ökologischen Dimension Schadstoffemissionen und Energieverbräuche und
- als soziale Dimension der Zugang zu Computer und Internet und mögliche gesundheitliche Auswirkungen (z. B. im Bereich Mobilfunk durch Elektrosmog) sowie
- als ökonomische Dimension Investitionen in den IuK-Sektor und die Entwicklung neuer Unternehmenstypen .

Die Betrachtung der ökologischen Dimension zeigt, dass sich auch hinter vermeintlich immateriellen Produkten (z. B. einer Videokonferenz) physikalische Produkte (Monitor, Netzinfrastruktur etc.) verbergen, die in industriellen Prozessen hergestellt werden, Energie für ihren Betrieb benötigen und nach Ende der Nutzungsdauer zur Entsorgung anfallen. Diese konventionellen Industrieprozesse widerlegen das bei der Chipherstellung im Reinraum vermittelte Bild einer sauberen Technologie.

Doch nicht nur die Wirkung auf Ökologie und Ökonomie, auch die sozialen Effekte der IKT sind inzwischen deutlich sichtbar: So ist die Mehrzahl der Internetnutzer in Deutschland männlich und mittleren Alters und hat einen hohen Grad an formeller Schulbildung sowie ein hohes Einkommen. Dieses Bild ist trotz leichter Veränderungen bezüglich des Geschlechteranteils an der Internetnutzung in den letzten Jahren stabil. Das Phänomen *Digitale Spaltung,* im Englischen *Digital Divide*, hat vor allem die Wirkung, dass sie die Partizipationsmöglichkeiten bestimmter Bevölkerungsgruppen einschränkt. Dies kann Nachteile zur Folge haben, beispielsweise hinsichtlich der Berufschancen und Bildungsmöglichkeiten, aber auch hinsichtlich der Beteiligung an demokratischen Prozessen. Die digitale Spaltung kann – mit Blick auf die Entwicklungsländer – auch ganze Nationen treffen.

Indirekte Auswirkungen von IuK-Technologien und deren Anwendungen

Neben direkten Effekten spielen auch so genannte indirekte Effekte von IKT eine wichtige Rolle in den Veränderungsprozessen der Informationsgesellschaft. Schließlich sind IuK-Anwendungen Dienstleistungen, die durch die Kombination von Hardware, Software und Vernetzung nutzbar werden. Dazu zählt die Bestellung und der Kauf von Waren über das Internet (e-commerce) genauso wie die Teilnahme an webbasierten, interaktiven Lehrgängen (e-learning), aber auch die mögliche Erreichbarkeit überall und zu jeder Zeit.

Intendierte indirekte Effekte sind beispielsweise der Transport eines über das Internet gekauften Buches nach der Bestellung. Dazu gehört auch die Dematerialisierung von Produkten. Dematerialisierung, d.h. der Ersatz physikalischer Produkte durch elektronisch vermittelte Dienstleistungen, die sich nicht – in Form von Papier, Geräten, Transporten etc. – wieder vergegenständlichen, ist hinsichtlich der Reduktion von Umweltauswirkungen eine der größten Hoffnungen, die auf IKT gesetzt werden.

Wesentlich stärker ins Gewicht fallen dürften demgegenüber aber die *nicht intendierten* indirekten Effekte von IuK-Anwendungen. So ermöglicht der Einsatz von IKT zwar Effizienzerhöhungen, verringert in der Regel aber den Ressourcenverbrauch nicht im gleichen Maße. Es kann sogar zu Rebound-Effekten kommen, wenn die Wachstumsrate des Verbrauchs höher ist als die Effizienzsteigerung.

Die neuen Möglichkeiten durch IuK-Technologien können auch zu Veränderungen in Lebensstilen und Konsummustern führen. Ein Beispiel ist e-commerce. Hier entstehen im Internet neue Marketing- und Vertriebskanäle, die zusätzliche Nachfrage nach Produkten generieren und entsprechend höhere Umweltauswirkungen zur Folge haben. Der bequeme Zugang zu Informationen über Reisegebiete, beispielsweise Reiseangebote und spontane Buchungsmöglichkeiten, lässt die begründete Vermutung zu, dass bestehende Konsumtrends durch Online-Angebote

verstärkt werden. Das heißt: Die Menschen reisen häufiger, über kürzere Zeit und längere Entfernungen. Andererseits unterstützt e-commerce aber auch den nachhaltigen Konsum: Mit der Erweiterung des Angebots können die individuelle und kollektive Verbrauchermacht gestärkt, Protestaktionen vereinfacht, eine größere Transparenz der Märkte ermöglicht und die Verbraucherbildung erleichtert werden.

Besonders für die indirekten Effekte von IuK-Anwendungen lassen sich aber zum jetzigen Zeitpunkt weder die Chancen noch die Risiken quantitativ abschätzen, was dazu führt, dass man sie auch nicht eindeutig gegeneinander abwägen kann. Weil die Prozesse, die zu diesen indirekten Effekten führen oder durch diese Effekte verändert werden, sehr komplex sind, und weil die gesellschaftlichen Subsysteme, auf die sie wirken, stark ausdifferenziert sind, sind diese Effekte zudem schwer zu steuern. Um diesem Ziel – im Sinne einer nachhaltigen Entwicklung – näher zu kommen, bedarf es zukünftig erheblicher Forschung.

Das Beispiel mobile Arbeit

Die Entwicklung der Industriegesellschaft hin zur Informationsgesellschaft ist mit einem tiefgreifenden Strukturwandel des Arbeitsmarktes verbunden. Dieser Strukturwandel ist u.a. gekennzeichnet durch einen Wandel der Erwerbsformen, Arbeitszeitflexibilisierung, erhöhte Qualitätsanforderungen sowie strukturelle Arbeitslosigkeit. Gleichzeitig lässt sich beobachten, dass sich die Alters- und Qualifikationsstruktur der Arbeitnehmer, die Lebensstile und Haushaltsstrukturen und der Qualitätsanspruch an den Arbeitsplatz ändern.

Die Bedeutung der IKT selbst liegt dabei vor allem darin, dass sie durch sozio-ökonomische Effekte ausgelöste Veränderungsprozesse ermöglicht und verstärkt. Informationsübermittlung und Informationsverarbeitung fusionieren immer stärker, und Telekommunikations- und Informationstechnologien verschmelzen zu Telematikanwendungen. Dies geschieht auf der Ebene der Endgeräte oder Anwendungen, aber vor allem durch den Aufbau einer Netzinfrastruktur, die informationsverarbeitende Endgeräte so verbindet, dass sie miteinander kommunizieren können (z. B. über das Internet).

Telematikanwendungen im Bereich mobile Telearbeit bezeichnen IKT-Anwendungen, die die zeit- und ortsunabhängige Arbeit von Personen unterstützen, die arbeitsbedingt sehr mobil sein müssen. Der Begriff mobile Arbeit bezieht sich dabei auf eine Arbeit, bei der die Arbeitszeit nicht ständig an einem Arbeitsort verbracht wird, sondern an wechselnden Orten, und der arbeitende Mensch zeitweise, i.d.R. unterwegs, von einer räumlichen Basis entkoppelt ist. Die Arbeit von zu Hause aus rechnet dabei nicht zur mobilen Arbeit, hingegen die Arbeit während geschäftlicher Reisen (z. B. in Zügen, auf Flughäfen, in Hotels, in Tagungsräumen), an Kundenstandorten oder in dezentral bereitgestellten Büroräumen (u.a. *hot desking*).

Von Telematikanwendungen im Bereich mobiler Telearbeit wird erwartet, dass sie die Erreichbarkeit, den Zugriff auf Informationen (z. B. Zugang zu Intra- und Internet, aber auch auf mitgeführte Daten), Datenaustausch und EDV-gestützte Zusammenarbeit (z. B. via Telekonferenzen) für den Anwender und seine Kooperationspartner zuverlässig sicherstellen. Im Englischen wurde für die extreme Ausprägung, des *jederzeit und überall*, der Begriff *ubiquitous computing* geprägt. Noch ist die allgegenwärtige Vernetzung nicht umgesetzt, insbesondere nicht für die Übermittlung großer Datenmengen. Allerdings ist hier z. B. durch den Aufbau von WLAN-Hotspots und den Aufbau des UMTS-Netzes ein stetiger Ausbau zu erwarten. Die steigende Nachfrage durch Unternehmen und berufliche Nutzer kann dabei als einer der treibenden Faktoren angesehen werden. Hintergrund ist das Problem der kritischen Masse, die erreicht werden muss, damit eine Vernetzung hinreichend dicht und verteilt ist, um für potenzielle Anwender attraktiv zu sein. Die technologischen Trends Standardisierung, Miniaturisierung, Preisverfall und Integration bei den Endgeräten erlauben eine immer komfortablere mobile Arbeitsweise mit z. B. Notebooks, PDAs, Smartphones, transportablen Scannern, Druckern, Kopierern etc. Daneben spielt die Bereitstellung von EDV-Tools für Kooperation (z. B. *Application Sharing*) und Datenverarbeitung (z. B. *Application Service Providing*) eine immer größere Rolle.

Die mobile Telearbeit ist zusammen mit der heimbasierten Telearbeit die häufigste Form von Telearbeit. EcaTT (2000) hat für Deutschland ermittelt, dass 1999 1,5 % der arbeitenden Bevölkerung - dies entspricht 540.000 Menschen - als mobile Telearbeiter tätig waren. Damit gibt es genau so viele mobile wie heimbasierte Telearbeiter. Für ganz Europa waren 1999 von insgesamt 5,5 Millionen Telearbeitern 2,3 Millionen mobile Telearbeiter (Ecatt 2000). Gleichzeitig wird gerade im Bereich mobile Telearbeit ähnlich wie für Call Center in den nächsten Jahren ein Anstieg im zweistelligen Prozentbereich prognostiziert. Dies würde den Trend der letzten Jahre bei der gesamten Telearbeit fortsetzen.

Bisherige Untersuchungen konzentrieren sich im wesentlichen auf heimbasierte oder alternierende Telearbeit. Die Studie „Umweltschutz im Cyberspace“ (Griesshammer et al. 1997) des Öko-Instituts konnte beispielsweise zeigen, dass das Reduktionspotenzial im Bereich Verkehr bei heimbasierter Telearbeit

Die Autoren

Dr. Dietlinde Quack ist seit vier Jahren wissenschaftliche Mitarbeiterin im Bereich Produkte & Stoffströme des Öko-Institut e.V.. Ihr Arbeitsschwerpunkt liegt im Bereich der Bewertung von Produkten und Dienstleistungen sowie Produktentwicklungsprozessen unter Nachhaltigkeitsgesichtspunkten. Ein besonderer Fokus liegt auf dem Themenfeld *Information und Kommunikation*, insbesondere IuK-Technologien und deren Anwendungen.

Dr. Esther Ruiz Ben ist promovierte Soziologin und wissenschaftliche Mitarbeiterin am Institut für Informatik und Gesellschaft der Albrecht-Ludwigs-Universität Freiburg. Forschungsarbeiten und Veröffentlichungen im Bereich Frauen in der Informatikausbildung und im Professionalisierungsprozess der Software-Entwicklung, aus nationaler und internationaler Perspektive. Lehrbeauftragte der Fakultät für Informatik der Albrecht-Ludwigs-Universität Freiburg im Bereich Informatik und Gesellschaft.

relativ gering ist und die tatsächlichen Einsparungen aufgrund unterschiedlicher Faktoren (z. B. keine Bündelung von Wegen mehr möglich) noch darunter liegen. Zudem führt die Notwendigkeit, zwei Arbeitsplätze auszustatten, zu einer weiteren Kompensation potenzieller Umweltentlastungen. Die bisherige Erfahrung zeigt eindeutig, dass Telearbeit von Unternehmen und Arbeitnehmern bewusst gestaltet werden muss, damit die erwarteten Vorteile realisiert und befürchtete Nachteile vermieden werden können. So können beispielsweise die Erwartungen im Hinblick auf Umweltentlastungen nur erfüllt werden, wenn sie gezielt in Zielsetzung und Planung berücksichtigt werden.

Unklar und bisher noch wenig untersucht ist die Frage, ob die Vor- oder Nachteile mobiler Telearbeit überwiegen und wie mobile Telearbeit gestaltet sein müsste, damit sie zu einer nachhaltigen Entwicklung beiträgt. Zur Zeit lassen sich diese Fragen nicht eindeutig beantworten – zu viele Unterfragen sind noch offen: Inwiefern ändert sich das Mobilitätsverhalten durch mobile Telearbeit? Welche Umweltauswirkungen sind mit der Bereitstellung von Endgeräten und Infrastruktur verbunden? Bestehen Gesundheitsgefahren durch drahtlose Vernetzung und Endgeräte? Welche Lebens- und Konsumstiländerungen sind mit mobiler Telearbeit verbunden? Welcher Einfluss besteht im Hinblick auf Arbeitsqualität und –intensität? Wie kann mobile Telearbeit die Vereinbarkeit von Familie und Beruf unterstützen? Inwiefern besteht die Gefahr der digitalen Spaltung?

Um sicherstellen zu können, dass mobile Telearbeit gemäß den Kriterien einer nachhaltigen Entwicklung ausgestaltet und angewendet wird, muss hier noch erhebliche Forschungs- und Entwicklungsarbeit geleistet werden. Wesentlich sind dabei geeignete Kriterien und die Integration der drei Nachhaltigkeitsdimensionen in die Entwicklung von Anwendungen für die mobile Telearbeit und in die betriebliche Umsetzung unter Einbezug der beteiligten Akteure wie Nutzer oder Unternehmen.

Das Beispiel e-learning

Mit dem Einsatz virtueller Lehre verändert sich die frühere exklusive Rolle der Hochschulen als Produzenten, Anwender und Verbreiten von Wissen. Andere Institutionen und private Organisationen werden dabei zu Akteuren. Das Weiterbildungsangebot im IT-Bereich ist in den letzten Jahren enorm angestiegen. Das liegt vor allem am Fachkräftemangel bzw. dem *Mismatch* (Licht et al. 2002) in der IT-Branche[5], der zum großen Teil durch Weiterqualifizierung von Quereinsteigern gelöst wird (Dostal 2001; OECD 2002), aber auch an den sich rasant verändernden kurzen Innovationszyklen und der entsprechenden Halbwertszeit des Wissens in diesem Feld. Öffentliche sowie private Bildungsträger, die zum großen Teil e-learning anbieten, können flexibler als die Hochschulen auf die Anforderungen des IT-Arbeitsmarkts reagieren. Die Hochschulen sind jetzt im Konkurrenzfeld und müssen ihre Studienangebote an die raschen Veränderungszyklen der Informationsgesellschaft anpassen. Vor allem mehr Flexibilität, schnelle Anpassungsfähigkeit an Qualifikationsansprüche von Arbeitsmarkt und Weiterbildung sowie Kostensparen und eine dynamische Kooperation mit der Industrie sind als wesentliche Aspekte zu beachten, in denen die Curricula geändert werden sollten. Ducatel et al. (2000, p. 13f) nennen folgende Chancen des Einsatzes der IuK-Technologien in der Ausbildung:

Größere Flexibilität dieser Lernwerkzeuge durch:

- Veränderungen der Zeiteinteilung und der Allokation des Lernens,
- neue Verteilungspraktiken,
- veränderte Formen der Informationsbenutzung.
- die Möglichkeit, Arbeit und Lernen z. B. mit Familienverantwortung zu kombinieren.

Dennoch behaupten Kirkup & Jones (2000), diese neuen Lernmethoden:

- seien teurer und komplexer zu produzieren,
- seien in ihrer Effektivität umstritten,
- erforderten individuelles Lernen und Organisation,
- seien häufig an männliches Eigentum von IKT im Haushalt gebunden (stärkstes Beispiel: Internet).

Empirische Untersuchungen (Vir 1999, Blum 1998, Prümmer 1997, Spennemann 1996) von existierenden Systemen und Designs für computerunterstütztes Lernen haben *Gender*-basierende Unterschiede auf verschiedenen Ebenen gezeigt:

- technologiebasierte und –zentrierte Modelle des Lehrens und Lernens,
- nicht wertneutrale Sprache, Terminologie und Metaphoriken,
- mangelnde Unterstützung der Lernmotivation, geringer Zugang zu Ressourcen, fehlendes Kennenlernen der Kontexte, der Art der Inhalte und Lern- und kognitiven Stildifferenzen.
- Designs, die abstrakte, formale Operationen ohne Kontextbeziehungen verwenden, und damit rationale kognitive Lerntypen gegenüber konkret und assoziativ kognitiven Lernstilen privilegieren.

Andererseits zeigen manche Studien, dass e-learning Angebote attraktiv für Frauen sind. Nicht nur Flexibilität und Zeitsouveränität werden hier positiv bewertet, sondern auch die Möglichkeit, sich *gendered* Kontexten in männlich konnotierten Bereichen (Informatik und Ingenieurwissenschaften) zu entziehen (Gfrerer & Pauschenwein 2002). e-learning Angebote eröffnen, nach einer Studie über die Strukturchancen für Frauen im Bereich Multimedia, gute Perspektiven für die Beteiligung von Frauen in diesem IT-Bereich:

> *„Eröffnen sich alternative, frauen-/arbeitnehmerinnenfreundliche Lernsettings (Zeit- und Raumsouveränität), wie z. B. partielles Telelearning oder Weiterbildung in Teilzeit, treten Frauen auch in technisch ausgerichtete Qualifizierungsmaßnahmen ein, absolvieren sie offensichtlich erfolgreich und erschließen sich sehr gute*

Perspektiven auf dem Arbeitsmarkt (unter der Maßgabe räumlicher und zeitlicher Flexibilität)."[6]

Entscheidend ist neben dem Inhalt der Angebote[7] und der Unterstützung der Dozentinnen und Dozenten[8] auch die Berücksichtigung der kulturellen Gegebenheiten in den verschiedenen Ländern. Gibson behauptet, bezüglich der teilweise zu beobachtenden steigenden Präsenz von Frauen in e-learning Angeboten der Ingenieurwissenschaften an Hochschulen Irlands, dass auch kontextuelle und konjunkturelle Faktoren, die länderspezifisch sind, in der Analyse berücksichtigt werden müssen und plädiert für eine tiefere und ausführliche Untersuchung dieses noch unberücksichtigen Faktors[9].

Dematerialisierungsfaktor „Faktor 10"

Im Projekt „Factor 10 Visions" der Open University in UK wurden zwei ähnliche Kurse, ein *print-based* und ein *internet-based* Kurs, miteinander verglichen. Die Studie ergab, dass, obwohl die Teilnahme an einen Online-Kurs zur Reduktion des Energieverbrauchs sowie der CO_2-Emisionen aufgrund geringerer Personentransporte geführt hat, sie gleichzeitig auch eine Steigerung der Computernutzung und des Papierverbrauchs bewirkt hat. Basis dieses Vergleichs war das Potenzial für „Factor 10", also eine Verringerung auf ein Zehntel des Ressourcenkonsums und der CO_2-Emissionen. Auf der einen Seite wurde festgestellt, dass das papierlose Büro eher eine Illusion bleibt, andererseits sind weitere indirekte Effekte mit dem Einsatz von Internet Kursen verbunden: Während für manche Teilnehmerinnen und Teilnehmer der Kurs eine Art Katalysator für deren *Internet literacy* wurde und damit Personentransporte reduzierte, zeigte gerade dieses neues Wissen für andere Teilnehmer genau den gegenteiligen Effekt: Reisen wurde zugänglicher und billiger durch das Internet und damit häufiger (Hilty/ Gilgen 2001).

In Deutschland gibt es keine Studie dieser Art und die indirekten Effekte des Einsatzes von e-learning bleiben daher noch unbekannt. Die Strategie des BMBF für das e-learning in der beruflichen Bildung wird von der Problematik des Fachkräftemangels im IT-Bereich geprägt. Vorrangig bleiben der Zugewinn von Ausbildungskapazitäten sowie die Verbesserung von Weiterbildungsangeboten im Multimedia-Bereich und im IT-Sektor[10]. Dennoch hatte der Einsatz von e-learning Angeboten im Hochschulbereich in den letzten Jahren finanzielle Priorität für das Ministerium, wobei insbesondere im Hinblick auf die Konkurrenz ausländischer Universitäten v.a. in den USA die Förderung virtueller Lehrangebote sowie die Stärkung der IT-Ausbildung programmatische Hauptpunkte darstellen (Wischkowski 2001). Bezogen auf die bundesdeutschen Hochschulen und Universitäten existieren an manchen technischen und wirtschaftswissenschaftlichen Fachbereichen positive Erfahrungen mit *Virtuellen Seminaren* und Fernstudiengängen im WWW, mit Tele-Tutorien und Online-Lerngruppen im Bereich Informatik (bspw. Viror[11]). Aber auch Probleme wurden dabei sichtbar. Denn die Teilnehmerinnen und Teilnehmer virtueller Lernumgebungen müssen sich viel stärker selbst motivieren als bisher, und auch das Feedback von Seiten der Lehrenden lässt oftmals noch zu wünschen übrig. Ganz zu schweigen von dem Aufwand, der mit der Herstellung und der Aktualisierung multimedialer Lernangebote einhergeht.

1 *Der Einsatz von IKT ermöglicht zwar Effizienzerhöhungen, verringert in der Regel aber den Ressourcenverbrauch nicht im gleichen Maße. Die Wachstumsrate des Verbrauchs kann sogar höher sein als die Effizienzsteigerung, der „Rebound Effekt".*

2 *der Ersatz physikalischer Produkte durch elektronisch vermittelte Dienstleistungen*

3 *Flexible Arbeitszeiten und der Zwang zur Gestaltung der eigenen Arbeitstätigkeit, zum selbstgesteuerten Qualifikationserwerb u.a.m. (Subjektivierung) lassen die Grenzen zwischen Erwerbsarbeit und Leben erodieren, zugleich steigt der Erholungsbedarf an. Flexible Arbeitszeiten fordern insbesondere ein aktives Zeitmanagement und eine effizienzorientierte Gestaltung der Lebensführung der Beschäftigten ein. [...] Der zeitliche und mentale Freiraum für sozial-ökologische Verhaltensweisen, z. B. für bewussten Konsum, verringert sich damit tendenziell. (Brandl und Hildebrandt 2002)*

4 *"(...) by early 2000, Cisco, Microsoft, Novell and other firms or private bodies had awarded more than 1,8 million credentials certifying IT skills to individuals. (...) There is still insufficient information on the exact role played by such certification programms in terms of IT employment (...)". (OECD 2002b)*

5 *„Eine Expertengruppe der Initiative D21 ermittelte 2001 einen Bedarf von mindestens 25.000 Hochschulabsolventinnen und –absolventen aus IT- Studiengängen, um den aktuellen Bedarf bis 2005 an IT-Fachkräften mit Hochschulausbildung zu decken. Studienabbruch und Studienzeiten stellen jedoch die Wachstumsbremse für die Informationstechnologie dar." In: Möller, I. (2002) Frauen in Zukunftsberufen – Chance Multimedia, Hamburg, Senat für Gleichstellung. S. 9.*

6 *Möller, I. (2002) Frauen in Zukunftsberufen –Chance Multimedia, Hamburg, Senat für Gleichstellung. S. 9.*

7 *Über diesen Aspekt s.: Schinzel, B. & Ruiz Ben, E. (2002) Gendersensitive Mediadidactics. In: SEFI Proceedings (ISBN 2-87352-046-9) S. 115-125.*

8 *Gfrerer, M. & Pauschenwein, J. (2002) Is the change from traditional teaching methods to ICT-based methods going to attract more female students to study engineering? In: SEFI Proceedings (ISBN 2-87352-046-9) S. 51-61.*
Bissell, C.; Chapman, D.; Herman, C.; Robinson, L. (2002) Some gender issues in the teaching of the Information and Communication Technologies at the UK Open University. In: SEFI Proceedings (ISBN 2-87352-046-9) S. 9-19.

9 *Gibson, I. (2002) A preliminary study of female student enrolment and attitudes to engineering and engineering education in the west of Ireland. . In: SEFI Proceedings (ISBN 2-87352-046-9) S. 61-69.*

10 *Wischkowski, H.G. (2001) Informationstechnik in Bildungspolitischen Programmen von Bund und Ländern. In: FIfF-Kommunikation 1/2001, S. 34. Zur Situation führender Anbieter von beruflichen Weiterbildung in Deutschland: http://www.luenendonk.com/html/marktanalysen_listen_weiterbildung.html Zur Situation in Firmen: http://www.unicmind.de/unicmindstudie2002.pdf Zur Situation in Spanien: http://www.teleformacion.edu/futuro.htm*

11 *Meyer, L. & Zimmer, C. (2001) Didaktischer Mehrwert durch Neue Medien in der Lehre? Erfahrungen und Ergebnisse aus der Televorlesung „Informatik und Gesellschaft". In: FIfF-Kommunikation 1/2001, S. 35-44*

Literatur

Anders, G.: Die Antiquiertheit des Menschen. München 1980

Baukrowitz, A., Boes, A (2000): Neue Arbeitskrafttypen in der IT-Industrie. Darmstadt. In:

http://staff-www.uni-marburg.de/~boes/texte/ARB-IT4.html (retrieved 2. 07. 2003)

Beck, U. (1986): Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt a.M.

Beck, U., Giddens, A., Lash, S.: Reflexive Modernisierung: Eine Kontroverse. Frankfurt a. M. 1996

Blum, K. D.: Gender differences in CMC-based distance education. In: Feminista, 2: 5, 1998

Brandl, S.; Hildebrandt, E.; Expertise „Arbeit und Ökologie" als Baustein des BMBF-Förderschwerpunktes „Sozial-ökologische Forschung". Wissenschaftszentrum Berlin. Berlin 2001

Di Martino, V.; The High Road to Teleworking. International Labour Organisation. Geneva 2001

Dostal, W.: Turbulenzen im Arbeitsmarkt. In: Informatik-Spektrum 24, 4, 2001, S. 207-217

Ducatel, K. et al. : Information Infrastructures or Societies? In: Ders. (Eds.): The Information Society in Europe. Maryland, Rowman & Littlefield Publ., S. 1-21. 2000

Electronic Commerce and Telework Trends. Benchmarking Progress on new ways of working and new forms of business across Europe. EcaTT Final Report. IST Programme. 2000

Gfrerer, M.; Pauschenwein, J.: Is the change from traditional teaching methods to ICT-based methods going to attract more female students to study engineering? In: SEFI Proceedings 2002, S. 51-61

Gibson, I.: A preliminary study of female student enrolment and attitudes to engineering and engineering education in the west of Ireland. In: SEFI Proceedings 2002, S. 61-69

Global e-Sustainability Initiative (GeSI); Information and Communications Technology. UNEP. Paris 2002

Glotz, P. Von Analog nach Digital: Unsere Gesellschaft auf dem Weg zur Digitalen Kultur. Huber Verlag, Stuttgart 2001

Grießhammer, R.; Gensch, C.-O.; Kupetz, R.; Lüers, A.; Seifried, D.; unter Mitarbeit von Buchert, M.; Führ, M.; Jülich, R.; Schmidt, G.; Tappeser, B.. Umweltschutz im Cyberspace? – Zur Rolle der Telekommunikation für eine nachhaltige Entwicklung. Eigenprojekt des Öko-Instituts e.V.. Freiburg/ Darmstadt 1997

Irani, A. ; Sampemane, S.; Gothoskar, S.. (ed.) Proceedings of the Workshop on Telework, Teletrade and Sustainable Development: The Indian Experience in a Global Context. Mumbai, India 15-16 November, 1999. Organised by NCST and UNU/INTECH with support from IDRC. Mumbai. 1999

Joas, H.: Das Risiko der Gegenwartsdiagnose. In: Soziologische Revue, 11. Jg., 1988

Kirkup, G.; Jones, A.: Information and Communication Technologies in Distance and Lifelong Learning. In : Ducatel, K. et al. (Eds.): The Information Society in Europe. Maryland, Rowman & Littlefield Publ. 2000, Pp. 201-233

Licht, G., Steiner, V., Bertscheck, I., Falk, M., Fryges, H.: IKT-Fachkräftemangel und Qualifikationsbedarf. ZEW Wirtschaftsanalysen, Bd. 61, Baden-Baden 2002

OECD: OECD Information Technology Outlook. ICTs and the Information Economy. Paris, OECD Publ. 2002, S. 166-167

Prümmer, C.: Frauen im Fernstudium. Frankfurt 1997

Sennett, R. (1998) Der flexible Mensch. Die Kultur des neuen Kapitalismus. Btb Verlag.

Spennemann, D. H. R.: Gender imbalances on computer access among environmental science students. 1996

Voss, G. (1998): Die Entgrenzung von Arbeit und Arbeitskraft. Eine subjektorientierte Interpretation des Wandels der Arbeit, in: Mitteilungen aus der Arbeitsmarkt- und Berufsforschung, 31.Jg., H. 3/98, S. 473 ff.

Wischkowski, H. G.: Informationstechnik in Bildungspolitischen Programmen von Bund und Ländern. In: FIfF-Kommunikation 1, 2001, S. 34.

Cornelia Gschmack

Von der Hochschule ins richtige Leben

und was man dazu wissen sollte

Liebe neue Kollegin, nach jahrelangem Durchlaufen der „Institution" Universität bist du nun hier: in einem wirklichen Unternehmen. Vollgepackt mit viel neuem und theoretischem Wissen springst du ins kalte Wasser – in die berufliche Praxis. Natürlich sind wir hier schon lange beschäftigt und kennen die betrieblichen Abläufe im Schlaf.

Wir mussten uns anfangs auch erst mal zurechtfinden und taten zweierlei: die Kollegen kennenlernen und, aufbauend auf unserem damaligen theoretischen Wissen, sei es aus der Lehre oder einem Studium, Theorie und Praxis miteinander kombinieren. Das Kennenlernen war einfach, da eine große Ähnlichkeit zwischen uns bestand: das Alter, die Interessen und das Wissen sowie das familiäre Umfeld. Aber das hat sich im Laufe der Zeit geändert, weil immer neue Kollegen und auch Kolleginnen dazu gekommen sind. Theorie und Praxis zu kombinieren, war auch nicht allzu schwer, denn vor 20 Jahren sah die EDV im gesamten Unternehmen so aus, wie es uns damals gelehrt wurde. Heute nennt man's Informationstechnologie und es gibt enorm viele Studien- und Ausbildungsgänge, die sich damit beschäftigen.

Was erwartet dich bei uns? Warum bist du überhaupt da? Ach ja, du hast dein Studium absolviert und möchtest endlich ran ans "richtige" Arbeiten, Geld verdienen und möglichst auch noch Karriere machen. Arbeitszeiten sind dir egal, du bist ja noch sehr jung, ungebunden und vom Studium her auch anderes gewohnt. Ich möchte dir nicht zu nahe treten, aber du wurdest als "Ersatz" für eine Kollegin eingestellt, die in den Ruhestand geht,

und übernimmst teilweise neue Aufgaben, aber auch alte von ihr. Technologien, die an der Uni schon längst als ausgestorben gelten. Und du kommst zu uns ins Team. Dass eines klar ist: Besserwisser können wir hier nicht brauchen. Aber wenn du wirklich zupacken kannst, dann bist du herzlich willkommen!
Deine neuen Kollegen und Kolleginnen

Der Berufsstart

Aller Anfang ist schwer! Und wer einen Brief wie diesen beim Arbeitsantritt bekommt, kann darin schon einiges mitschwingen spüren, auch Einstellungen, aus denen sich Konflikte ergeben könnten: Solidarität mit der Kollegin, Sorge um eine fachliche Konkurrenzsituation, ... Das muss nicht unbedingt sein. Dennoch können beim Berufsstart, und das trifft auch bei jedem Jobwechsel zu, zu Beginn einige Schwierigkeiten auftreten, die meist daraus resultieren, dass man – aus Sicht des Neueinsteigers bzw. der Neueinsteigerin – sich selbst und auch das neue Umfeld nur ungenügend kennt. Entsprechend lauert an vielen Stellen Konfliktpotenzial, das man leider oft erst erkennt, wenn es zu spät ist.

1. Siemens
2. IBM Deutschland GmbH
3. Fraunhofer-Gesellschaft
4. SAP AG
5. DaimlerChrysler AG
6. BMW Group
7. SuSe Linux AG
8. Sun Microsystems GmbH
9. Max-Planck
10. Lufthansa Systems Group GmbH

Abbildung 1: beliebte Arbeitgeber aus Sicht von Informatikstudierenden [1]

Unternehmen selbst sind ein komplexes Gebilde aus Aufgaben, Zielen und Menschen. Eines der wichtigsten Merkmale ist – und das in zunehmendem Maße je größer das Unternehmen ist – Arbeitsteilung. Zur Lösung der anfallenden Aufgaben werden Teams eingesetzt, die sich aus Mitarbeitern beider Geschlechter, unterschiedlichen Alters, sozialer und kultureller Herkunft und einer breiten Palette von Erfahrungen zusammensetzen. Hier ist vorauszusehen, dass es zu Missverständnissen kommt, zu Spannungen und tiefergehenden Konflikten, individueller oder zwischenmenschlicher Art.

Konflikte im Berufsleben

Konflikte[2] bringen Menschen in emotionale Spannungen, die belastend wirken und Verunsicherung sowie Ungewissheit auslösen. Konflikte am Arbeitsplatz führen in der Regel zu negativen Auswirkungen auf die Arbeitsleistung, die Arbeitsorganisation, den Arbeitsablauf und auf die Arbeitszufriedenheit.

Ein wesentlicher Aspekt ist dabei, dass Spannungen bzw. Konflikte in der Regel sowohl eine Sach- als auch eine Beziehungsebene haben: Es geht einerseits um Themen und äußere Streitpunkte und andererseits um Gefühle und Befindlichkeiten, Wahrnehmungen und Werthaltungen auf der Beziehungs- aber auch auf der persönlichen Ebene der Individuen, die den Konflikt miteinander austragen.

Niemand kann eine Auseinandersetzung über ein Thema führen, ohne dabei von seinen Einstellungen und seinem Selbstbild beeinflusst zu sein. Umgekehrt ist jede Auseinandersetzung auch eine Herausforderung an das Selbstbild und Selbstwertgefühl. Mit der Auseinandersetzung über berufliche Fragen geht deshalb stets auch eine Auseinandersetzung mit der eigenen Persönlichkeit und der Persönlichkeit der anderen einher.

Typische Beispiele aus der Berufspraxis

Ein Unternehmen[3] ist eine planvoll organisierte Wirtschaftseinheit, in der Sachgüter und Dienstleistungen erstellt und/oder abgesetzt werden. Kennzeichen sind: Kombination von Produktionsfaktoren (v.a. Menschen und Kapital), Prinzipien der Wirtschaftlichkeit bezogen auf Ergebnis und Ergebniserreichung, finanzielles Gleichgewicht und langfristig: Gewinn.

Ausgehend von dieser Definition sind nachstehende typischen Spannungsfelder vorhersehbar. Hier lauert insbesondere für Berufsanfänger Konfliktpotenzial:

- Ausgeprägtes theoretisches (aktuelles) Wissen trifft auf Praxiserfahrung und theoretisches (älteres) Wissen
- Theorie ist in die Praxis nicht immer umsetzbar, z.B. beim Einsatz neuer Technologien. Enthusiasmus allein reicht nicht aus. Ein gewisser Pragmatismus im Hinblick auf die Sinnfrage und die nachhaltige Wirksamkeit der Theorie sowie die Fähigkeit zu erkennen, was die Praxis am Leben hält, sind entscheidend.
- Unternehmen haben unterschiedliche Entwicklungsstände: Unternehmen lernen nicht, weil das Thema gerade "in" ist, sondern aufgrund von Veränderungsdruck. Wobei die Lernfähigkeit eines Unternehmens in Summe auf der Lernfähigkeit der darin befindlichen Einzelpersonen beruht. Dies führt dazu, dass Unternehmen nur sehr langsam lernen.
- Der Umgang mit Komplexität ist nur praktisch und nicht theoretisch erfahrbar. In der Wirklichkeit ereignen sich viele

Cornelia Gschmack

Cornelia Gschmack ist im IT-Bereich eines Automobilkonzerns mit Themen wie strategischem Management, Projektmanagement und Mitarbeiterqualifizierung betraut und hält daneben Vorträge und Kurse an Universitäten. Ihr Studium zur Dipl.-Wirt. Inf. (FH) und Dipl.-Kffr. (FH) hat sie parallel zu ihrer Tätigkeit in der Softwareentwicklung absolviert, diese Tipps sind Erfahrungen aus erster Hand.

HIN zu ihnen	WEG von ihnen	GEGEN sie
• Verlangen nach Beachtung, Anerkennung, gemocht werden • Kritik und Distanz als Zeichen der Ablehnung • Konkurrenz und Auseinandersetzung als Bedrohung	• Verlangen nach Unabhängigkeit und Selbstgenügsamkeit • Nähe und emotionale Hinwendung als Abhängigkeit und Einengung • Einfühlung und Verstehen anderer Menschen als Bedrohung • Vermeiden von Gefühlen durch Einsatz von Intellekt und Sachlichkeit	• tiefe Abneigung gegen andere Menschen • Bedürfnis, sie zu bekämpfen und zu unterwerfen/ erniedrigen • Annahme, der Mensch sei dem Menschen ein Wolf (homo homini lupus) • soziale Kontakte als Form des Kampfes • Verachtung und Vermeiden von Frieden und Harmonie

Tabelle 1: Gefühle, die anderen Menschen entgegengebracht werden

Dinge gleichzeitig und es zeigen sich Alltagsphänomene, die in den (Lehr-)Modellen meist nicht vorkommen.

- Begriffe werden unterschiedlich verwendet, es gibt unterschiedliche Alltagssprachen oder Dinge, über die man einfach nicht spricht. Begriffe wie Projekt und Projektleitung, Kompetenz und Verantwortung, Führung und Team, Systeme bedeuten im Unternehmensalltag etwas anderes als an der Hochschule.

- Die Form der Zusammenarbeit und deren Folgen lösen Spannungen aus, beispielsweise Einzelkämpfertum vs. Teamarbeit, Arbeitsteilung, Konkurrenz, Abhängigkeit von anderen Personen, Führung und Kontrolle, Rollenerwartungen und –widersprüche.

Studienabgänger wechseln von einer Unternehmens-Kultur (Uni/FH) in eine andere (Firma). Die Werte und Motivationen der darin befindlichen Menschen oder die Erwartungen der Unternehmensleitung, aber auch Regelungen für das Miteinander können anders sein: Arbeitszeitregelungen, Pünktlichkeit, Zielorientierung, Umgangsformen/Dresscodes, Verdienst, zusätzliche soziale Absicherungen und Benefits (Dienstwagen etc.), Sicherheit des Arbeitsplatzes, Arbeitsumfeld und Kollegen, Führungsstile, Umgang mit Macht und Anerkennung, ...

- Der Erfolgsdruck und die Erwartungen der Neueinsteiger an sich selbst sind sehr hoch. Viele Anfänger setzen sich selbst unter enormen Erfolgsdruck und verlieren dabei das Wesentliche aus den Augen – sie lassen sich blenden (oder werden geblendet) von Nebensächlichkeiten. Die Konzentration auf die Sache allein reicht dabei nicht aus – außerdem drängt sich die Frage auf, welche Erwartungen bei anderen Menschen geweckt werden.

- Im Unternehmen wird man damit konfrontiert, selbst Entscheidungen zu treffen, aber auch Entscheidungen anderer zu akzeptieren. Entscheidungen treffen heißt, zwischen Alternativen zu wählen, die positive aber auch negative Auswirkungen mit sich bringen, und dass man auch die Folgen der Entscheidung (er)trägt. Zielorientierung und unterschiedliche Zielausrichtungen sind dabei zu berücksichtigen, die sich aus den Zielinhalten oder den Personen ergeben, die die Ziele verfolgen.

- Ressourcen (Mitarbeiter, Finanzen, HW/SW, ...) werden meist gemeinsam genutzt. Daraus ergeben sich Differenzen bei der Verteilung/Zuordnung, den Zuständigkeiten sowie ein harter Wettbewerb um knappe Ressourcen.

- Spannungen ergeben sich oft aufgrund unterschiedlicher „Persönlichkeiten": Die Eigenart der Persönlichkeit, ihr Umgang mit Konflikten, das Vertrauen und Misstrauen, das anderen entgegengebracht wird, der Umgang mit bzw. Wunsch nach Macht und Einfluss.

- Kommunikation findet nicht nur auf der Sachebene statt. Über die Beziehungs-, Appell- und auch Selbstoffenbarungsseite [4] werden wesentlich mehr Botschaften übertragen. Was kommt davon tatsächlich beim Gesprächspartner bzw. der Gesprächspartnerin an? Manipulationsversuche werden glücklicherweise im Laufe der Zeit meist erkannt.

Mögliche Erklärungen

Es gibt viele Theorien über Konflikte. Nachfolgend eine kleine Auswahl von Ursachen, auch als Einladung zum individuellen Reflektieren.

1. Jeder Mensch nimmt seine Umwelt unterschiedlich wahr. Dies ist abhängig von den jeweiligen Personen, ihren Sinneseindrücken und Erfahrungen sowie den individuellen Standpunkten und Blickrichtungen.

2. Gefühle, die anderen Menschen entgegengebracht werden, lassen sich in drei Kategorien einteilen (siehe Tabelle 1).

3. Die Menschen haben unterschiedliche Einstellungen zu Beziehungen:

- kooperativ: Beziehungsgestaltung im Hinblick auf Nutzen für alle Beteiligten

- individualistisch: Beziehungsgestaltung im Hinblick auf eigene Unabhängigkeit
- konkurrierend: Beziehungsgestaltung im Hinblick auf eigenen Nutzen

4. Innerhalb verschiedener Altersgruppen lassen sich, aus psychologischer Sicht, spezifische Konfliktschwerpunkte feststellen. Diese Einteilung kann man im übertragenen Sinn auch auf die Berufserfahrung und Dauer der Unternehmenszugehörigkeit verwenden (siehe Tabelle 2)

Altersgruppe	*Konflikte kreisen um*
Schulkind	Auseinandersetzung mit Leistungsanforderungen und Rivalität
Jugendlicher	Entscheidungen für einen Beruf und Partner
Junger Erwachsener	Konkurrenz und Behauptung im Beruf, Aufbau einer Familie, Spannung zwischen Beruf und Familie, Schwerpunkte persönlicher Lebensführung
Älterer Erwachsener	Konsolidierung im Beruf, Entwicklung der Partnerschaft und der Kinder, Möglichkeiten eines neuen beruflichen oder privaten Anfangs, Verantwortung in der Gesellschaft, Lebenssinn und Transzendenz
Alter Mensch	Lebensaufgabe zum Abschluss bringen, sein eigenes Leben als sinnvoll erkennen, Erfahrungen an die nächste Generation weitergeben, sich auf den Tod vorbereiten

Tabelle 2: Berufserfahrung und Dauer der Unternehmenszugehörigkeit

Lösung von Konflikten

Konflikte am Arbeitsplatz frühzeitig aufzugreifen und einer Lösung zuzuführen ist ein wesentlicher Aspekt für eine erfolgreiche Zusammenarbeit. Wie in allen anderen zwischenmenschlichen Kommunikationsbereichen ist dieses aber häufig nur mit einer neutralen Klärungshilfe möglich, beispielsweise mit einem Mentor oder einer Vertrauensperson, und selbstverständlich nicht ohne persönliches Engagement aller Beteiligten. Verdrängung funktioniert meist nur kurzfristig. Manchmal ist allerdings auch keine wirkliche Lösung möglich.

1 http://www.forum-jobline.de/de/forum/karriere/berufseinstieg/top_arbeitgeber.html

2 Von einem Konflikt spricht man im allgemeinen dann, wenn zwei Handlungstendenzen (Alternativen, Verhaltensweisen, Bewertungen etc.) oder Motivationen (Wünsche, Anreize etc.) nicht zum gleichen Zeitpunkt verwirklicht werden können oder in sich gegensätzlich bzw. unvereinbar sind UND wenn die Notwendigkeit besteht, dazu Stellung zu beziehen.

3 unabhängig davon, ob es sich um ein Gewinn orientiertes oder ein Non-Profit-Unternehmen handelt

4 siehe Kommunikationsmodell von Schulz von Thun

Literatur

A. Hugo-Becker, H. Becker: Psychologisches Konfliktmanagement. dtv Verlag C.H. Beck, München, 2. Auflage 1996

K. Berkel: Konflikttraining – Konflikte verstehen, analysieren, bewältigen. Arbeitshefte Führungspsychologie (Hrsg. W. Bienert/E. Crisand), Sauer-Verlag, Heidelberg, 6. Auflage 1999

L. von Rosenstiel: Grundlagen der Organisationspsychologie, Schäffer-Poeschel Verlag, Stuttgart, 4. Auflage 2000

Claudia Eckert

Sicheres mobiles Arbeiten

Zwischen Wunsch und Wirklichkeit

Die zunehmende Nutzung des Internets für private und berufliche Zwecke sowie die neuen Möglichkeiten, die uns die Telekommunikation bietet, führen zu einer drastischen Veränderung unserer Arbeitswelt und unseres Alltags. Mit mobilen Endgeräten wie Laptops, Mobiltelefonen oder PDAs (Persönliche Digitale Assistenten) *und neuen Kommunikationsmöglichkeiten wie* GPRS, UMTS *und drahtlosen Netzen wie* WLAN *oder* Bluetooth *können Mitarbeiter von überall auf Unternehmensdaten zugreifen.*

Die Endgeräte verfügen in der Regel über verschiedene Möglichkeiten, um mittels mobiler, drahtloser Netze Zugriff auf das Internet oder auf andere öffentliche oder private Netze (z. B. das lokale Unternehmensnetz) zu erhalten. Einige der neueren Netztechnologien ermöglichen es darüber hinaus, dass ihre mobilen Benutzer spontan (z. B. bei einem Treffen mit Geschäftspartnern) ein Ad-hoc-Netz aufbauen und ohne eine vorab installierte Infrastruktur mit bekannten oder auch unbekannten Partnern bzw. Geräten Daten austauschen.

Mobiles Arbeiten eröffnet somit interessante Perspektiven für zukünftige IT-Anwendungen. Problematisch ist jedoch, dass diese technologischen Entwicklungen gleichzeitig auch eine Öffnung von Netzen zur Folge haben, durch die sich Unternehmen und Behörden zunehmend Angriffen aussetzen. Wer kennt sie nicht, die Warnungen vor virenverseuchten E-Mails und anderen Angriffen, die ganze Unternehmensnetze lähmen oder wichtige Daten vernichten. Welche Konsequenzen für die Sicherheit ergeben sich aus den technologischen Fortschritten, und wie gehen wir damit um?

In unseren normalen Lebensgewohnheiten haben wir Schutzvorkehrungen geschaffen, um uns vor Gefahren wie Unfällen, Diebstahl oder dem Eindringen in unsere Privatsphäre zu schützen. Mit der Einführung von Informations- und Kommunikationstechnologie (IuK) hat sich die Situation jedoch drastisch verändert. Bereits heute sind ca. 70 – 80 % der Menschen direkt oder indirekt von der Informationstechnik abhängig. Wir produzieren und verarbeiten Informationen zu wertvollem Wissen, um dieses sowohl privat als auch geschäftlich zu nutzen. Unser Wissen und unser Umgang mit Wissen hat neue Begehrlichkeiten geweckt und unsere vermeintliche Sicherheit massiv verändert. Zur Abwehr der neuen Sicherheitsbedrohungen wurden bereits viele technische Konzepte und Verfahren [C. Eckert 2002, B. Schneier 2001], wie Verschlüsselung, Firewalls, digitale Signatur, Biometrie oder Smartcards entwickelt. Es stellt sich nun die Frage, welche Auswirkungen die zunehmende Mobilität auf die Sicherheit der verarbeiteten Daten und Informationen und damit die Benutzer derartiger Systeme hat.

Mobile Kommunikation und mobiles Arbeiten

Die mobile Kommunikation (u. a. [C. Eckert 2002, J. Roth 2002]) ist aus dem heutigen Alltag kaum noch wegzudenken. Abbildung 1 gibt einen Überblick über die heute bereits im Einsatz befindlichen Technologien, zur mobilen Kommunikation und zum mobilen Arbeiten. Dazu gehört der mobile Zugriff auf das Internet via Handy ebenso wie der Netzzugang über ein „klassisches" Modem am Heimarbeitsplatz oder über einen Hot-Spot-Zugang z. B. im Flughafen. Im Folgenden werden die verschiedenen Technologien kurz erläutert.

Mobilkommunikation

Mobilfunknetze überspannen Länder und Kontinente. Sie ermöglichen so eine nahezu ungebrochene Erreichbarkeit von Kommunikationspartnern. Eine wichtige Rolle spielt hierbei der Mobilfunkstandard *GSM (Global System for Mobile Communication* [V. K. Garg, J. E. Wilkes 1999]), der alle Kontinente erreicht.

Das GSM-System zählt zu den Mobilfunksystemen der zweiten Generation (2G). Schaltet ein Benutzer sein Mobiltelefon ein, so bucht es sich über den nächstgelegenen Funkmast mit ausreichender Signalstärke beim zugehörigen Netz ein. Das Netz prüft, ob eine Berechtigung zur Nutzung seiner Dienste vorliegt. Mobilfunkteilnehmer können von beliebigen Orten aus anrufen bzw. angerufen werden, ohne dass der jeweilige Teilnehmer explizit seinen aktuellen Aufenthaltsort hinterlegen muss. Das Netz bestimmt den Aufenthaltsort des Teilnehmers automatisch, falls er sich irgendwo eingebucht hat. Das macht das mobile Telefonieren ja gerade so attraktiv und liefert eine einfach zu handhabende Basis für das entfernte mobile Arbeiten.

GPRS (General Packet Radio Service) ist die Technologie der 2,5-ten Generation. Da die Übertragung paketorientiert erfolgt, wird unter GPRS auf der Grundlage des übertragenen Datenvolumens und nicht nach Zeitdauer wie beim *klassischen* Telefonieren abgerechnet. Es eignet sich damit sehr gut zur Übertragung kleinerer Datenmengen oder von teil- und zusammensetzbaren Datenströmen, wie z. B. E-Mails. Natürlich kann die Nutzung der GPRS-Technologie auch schnell zu einem teuren Spaß werden, bedenkt man, welche großen Datenvolumina bereits heute mit E-Mails und deren vielfältigen Multi-Media-Anhängen versendet werden. Jedes GPRS- und auch UMTS-fähige Endgerät besitzt eine eigene IP-Adresse und ist somit ein Rechner im Internet. Mobile Teilnehmer können jederzeit online sein, sie sind aber dadurch auch in sehr starkem Maß Angriffen aus dem Internet ausgesetzt.

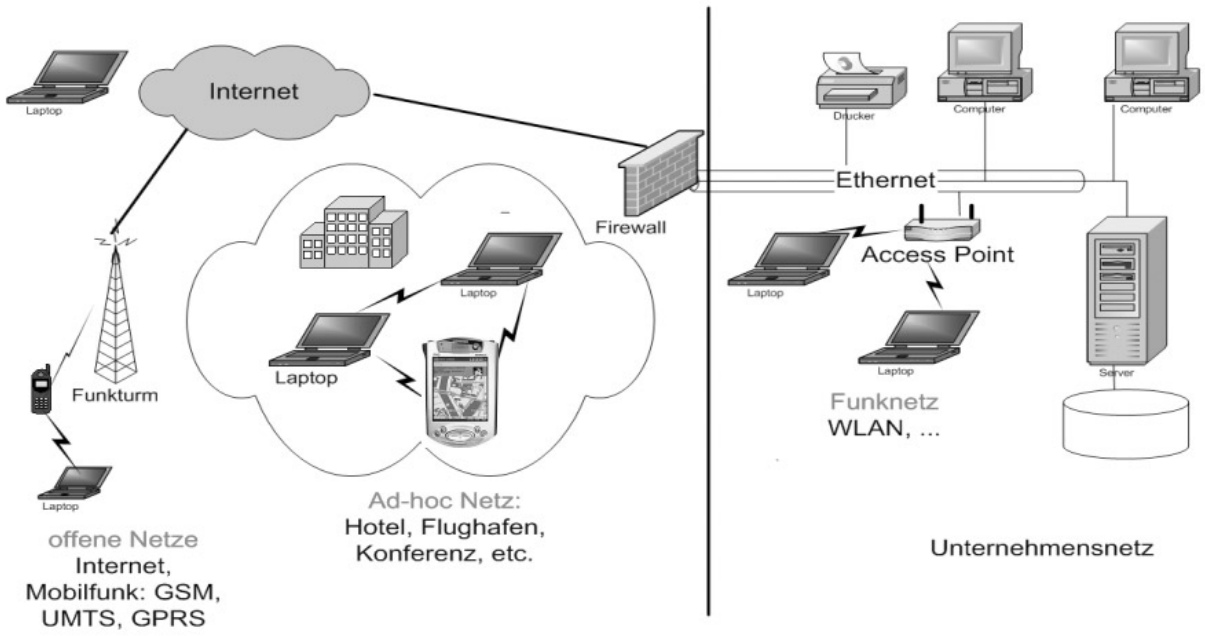


Abb. 1: Mobiles, vernetztes System

Mit *UMTS (Universal Mobile Telecommunication System)* kommt nunmehr die dritte Generation von Mobilfunksystemen zum Einsatz. UMTS bietet eine deutlich größere Bandbreite als die beiden Vorgänger-Technologien und soll erweiterte Telefonie-Fähigkeiten (Rich Telephony) mit gleichzeitiger Übertragung von Sprache, Bild und Ton ermöglichen. Weiterhin sollen bei dieser Bandbreite auch Audio- und Videodaten, beispielsweise ganze Filme, übertragbar sein, wodurch UMTS insbesondere für Video-Konferenzschaltungen attraktiv sein könnte.

Drahtlose Netze

Drahtlose lokale Funknetze, die *WLANs* (Wireless Local Area Networks) verbreiten sich mit einer rasanten Geschwindigkeit. Derartige Netze setzt man unter anderem zur Vernetzung von Gebäuden ein, oder in öffentlichen, stark frequentierten Bereichen *(Hot Spots)* wie Flughäfen, Bahnhöfen oder Einkaufszentren. Die lokalen Funknetze basieren in der Regel auf dem internationalen IEEE 802.11 Standard, der eine Datenkommunikation über das lizenzfreie *ISM (Industrial, Scientific, Medical)* Frequenzspektrum zwischen 2,4 und 2,48 GHz erlaubt und deshalb kostenfrei und ohne großen Zusatzaufwand nutzbar ist. Für PCs oder Laptops benötigt man z. B. lediglich eine WLAN-Karte, neuere Geräte haben eine WLAN-Schnittstelle bereits integriert. Mobile Endgeräte kommunizieren über die Funkschnittstelle mit einem Zugangspunkt *(Access Point),* der seinerseits über ein drahtgebundenes Netz an andere Netze angeschlossen ist.

Ein Zugangspunkt sendet in regelmäßigen Abständen Signalnachrichten aus, damit mobile Geräte, die sich in seiner Signalreichweite befinden, mit ihm Kontakt aufnehmen können. Die Signalreichweite beträgt zwischen 30 und 150 m. Die Funksignale können, anders als die Infrarotstrahlen, auch feste Gegenstände und Mauern durchdringen, so dass mit einem WLAN ein Bereich mit einer relativ großen Ausdehnung abgedeckt werden kann. Diese ungehinderte Signalausbreitung und damit Datenübertragungsmöglichkeit unterstützt zwar einerseits das breite Anwendungsspektrum der WLAN-Technologie (ungehinderter Netzzugang von vielen Aufenthaltsorten), andererseits macht sie aber auch solche Netze sehr viel verwundbarer als beispielsweise Infrarotnetze, die nur eine Reichweite von bis zu einem Meter besitzen.

Im Gegensatz zum WLAN zielt die *Bluetooth*-Technologie darauf ab, kurze Entfernungen (bis zu 10 m) zu überbrücken, um den *Kabelsalat* bei der Vernetzung der Geräte der persönlichen Umgebung, wie PC, Mobiltelefon, Drucker oder PDA, überflüssig zu machen. Man spricht von einem *PAN (Personal Area Network).* Bis zu acht Bluetooth-Geräte können sich spontan zu Netzen zusammenfinden, die wiederum zu einem größeren Netz zusammengeschaltet werden können. Auf diese Weise lassen sich ad hoc größere Netz bilden, ohne dass vorab eine Infrastruktur aufgebaut werden muss, wie sie in der drahtgebundenen Welt üblich ist.

Mobile Endgeräte

Mobile Endgeräte wie Laptops, Mobiltelefone, Organizer und Persönliche Digitale Assistenten (PDA) gehören immer mehr zu unserem alltäglichen Leben.

PDAs, diese tragbaren Kleinstcomputer mit ihren Funktionen zur persönlichen Organisation, wie beispielsweise Termin- und Adressverwaltung, Notizblock und mit Funktionen zum Führen von *ToDo-Listen*, werden immer beliebter. Sie verfügen über ein grafisches Display, welches die Darstellung kleinerer Texte, Tabellen oder Bilder erlaubt. Mittels eines Touch-Screens können Eingaben zur Steuerung der Programme oder zur Eingabe von Daten vorgenommen werden. Zur Kommunikation mit der externen Welt werden neben den *Cradles*, die eine feste Verbindung zum PC des Benutzers ermöglichen, Infrarot-, Bluetooth- oder GSM-Schnittstellen zur Anbindung an die Mobiltelefonie angeboten. PDAs stellen Arbeitsumgebungen zur Verfügung, die man aus dem PC- und Laptop-Umfeld gewohnt ist. Zur Ausstattung gehören daher neben angepassten Office-Paketen auch u. a. ein Browser oder eine *Java Virtual Machine*, so dass

auf bekannte Weise im Internet gesurft und mobiler Code dynamisch auf das Gerät herunter geladen und zur Ausführung gebracht werden kann.

Natürlich zählen auch Mobiltelefone zu den mobilen Endgeräten. Waren noch vor wenigen Jahren nur einfache Handys auf dem Markt zu finden, die lediglich Sprachübertragung unterstützten, hat sich die Handy-Technik bis heute rasant weiter entwickelt. Entwicklungsschritte gingen über *Triple-Band*-Geräte, die Daten- und Sprachdienste sowohl in europäischen als auch in US-amerikanischen Netzen ermöglichen, über die Bereitstellung von drahtlosen Übertragungsmöglichkeiten auf kurzen Distanzen, wie das Infrarotprotokoll *IrDA* oder *Bluetooth*, bis hin zu multimediafähigen Handys und Smartphones mit Farbdisplay und einer Vielzahl von Anwendungen, wie Terminkalender, Adressbuch oder Spielen.

Anwendungsszenarien für mobile Technologien

Vertraut ist uns der Anblick eines Assistenzarztes im Krankenhaus, dessen Kitteltaschen unschön aufgebläht sind von den vielen Utensilien, die er bei sich tragen muss. Neben Stethoskop, Reflexhammer und Taschenrechner gehören dazu Notizbücher, Listen mit Zusammenstellungen von Medikamenten, Checklisten, Therapie-Schemata, etc. Sie beherbergen das Wissen, das nicht unbedingt im Gedächtnis gespeichert sein muss, aber jederzeit abrufbar sein sollte. All das kann mit der Einführung von PDAs der Vergangenheit angehören. Die mobilen Endgeräte können in Zukunft gleichzeitig Beeper, Telefon, Agenda, Taschenrechner, Kamera, Diktiergerät und Web-Browser sein. Über eine drahtlose Vernetzung könnte der Arzt jederzeit einen Datenaustausch zwischen dem mobilen Gerät und den Servern im Krankenhaus durchführen. Einsetzbar sind PDAs u. a. vom Stationsarzt bei der Visite, bei der Patientenaufnahme oder auch vom Notarzt im mobilen Notfalleinsatz (vgl. Abbildung 2 (a)). Ein gänzlich anderes Anwendungsspektrum in der mobilen Gesundheitsversorgung eröffnet sich beispielsweise durch die Möglichkeit, mittels mobiler Technologien die Vitalfunktionen von Patienten kontinuierlich zu überwachen, ohne dass die Patienten dazu stationär im Krankenhaus sein müssen, sie können in das normale Berufs- und Privatleben integriert bleiben.

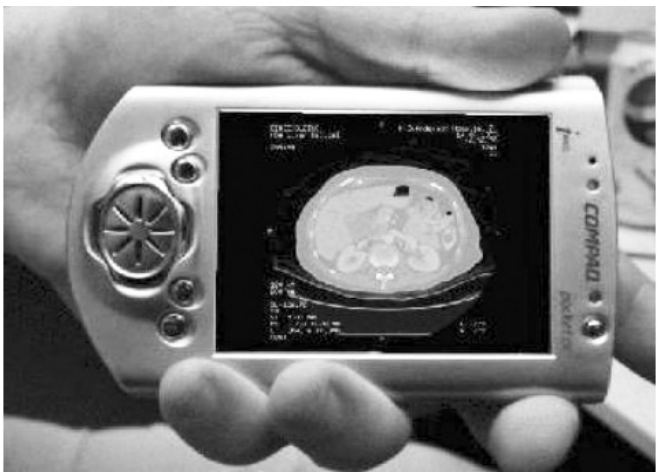


Abb. 2 (a) Radiologiebild auf PDA

Abb. 2 (b) Wegplanung mit dem PDA

Mobile Geräte und Dienste sind in vielen Alltagsbereichen einsetzbar, zum Beispiel bei der Unterstützung der Weg-Suche (zur nächsten Apotheke, Krankenhaus oder auch schlicht zum nächsten netten Restaurant, vgl. Abbildung 2 (b)), oder beim Kauf von Fahrkarten oder Eintrittskarten, ohne dass ihre Benutzer sich an einer Kasse anstellen müssen. Das mobil erstandene Ticket muss auch gar nicht ausgedruckt werden, sondern kann auf dem Gerät gespeichert bleiben. Bei der Eintrittskontrolle kommuniziert dann das Gerät direkt mit dem entsprechenden Lesegerät des Kinos, des Schaffners oder sonstiger Kontrolleinheiten. Auch die Bezahlung der gekauften Produkte kann durch das Gerät selber erfolgen. Es fungiert in diesem Fall als elektronische Geldbörse. Ein Beispiel eines solchen Bezahldienstes sind die Electronic Mobile Payment Services (EMPS) von VISA, die nach dem Prinzip Plug and Pay das mobile Bezahlen unterstützen. Weit verbreitet ist aber auch bereits das mobile Bezahlen via Handy.

Mobile Außendienstmitarbeiter, wie Handwerker oder auch Mechaniker können mit mobilen Anwendungen die benötigten Ersatzteile direkt beim nächstgelegenen Vertragshändler einkaufen. Damit dieser Beschaffungsprozess auch nahtlos in den Unternehmensablauf integriert wird, kann gleichzeitig mit der mobilen Bestellung ein Auftrag zur elektronischen Rechnungserstellung an das unternehmensinterne Ressourcen-Planungssystem *(ERP)* gesandt werden. Dadurch ist es nicht mehr nötig, dass mobile Mitarbeiter Papierformulare ausfüllen, die erst in einem weiteren manuellen und damit natürlich auch wieder fehlerträchtigen Bearbeitungsschritt in das IT-System übertragen werden. Über das mobile Endgerät kann auch auf die sonstigen Datenbanken im Unternehmen zugegriffen werden. Auf diese Weise ist es beispielsweise möglich, einen Kundenauftrag direkt vor Ort unter Rückgriff auf aktuelle Daten aus dem Unternehmen zu erstellen. Es ist aber auch möglich, bei einer schwierigen Reparatur eine Online-Hilfe in Anspruch zu nehmen oder das Ergebnis eines Prüfvorgangs mittels Spracheingabe direkt zur elektronischen Weiterverarbeitung zu übertragen.

Bei all diesen Szenarien für das mobile Arbeiten lassen sich Zeit, Ressourcen sowie aufwändige Arbeitsschritte sparen und auch Quellen für Fehler können damit entfallen, so dass sich hier-

durch ebenfalls Kosten einsparen lassen. Neben der Erhöhung der Lebensqualität des Einzelnen könnten die mobilen Technologien somit bei einer gezielten Integration in die Arbeitsabläufe deutlich zur Produktivitäts- und Qualitätssteigerung beitragen.

IT-Sicherheit

Mobiles Arbeiten eröffnet neue Möglichkeiten zur Zusammenarbeit bzw. zur Verbesserung der Arbeitsabläufe und zur Abwicklung digitaler Geschäftsprozesse. Aber mit der Verbreitung der Informations- und Kommunikationstechnologie war und ist eine zunehmende Gefährdung dieser Systeme zu verzeichnen. Diese Situation wird durch den Einsatz mobiler Technologien noch deutlich verschärft.

Sicherheitsprobleme bei der mobilen Kommunikation

Die drahtlose Kommunikation mittels der ungeschützten Funkübertragung birgt eine Reihe von Sicherheitsrisiken. Beim Einsatz von Funknetzen muss man sich stets darüber im Klaren sein, dass die Daten *über die Luft* übertragen werden. Das bedeutet, dass das Abhören dieser Funkverbindungen im Gegensatz zu drahtgebundenen Netzen deutlich einfacher ist. Bereits eine herkömmliche Antenne, die man z. B. als WLAN-Karte in seinen Laptop oder sein PDA stecken kann, reicht aus Daten aufzuzeichnen. Das Eindringen und Mithören *(sniffen),* aber auch das Verändern von Datenpaketen in einem Funknetz ist für Angreifer somit sehr viel einfacher als in herkömmlichen drahtgebundenen Netzen. Es haben sich bereits spezielle Angriffstechniken entwickelt, um mit frei verfügbaren Tools wie *Wellenreiter, NetStumbler* oder *Ministumbler* gezielt nach Zugangspunkten zu suchen.

Der **WLAN-Standard** 802.11 enthält zwar mit dem *WEP (wired equivalent privacy)* ein Sicherheitsprotokoll, das jedoch eine Vielzahl von Sicherheitslücken aufweist, so dass damit weder eine vertrauliche Kommunikation noch eine eindeutige Identifikation der Teilnehmer oder etwa ein verbindlicher Datenaustausch gewährleistet werden kann. Eine detaillierte Analyse der Sicherheitsmängel von WEP findet sich u. a. in [C. Eckert 2002]. So verlockend die Vorstellung der unkomplizierten drahtlosen Verbindung zum mobilen Arbeiten ist, so problematisch stellt sich dieser Datenaustausch bei näherem Hinsehen dar. Da WLANs standardmäßig ohne aktivierte Sicherheitsfunktionen installiert werden, ist davon auszugehen, dass die meisten heute im Einsatz befindlichen Netze noch nicht einmal den rudimentären WEP-Schutz aufweisen. In *Hot Spots* kann man generell von fehlenden Sicherheitsmaßnahmen ausgehen. Ad hoc gebildeten Netzen fehlt es an einer vorab etablierten Infrastruktur, so dass es sehr schwierig ist, Vertrauensbeziehungen nachzubilden, die man in herkömlichen Netzen über Public Key Infrastrukturen aufbaut, beispielsweise: Kommuniziere ich wirklich mit dem gewünschten Partner? WLAN-Nutzer, die ihre Laufwerke großzügig freigeben, müssen sich nicht wundern, wenn in Hot Spots und anderen WLAN-Umgebungen wildfremde Benutzer auf ihre Festplatte zugreifen; sie haben ja den Zugriff für z. B. Nutzer des gleichen Netzes (WLAN) selber erlaubt, obwohl bei der Freigabe natürlich an die Nutzer des lokalen Intranetzes gedacht war.

Sicherheitskritische Anwendungen wie das Abrufen von E-Mails oder der Zugriff auf unternehmenslokale Daten erfordern deshalb Zusatzmaßnahmen, wie beispielsweise die Etablierung eines *Virtuellen Privaten Netzes (VPN)* [C. Eckert 2002] zwischen einem mobilen Gerät und der Gegenseite. Hierfür ist auf beiden Seiten zusätzliche Software zu installieren, Das bedeutet natürlich zum einen administrativen Zusatzaufwand und zum anderen setzt es voraus, dass die mobilen Mitarbeiter auch stets diese Software verwenden, wenn sie mobil auf unternehmenslokale Daten zugreifen. Hierbei *allein* auf die Bereitwilligkeit der Mitarbeiter zu vertrauen, dass sie diese Zusatzmaßnahmen einsetzen, ist sicherlich naiv. Vielmehr muss durch technische Maßnahmen dafür gesorgt werden, dass die Nutzung der Sicherheitsdienste sich nicht umgehen lässt.

Das Sicherheitskonzept von **Bluetooth** ist für viele Anwendungsbereiche ausreichend und deutlich besser durchdacht als das von WEP bei WLANs. Bei einer korrekten Konfigurierung erhält man einen guten Basisschutz, der bei Bedarf aber durch zusätzliche Maßnahmen erweitert werden sollte. Zu bedenken gilt es jedoch, dass das Sicherheitskonzept ursprünglich für die Kopplung von Geräten des persönlichen Bedarfs entwickelt wurde, d. h. man ging von keiner allzu großen Sicherheitsanforderung der Benutzer aus. Mit dem Fortschritt der Technologie ist es mittlerweile aber schon möglich, auch Geräte, die bis zu 100 Meter weit entfernt sind, mittels Bluetooth zu koppeln, wodurch die Sicherheitsthematik natürlich an Bedeutung gewinnt.

Bedenklich am Bluetooth-Konzept ist, dass der Schutz auf der Verwendung von PINs basiert, von denen wir alle wissen, wie leicht man diese vergisst, sie sich am liebsten irgendwo notiert bzw. sie noch lieber gleich im Gerät selber gespeichert hat. Bluetooth bietet eine solche Möglichkeit, die dann natürlich dem nachlässigen Umgang mit PINs Vorschub leistet. Beim Einsatz von Bluetooth für sicherheitskritische Transaktionen wie z. B. Banktransaktionen muss man sich auch darüber im Klaren sein, dass ausschließlich Geräte und nicht einzelne Benutzer durch die Sicherheitsdienste identifiziert werden. Das bedeutet, dass jeder Besitzer eines Bluetooth-Geräts berechtigt ist, damit zu kommunizieren. Sicherheitskritische Anwendungen erfordern deshalb ebenfalls Zusatzmaßnahmen.

Bei der Mobilkommunikation via **GSM/GPRS/UMTS** werden die Daten nur solange verschlüsselt, wie sie über die Funkschnittstelle übertragen werden, also bis zum Funkmast. Danach liegen sie offen sowohl im Betreibernetz als auch im Festnetz vor. Es bestehen noch weitere erhebliche Sicherheitslücken, u. a. ist die Bildung von Bewegungs- und Aufenthaltsprofilen möglich (vgl. u.a [C. Eckert 2002]). Diese Probleme mögen für manche Privatanwender tolerabel sein, sie können aber für ein Unternehmen, das sensible unternehmensinterne oder kundenbezogene Daten austauscht, durchaus kritisch werden. Mögliche Verbesserungen bietet auch ein VPN zur sicheren Kommunikation zwischen dem mobilen Benutzer und seinem Partner im Unternehmen. Standardmäßig werden derartige Lösungen jedoch nicht angeboten, so dass man hierzu wiederum zusätzliche Software benötigt. Auch mit UMTS wird in Bezug auf die Sicherheit nur bedingt eine Verbesserung zu erwarten sein. Zwar wurden einige Probleme von GSM/GPRS beseitigt (u. a. wird auch das Netz authentifiziert und die Datenintegrität wird überprüft), aber eine *Ende-zu-Ende-Sicherheit* zwischen den Kommunikationspartnern wird auch hier nicht zur Verfügung gestellt.

Bei GPRS und UMTS werden die übertragenen Datenvolumina dem Benutzer in Rechnung gestellt. Damit erfährt das Empfangen von unerwünschten Mails (Spam etc.) eine weitere, höchst unschöne Dimension, nämlich, dass man auch noch dafür bezahlen muss, derartige Daten zu empfangen, oder dass man als Opfer einer Virus-Attacke für die vom eigenen Gerät ungewollt in großem Umfang abgesendeten Daten bezahlen muss. Mobilfunkbetreiber haben für diese Problematik noch keinerlei Lösung.

Sicherheitsprobleme bei mobilen Endgeräten

Charakteristisch für mobile Endgeräte ist, dass sie klein, leicht und natürlich portabel sind. Aufgrund der Tatsache, dass sie der Besitzer ständig bei sich trägt, werden sie meist als *sichere* Geräte betrachtet - ein trügerischer Schluss. Gerade ihre geringe physische Größe führt dazu, dass sie sehr schnell vergessen, unbeaufsichtigt liegengelassen oder auch gestohlen werden können. So ist beispielsweise aus Berichten der BBC [BBC-Statistik 2001] folgende beeindruckende Statistik zu entnehmen: Allein in den ersten sechs Monaten des Jahres 2001 blieben in Londoner Taxen 1.300 PDAs, 2.900 Laptops und 62.000 Mobiltelefone liegen. Allgemein gehen Studien von einer Verlustrate von ca. 30 % allein für PDAs aus. Der Verlust eines PDAs bedeutet für den Besitzer sicher mehr als nur den Verlust der Hardware. In den meisten Fällen ist die gespeicherte Information von sehr viel höherem Wert als die Wiederbeschaffung des Geräts; das wird unter Umständen sogar durch eine entsprechende Versicherung bezahlt. Die Wiederbeschaffung der Daten ist in allen Fällen in den Versicherungsbedingungen explizit ausgeschlossen. In Anbetracht der Tatsache, dass diese mobilen Geräte zunehmend neben sensiblen privaten auch geschäftliche Daten beispielsweise über Kunden oder über Unternehmens-Interna beinhalten, kann es dadurch zu beträchtlichen Schäden für die betroffenen Unternehmen kommen.

Das Risiko ist deshalb sehr hoch, weil alle marktführenden Betriebssysteme, ob PalmOS, Symbian oder auch WindowsCE/PocketPC, sehr ähnliche Defizite aufweisen [C. Eckert 2001]. So bieten zwar alle diese Systeme eine Zugangskontrolle, so dass nur ein per Passwort authentifizierter Benutzer Zugriff auf die gespeicherten Daten erhält. Dies ist jedoch nur eine Option und wird leider zu oft von Benutzern gar nicht erst genutzt. Ferner sind die verwendeten Maßnahmen unzureichend, da entweder schwache Verfahren verwendet oder die geheimen Passworte relativ ungeschützt auf dem Gerät abgelegt werden. Im Internet gibt es bereits zahlreiche Programme, um den integrierten Passwortschutz dieser Systeme zu knacken. Da die Zugangskontrolle in der Regel nur beim Einloggen durch den Benutzer erfolgt, erhält jeder, dem ein solches unbeaufsichtigt herumliegendes Gerät in die Hände fällt, direkten Zugriff auf die darauf gespeicherten Daten. Unternehmensdaten wie Angebote, Konstruktionsunterlagen oder strategische Planungsdaten sind für eine Firma unter Umständen überlebenswichtig und sollten nicht in falsche Hände geraten, was beim heutigen Stand der Technik nur durch die Integration zusätzlicher Software wie beispielsweise von Programmen zur Dateiverschlüsselung zu erreichen ist.

Durch die Portabilität der Geräte kommen diese in einer Vielzahl unterschiedlicher Umgebungen zum Einsatz, so dass eine erheblich größere Gefahr besteht, dass der Benutzer bei der Eingabe seiner PIN oder seines Passwortes beobachtet wird. Zusätzlich wird das mobile Gerät über die vorhandenen Kommunikationsschnittstellen den aus der PC-Welt bekannten Bedrohungen ausgesetzt, wie dem Übertragen von Viren oder Ausspähen der Festplatte. Virenschutzprogramme gehören heutzutage für PCs und Laptops zu den Standardsicherungsmaßnahmen. Dies ist aber bei PDAs keineswegs in gleicher Weise der Fall. Seit die ersten Viren für PDAs aufgetreten sind, werden solche Virenschutzprogramme auch für PDAs angeboten und sollten auch genutzt werden, da nach wie vor eine sehr hohe Bereitschaft unter PDA-Benutzern besteht, kostenlose Software auf dem Gerät zu installieren und sich damit Gefahren durch Viren auszusetzen.

Zusammenfassung

Mobiles Arbeiten eröffnet neue Möglichkeiten zur Zusammenarbeit bzw. zur Verbesserung der Arbeitsabläufe und zur Abwicklung digitaler Geschäftsprozesse. Neben der Erhöhung der Lebensqualität des Einzelnen könnten die mobilen Technologien somit bei einer gezielten Integration in die Arbeitsabläufe deutlich zur Produktivitäts- und Qualitätssteigerung beitragen. Diesen Chancen stehen aber zurzeit leider noch erhebliche Risiken gegenüber, auf die dieser Beitrag aufmerksam machen wollte. Sowohl heutige mobile Endgeräte als auch die drahtlosen Übertragungstechnologien bieten zum Teil nur sehr unzureichende und lückenhafte integrierte Mechanismen zum Schutz der verarbeiteten Daten und Informationen. Beispiele hierfür sind schwache Verschlüsselungsprotokolle, fehlende oder fehlerhafte Konzepte, um Manipulationen an Daten zu verhindern, und eine einseitige Geräte-Identifizierung. Hinzu kommt eine unzureichende Transparenz auf der Dienstebene. Dienstanbieter sammeln beispielsweise individuelle Benutzerdaten zur Profilbildung, um Kunden gezielt nach Interessen und Bedürfnissen mit Diensten zu bedienen. Dagegen steht das begründete Interesse

Prof. Dr. Claudia Eckert

Claudia Eckert ist Professorin für Informatik an der TU Darmstadt und leitet dort das Fachgebiet Sicherheit in der Informationstechnik. Gleichzeitig ist sie Leiterin des Fraunhoferinstituts für Sichere Telekooperation (FhG-SIT) in Darmstadt *(Anm. der Redaktion: die erste und bisher einzige!)* sowie zusammen mit J. Buchmann Leiterin des Darmstädter Zentrums für IT-Sicherheit (DZI) an der TU Darmstadt. Nach dem Studium der Informatik in Bonn promovierte sie an der TU München und habilitierte sich dort für das Fach Informatik. Sie forscht und lehrt in den Bereichen Betriebssysteme, Rechnernetze und schwerpunktmäßig im Bereich der Informationssicherheit.

des Benutzers, Profildaten persönlich zu verwalten und nur die absolut notwendigen Informationen preiszugeben (informationelle Selbstbestimmung und Schutz personenbezogener Daten).
Zur Verbesserung der Sicherheit mobiler Technologien existiert bereits eine Vielzahl von zusätzlichen Soft- und Hardwarelösungen. Es ist den Benutzern aber kaum zuzumuten, sich mit den Stärken und Schwächen der verschiedenen Produkte auseinander zu setzen, um die richtige und untereinander verträgliche Mischung aus Zusatzmaßnahmen auszuwählen. Diese Software muss dann auch noch korrekt konfiguriert und in Betrieb genommen werden, eine Überforderung der einzelnen Benutzer. Das sollte aber auch jedem Unternehmen bewusst sein, das es seinen Mitarbeiterinnen und Mitarbeitern erlaubt, mobile Technologien nach eigenem Gutdünken zu verwenden. Hier muss eine unternehmensweite Sicherheitspolitik dafür sorgen, dass das mobile Arbeiten nicht zu einem Risiko für das gesamte Unternehmen wird. Für PDAs sollten auf jeden Fall die gleichen Schutzmechanismen genutzt werden wie für Laptops oder PCs. Zu hoffen ist, dass in den weiteren Entwicklungsschritten die Sicherheitsdienste der Funknetze deutlich verbessert und die dringend benötigten Sicherheitsdienste so in die Betriebssysteme der Geräte integriert werden, dass die Benutzer sich auf deren korrektes Funktionieren verlassen können und nicht ständig selber Hand anlegen müssen, um Sicherheitslöcher zu stopfen. Leider sind wir von diesem Ziel noch ein gutes Stück entfernt, aber die sich abzeichnenden Entwicklungen zeigen zumindest in die richtige Richtung.

Literatur

C. Eckert IT-Sicherheit – Konzepte, Verfahren und Protokolle(2002) , zweite Auflage, Oldenbourg-Verlag

V. K Garg, J. E. Wilkes Principles and Applications of GSM (1999). Prentice Hall

C. Eckert Zur Sicherheit mobiler persönlicher Endgeräte – eine Bestandsaufnahme (2001). *In: Arbeitskonferenz Kommunikationssicher heit, 27.3.–28.3. 2001, SAP University Rot*

J. Roth Mobile Computing – Grundlagen, Technik, Konzepte. dpunkt-Verlag

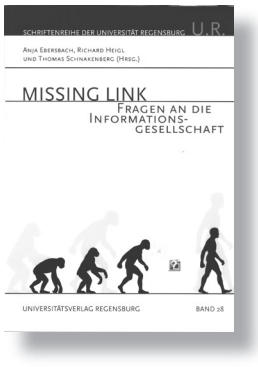
B. Schneier (2001) Secrets & Lies – IT-Sicherheit in einer vernetzten Welt, dpunkt-Verlag

BBC-Statistik (2001), *http://news.bbc.co.uk/hi/english/uk/newsid_1518000/1518105.stm*

Lesen - Neues für den Bücherwurm

Besprechungen von Ralf E. Streibl

Missing Link – Fragen an die Informationsgesellschaft



Das Buch dokumentiert eine von Studierenden der Universität Regensburg organisierte Veranstaltungsreihe. Schon in ihrer Einleitung machen die Herausgeber deutlich, dass hinter dem Begriff „Informationsgesellschaft" kein einheitliches Konzept steht, vielmehr wurde und wird diese Bezeichnung in vielfältiger Weise politisch instrumentalisiert. In diesem Sinne thematisierten die in dem Band dokumentierten Vorträge vor allem auch Machtfragen und Ausgrenzungen.

Vor einem geistesgeschichtlichen Hintergrund schreibt Rafael Capurro über mediale „(R-)Evolutionen" anhand dreier Medienbrüche: Oralität zur Schriftlichkeit, Handschriftlichkeit zur Drucktechnik, Drucktechnik zu elektronischer Vernetzung. Dabei wehrt er sich – unter Verweis auf die Originalquellen – gegen verkürzende Interpretationen (beispielsweise Platons Kritik an der Verschriftlichung als reine Medienkritik). Besonders wichtig sind dem Autor die Bezüge der Medienentwicklungen zu politischer Öffentlichkeit. Auch im Zeitalter der Cyberkultur sieht er den sozialen Bedarf an Kommunikation und Information im Zentrum. Unter Verweis auf vielfältige aktuelle Probleme einer zunehmend globalisierten Informationsgesellschaft (Spaltung zwischen Informationsreichen und -armen, Erhalt der Multikulturalität, Privatheit, etc.) fordert er die Weiterentwicklung einer umfassenden Informationsethik (unter Einbeziehung von Computerethik und Medienethik).

Das bei Capurro anklingende emanzipatorische Potenzial der Internetöffentlichkeit thematisiert Uwe Afemann mit Blick auf die Fragestellung, die ihn ja schon seit vielen Jahren beschäftigt: Welche Bedeutung kann dem Internet als entwicklungspolitischem Werkzeug zukommen? In seinem Beitrag verweist er auf Erfahrungen und Studien, nach denen durch die Einführung von IuK-Technologien in Entwicklungsländern vor allem die Hersteller dieser Geräte, Netzbetreiber, Banken und *lokale Verwertungseliten* profitierten. Die Kluft innerhalb der Länder wird größer, gleichzeitig nimmt die Verschuldung weiter zu. Zur Verdeutlichung hat Afemann aktuelles Zahlenmaterial zur globalen digitalen Spaltung zusammengestellt. Er diskutiert kritisch die

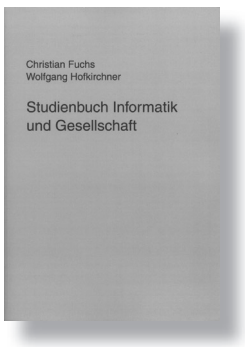
Chancen von Entwicklungsländern, diese Situation gesamtgesellschaftlich zu verbessern - durch den Einsatz von e-commerce, Nutzung des Internets im Bildungsbereich, oder auch im Bereich Menschenrechte. Vor dem Hintergrund seiner Betrachtungen kommt Afemann allerdings zum Schluss, dass das Internet zwar zur Schaffung einer sehr gut vernetzten internationalen Elite beiträgt – der Beweis, dass sich dadurch Lebenssituation und Wohlstand der breiten Bevölkerung systematisch verbessern würde, sei jedoch nicht erbracht worden.

In weiteren Beiträgen des Buches geht es unter einer *Gender*-Perspektive um die Situation von Männern und Frauen in kleinen Softwarefirmen (Annette Henninger, Ergebnisse einer empirischen Studie) sowie um das Themenfeld Open Source, Eigentum und (Informations-)Gesellschaft. Während Stefan Meretz, ausgehend von freier Software, über „Ideen für eine andere Gesellschaft" nachdenkt, kritisiert Sabine Nuss allzu euphorische Hoffnungen und sieht die bürgerliche Eigentums- und Rechtsordnung nicht unter gravierendem Veränderungsdruck. Der letzte Beitrag des Bandes ist das Protokoll einer Videokonferenzdiskussion mit Joseph Weizenbaum und Andy Müller-Maguhn. Der Versuch, den Gesprächscharakter zu dokumentieren, führt zwangsläufig dazu, dass dieser Buchbeitrag bei weitem nicht die inhaltliche Dichte und Stringenz anderer Beiträge des Bandes aufweist – andererseits scheint im Klima des Gespräches zwischen den beiden Videokonferenzteilnehmern und dem Publikum im Saal recht deutlich das angenehme Klima der Veranstaltung auf.

Als thematischem Sammelband würde man sich von dem Buch eine klarere inhaltliche Ausrichtung und besser aufeinander abgestimmte Beiträge wünschen. Als Dokumentation einer Vortragsreihe jedoch sind vor allem die Beiträge als solche zu betrachten, die lesenswert bis sehr interessant sind. Ein Blick in das Buch empfiehlt sich daher für alle, die beruflich oder aus persönlichem Interesse verschiedene Facetten der *Informationsgesellschaft* betrachten wollen.

Anja Ebersbach, Richard Heigl, Thomas Schnakenberg (Hrsg.): Missing Link – Fragen an die Informationsgesellschaft. Schriftenreihe der Universität Regensburg, Band 28. Regensburg: Universitätsverlag, 2003, ISBN 3-930480-45X, 172 S.

Studienbuch Informatik und Gesellschaft



Informatik und Gesellschaft ist seit geraumer Zeit zumindest an einigen Universitäten im deutschsprachigen Raum Teil der Ausbildung von Informatikstudierenden. Über die Möglichkeiten und Probleme und auch die Geschichte dieses Fachgebietes berichteten im Heft 4/2001 der FIfF-Kommunikation die Fachvertreter dieser Hochschulen. Eine Schwierigkeit stellt das Fehlen aktueller Lehrbücher dar. Natürlich gab es in der Vergangenheit mehrfach Versuche umfassender Darstellungen, die für eine Einführung in das Thema oder für spezielle Teilthemen hilfreich und nützlich sind (z.B. W. Steinmüller: Informationstechnologie und Gesellschaft, 1993; J. Friedrich, T. Herrmann, M. Peschek, A. Rolf (Hrsg.): Informatik und Gesellschaft, 1995; oder die Tübinger Fernstudienmaterialien zu „Informatik und Gesellschaft"). Doch ist – so zeigt sich in der Praxis – die Gratwanderung zwischen theoretischen Reflexionen einerseits und konkreten Beispielen andererseits schwer zu leisten. Illustrative Fallbetrachtungen werden relativ schnell von aktuellen Entwicklungen überholt – zwar kann man auch an älteren Beispielen grundsätzliche Probleme sehr gut veranschaulichen, doch darf nicht der Eindruck entstehen, das Fach mache seine Identität vorrangig an *Volkszählungsurteil, Fabrikautomatisierung mit Industrierobotern* und *Krankenversichertenkarte* fest. Bei eher theoretischen Betrachtungen stellt sich die Frage nach der Basis: Sucht man die zentrale Sichtweise, unter der man die Inhalte des Fachgebietes subsumieren will, wirkt das Ganze schnell verkrampft und einengend. Ja, das Fachgebiet mag theorielos sein (es steht damit nicht alleine da - vgl. die Bestrebungen für eine *Theorie der Informatik* im Umfeld der gleichnamigen Arbeitstagungen), gleichzeitig ist es jedoch auch voll von Theorien und Sichtweisen, die nicht zuletzt aus anderen Disziplinen entliehen und flexibel - manchmal auch gnadenlos - angewandt werden.

Um es vorwegzunehmen: Nein, das fehlende Lehrbuch haben Fuchs und Hofkirchner nicht vorgelegt – aber kann es das überhaupt geben? Das Verdienst der Autoren liegt darin, in dem Band sehr systematisch grundlegenden Begriffen nachzuspüren, die – nicht nur im wissenschaftlichen Diskurs des Fachgebietes *Informatik und Gesellschaft* – gerne ohne hinreichende Reflexion verwendet werden. In diesem Sinne sind die zentralen Kapitel des Bandes überschrieben mit „Information", „Gesellschaft", „Technik" und ihren Verknüpfungen wie „Informationstechnik", „Informationsgesellschaft" etc. Dieser Teil des Buches nennt sich „Einsichten". Hier versuchen die Autoren, anhand zahlreicher Quellen und Theorien, Struktur in die vielfältigen Betrachtungsmöglichkeiten von Technik zu bringen, die es sowohl von Technikentwicklung als gesellschaftlichem Prozess als auch von den gesellschaftlichen Wirkungen und Folgen gibt. Zur Einbettung dieser Reflexionen – gleichsam als Motivation des Vorhabens – ist dem Ganzen ein Teil „Ansichten" vorgeschaltet, in dem kurze Publikationsauszüge verschiedener Autoren Chancen und Risiken von Informatikanwendungen in den Feldern Technik, Umwelt, Gesellschaft, Wirtschaft, Politik und Kultur illustrieren.

Mit Blick auf die Breite der dargestellten Ansätze und vor allem die Systematik des Aufbaus und der Darstellung ist die Bezeichnung „Studienbuch" für das Werk mehr als angemessen. Es enthält viele Quellen und Anregungen für das weitere eigene Nachdenken und ist vor allem eines: ein Impuls für die weitere kritische Auseinandersetzung mit *Informatik* und *Gesellschaft*.

Christian Fuchs, Wolfgang Hofkirchner: Studienbuch Informatik und Gesellschaft. Norderstedt: Books on Demand, 2003. ISBN 3-8330-0252-2, 441 S.

Netkids und Theater

Der letztes Jahr veröffentliche Sammelband ist eine erweiterte Dokumentation eines Symposions im Jahr 2000. Die Autorinnen und Autoren – Schauspieler, Literatur- und Theaterwissenschaftler, Kultur- und Sozialwissenschaftler sowie Informatiker – beschäftigen sich in ihren Beiträgen mit Veränderungen der So-

zialisation in einer zunehmend informationstechnisch geprägten Welt (bis hin zur Veränderung der Sprache als identitätsstiftendem Merkmal), mit der Rolle und Bedeutung des Theaters sowie mit dem Einsatz von Maschinen und Medien im Theater.
In mehreren Beiträgen des Bandes wird die Bedeutung des Theaters als künstliche Welt hervorgehoben, Ingrid Hentschel beispielsweise spricht vom „Theater als Illusionsraum". Sie verweist darauf, dass Theater lange vor Film, Fernsehen und Computerwelten als „bevorzugtes Medium des Scheins und der Phantasie" etabliert waren. Ist es dann nicht nur natürlich, ja fast zwangsläufig, dass die heutigen Kunstwelten zum Einen Gegenstand von Theater werden, zum Anderen aber auch als Werkzeug und Medium in aktuellen Theaterprojekten eingesetzt werden?

Wer sich mit den kulturellen Möglichkeiten neuer Technologien beschäftigen möchte, kann in diesem Band eine Reihe von Anregungen finden – die vergleichsweise heterogene fachliche Herkunft der Beiträge erschwert zwar einerseits die Suche nach Querverbindungen, andererseits bietet solch interdisziplinärer Rahmen auch immer wieder den Raum für viel konstruktive Reibung.

Jörg Richard (Hrsg.): Netkids und Theater. Studien zum Verhältnis von Jugend, Theater und neuen Medien. Frankfurt/Main: Peter Lang, 2002. ISBN 3-631-37917-X, 260 S.

Qualität des Lernens im Internet

Der Autor, Erziehungswissenschaftler an der Universität Salzburg, versucht in seinem Buch Standards und Qualitätssicherungsmaßnahmen der internationalen erziehungswissenschaftlichen Forschung zu webbasierten Lernumgebungen zu identifizieren. Seine Beispiele bezieht er dabei vor allem aus dem angloamerikanischen Raum. Anders als in vielen anderen Publikationen zum Modethema „Internet und Bildung" bzw. allgemeiner „Computer und Lernen" verfällt Astleitner nicht in euphorische Schilderungen dessen, was durch die Technik nun alles machbar wird.

Nicht die Möglichkeiten, die das Medium technisch gesehen bietet, sondern die Qualität des Lehrens und Lernens stellt Astleitner in den Mittelpunkt seiner Betrachtung. Seiner Ansicht nach muss bei der Behandlung dieses Themas der Fokus der Aufmerksamkeit auf den Menschen und seine individuellen kognitiven, motivationalen und emotionalen Prozesse gerichtet sein. Folgerichtig verschweigt Astleitner – anders als andere – auch nicht die großen Probleme, mit denen manche Projekte zu kämpfen haben. Dazu gehört beispielsweise, dass die Lernenden Fernstudienmaßnahmen oft vorzeitig verlassen (Dropout-Raten von 95% und mehr bei Studien mit hohem Schwierigkeitsgrad wie z.B. Informatik). Erfreulich vorsichtig bleibt Astleitner auch bei der Frage, ob webbasierte Lernumgebungen zur Förderung höherer Denk- und Lernprozesse im Sinne eines *Kritischen Denkens* beitragen können. Ausgehend von einer allgemeinen Betrachtung der – oft wenig erfolgreichen – Förderung *Kritischen Denkens* im Unterricht thematisiert er Bedingungen, unter denen neue Medien eventuell Hilfestellungen bieten können. Nicht nur hier verweist er jedoch auch auf die notwendige Betrachtung sozialer Lernprozesse bei Planung und Einsatz webbasierter Lernumgebungen. Auch wenn das Werk in manchen Teilkapiteln etwas aufzählungshaft wirkt und teilweise auch klarere Stellungnahmen und Bewertungen von Beispielen wünschenswert wären, kann man das Buch auf jeden Fall als eine Bereicherung des explodierenden Buchmarktes zu diesem Themenfeld ansehen. Manchem *Macher* webbasierter Lernumgebungen sei es vor dem *Basteln* zur Lektüre empfohlen – am besten schon vor dem Schreiben entsprechender Förderanträge. Hektischer Aktionismus und der Glauben an die Potenz des Mediums führen nicht zu brauchbaren Systemen. Qualitätsevaluation dient für Astleitner in diesem Sinne nicht nur als Selbstzweck, um hinterher *aufzuräumen*, sondern vielmehr als Instrument, die Bedürfnisse der am Bildungsprozess beteiligten Gruppen expliziter zu machen.

Hermann Astleitner: Qualität des Lernens im Internet. Virtuelle Schulen und Universitäten auf dem Prüfstand. Frankfurt/Main: Peter Lang, 2002. ISBN 3-631-38982-5, 184 S.

Besprechungen von Werner Hülsmann

Bürgerrechte im Netz

Die neue Publikation der Bundeszentrale für politische Bildung beschäftigt sich in 17 Kapiteln mit den Auswirkungen der Internetnutzung auf die Politik. Scherpunkt ist hierbei das Spannungsfeld zwischen Selbstbestimmung im Netz, strafrechtlichen Inhalten und dem Recht auf freie Meinungsäußerung. Eine Einleitung und ein Glossar runden das Themenspektrum ab.

Als vor über 50 Jahren die Verfassungseltern das Grundgesetz formulierten, gab es noch kein Internet. Dennoch müssen sich die Gesetze und Verordnungen zur neuen Informationsgesellschaft am Grundgesetz orientieren: Sich hieraus ergebene Fragestellungen werden in diesem Buch behandelt: Wie groß ist die Meinungsäußerungsfreiheit im Netz, und wann sind Begrenzungen möglich und sinnvoll? Wie sehen virtuelle Demonstrationen aus? Was bedeutet das Internet für die Demokratie? Inwieweit ist Wissen als geistiges Eigentum geschützt? Reicht staatlicher Datenschutz aus, oder müssen Bürgerinnen und Bürger ihr Recht auf informationelle Selbstbestimmung im Internet selbst durchsetzen? Der vorliegende Band dokumentiert, wie die Internetpraxis die Grundrechte auf die Probe stellt und sollte daher zur Lektüre kritischer Internetnutzerinnen und –nutzer gehören. Bezogen werden kann dieser Band preisgünstig über *http://www.bpb.de/publikationen/UZX6DW,,0,B%FCrgerrechte_im_Netz.html*. Dort können auch alle Kapitel als PDF-Dateien heruntergeladen werden.

Christiane Schulzki-Haddouti (Hrsg.): Bürgerrechte im Netz, Bundeszentrale für politische Bildung, Bonn, 2003, ISBN 3-89331-458-X.

Korrektur: In der FIfF-Kommunikation 2/2003 wurde leider ein Titel falsch angegeben. Das von Stiefenhofer, Schlosser und Feil herausgegebene Buch (ISBN 3-446-21945-5) trägt den Titel „Praxisleitfaden Netzwerksicherheit". Wir bitten das Versehen zu entschuldigen.

Netzpiraten – Die Kultur des elektronischen Verbrechens

Dieses Buch aus der Telepolis-Reihe zur Netzkultur versucht einen vorurteilsfreien Blick auf die so genannten Subkulturen der Hacker, Cracker, Virenschreiber und Netzkrieger sowie einen Überblick über die Rechtslage zu geben.

Die Sammlung von sehr gut recherchierten Artikeln beschreibt in amüsanter und anschaulicher Weise die Welt des elektronischen Verbrechens. Anhand von realen Beispielen wird in leicht verständlicher Sprache der Unterschied zwischen Hackern und Crackern erklärt, beschrieben, was *Script Kiddies* sind und warum Wettbewerbe zum Cracken einer neuen Software ausgeschrieben werden. Dabei sind mehr oder weniger geheime Regierungsprojekte erwähnt und auch die *Großen* der Computer-Industrie bleiben nicht verschont. Die Lektüre des Buches ist wärmstens zu empfehlen für alle – auch und gerade die Nicht-Computer-Freaks –, die Stolperfallen und Gefahren des Internets einmal aus einer weniger technischen Sicht bei durchaus humoriger Sprache kennen lernen wollen.

Dabei kommen vor allem diejenigen, die sich mit dem Thema Sicherheit oder Netzkultur auseinandersetzen, kaum an diesem Werk vorbei. Das Buch ist rundherum gelungen und hebt sich deutlich von anderen Publikationen zu diesem Thema ab.

Medosch, Armin; Röttgers, Janko (Hrsg.): Netzpiraten – Die Kultur des elektronischen Verbrechens, Verlag Heinz Heise GmbH & Co KG, Hannover, 2001, ISBN 3-88229-188-5, 189 Seiten

Privat! - Kontrollierte Freiheit in einer vernetzten Welt

Dieses Buch stammt ebenfalls aus der Telepolis-Reihe zur Netzkultur und bietet einen Überblick über die Bedeutung der Privatheit in einer vernetzten Welt aus der Sicht von Philosophen, Ökonomen, Rechtstheoretikern, Sozialwissenschaftlern und Journalisten.

Im Fortschritt der Vernetzung unseres Lebens mit E-Mail, Internet, Mobiltelefonie etc. wird die Privatheit (engl. *privacy*) immer stärker in Mitleidenschaft gezogen. Auch wenn die Autoren und Autorinnen nicht vom einem Ende der Privatheit ausgehen, auch nicht nach dem 11. September 2001, so sehen sie doch vielfältige Gefährdungen. Dabei werden Fragen in einer umfassenden Bandbreite aufgeworfen: Was ist der Wert des Privaten? Lässt sich der Schutz des Privaten auch ökonomisch begründen oder *Privacy* gar als Produkt vermarkten?

In drei Aufsätzen wird zu Beginn die Frage beantwortet, warum Privatheit nötig und möglich ist. Weitere vier Aufsätze beschäftigen sich insbesondere mit der Vision von Big Brother sowie der Videoüberwachung aus unterschiedlichen Sichtweisen. Den Schwerpunkt – zumindest vom Umfang her gesehen – bilden die Aufsätze zur Ökonomie der Privatheit. Auch zu diesem Themenkomplex werden unterschiedliche Aspekte berücksichtigt.

Wer den Schutz der Privatheit nicht nur als ein datenschutzrechtliches Problem ansieht, sondern sich auch mit dessen philosophischen, ökonomischen und sozialwissenschaftlichen Aspekten beschäftigen will, der findet in diesem Buch eine gute Zusammenstellung lesenswerter Aufsätze.

Grötker, Ralf (Hrsg.): Privat! - Kontrollierte Freiheit in einer vernetzten Welt, Heise Zeitschriften Verlag GmbH & Co KG, Hannover, 2003, ISBN 3-93631-01-1, 254 Seiten

Zum Datenschutz

Praxiskommentar Bundesdatenschutzgesetz und Teledienstegesetze (Praxishandbuch) und Kommentierte Urteilssammlung zu den Datenschutzgesetzen (Loseblattsammlung)

Was auf den ersten Blick vielleicht verwundert, ist auf den zweiten Blick doch sinnvoll: Beide genannten Werke werden vom Verlag zusammen als Paket vertrieben. Da nach dem derzeitigem Stand nicht davon ausgegangen werden kann, dass es in nächster Zeit zu einer grundlegenden Novellierung des Bundesdatenschutzgesetzes (BDSG) kommen wird, wurde der Kommentar zum BDSG und den Teledienstegesetzen als abgeschlossenes Werk herausgegeben. Im Gegensatz dazu wird es sicher einige bedeutenden Urteile geben, die sich auf das neue BDSG (vom Mai 2001 in der seit Januar 2003 geltenden Fassung) beziehen. Daher wurde die Urteilssammlung zu den Datenschutzgesetzen als Loseblattsammlung herausgegeben. Beide Werke ergänzen sich gegenseitig.

Ein Kommentar zum Bundesdatenschutzgesetz ist für die Arbeit der betrieblichen Datenschutzbeauftragten unverzichtbar, da sich häufig die Bedeutung der jeweiligen Paragraphen nicht mehr alleine aus deren Formulierung erschließt. Da viele Unternehmen sich im Internet präsentieren, müssen auch die datenschutzrechtlichen Regelungen für Teledienste von diesen berücksichtigt werden.

Verglichen mit manchen anderen Kommentaren alleine zum BDSG, die mit über 1.500 Seiten auf Dünndruckpapier daherkommen, lässt sich der „Praxiskommentar“ als kompakt bezeichnen. Natürlich können nicht alle juristischen Finnessen der 1500-Seiten-Kommentare enthalten sein, aber der oder die betriebliche Datenschutzbeauftragte benötigt solche Finnessen auch nicht für die tägliche Arbeit. Für die im Allgemeinen erforderliche Arbeit der betrieblichen Datenschutzbeauftragten ist der Kommentar mehr als ausreichend. Zusätzlich finden sich auf der beiliegenden CD auch noch diverse Mustertexte, angefangen von der Bestellung zum/zur Datenschutzbeauftragten über

die Verpflichtung auf das Datengeheimnis bis hin zum Verfahrensverzeichnis.

Als sinnvolle Ergänzung zu diesem Praxishandbuch erweist sich das Fachkompendium „Kommentierte Urteilssammlung zu den Datenschutzgesetzen". Die Urteile sind in sieben Teile untergliedert. Von „Grundlegenden Aussagen zum Datenschutz" mit Verfassungsgerichtsentscheidungen über die „Stellung und Aufgaben des Datenschutzbeauftragten", den „Umgang mit persönlichen Daten" sowie der Themenkomplex „Datenschutz und Betriebsrat" bis hin zum Themengebiet „Telekommunikation und Internet" reicht die Bandbreite der veröffentlichten Urteile. Dabei werden die Urteile nicht einfach abgedruckt, sondern zusammengefasst und jeweils mit einem Kommentar „Folgerungen für die Praxis" versehen. Bedingt durch die Fülle der Urteile ist die auf der CD integrierte Volltextsuche, die sich auch einzelne Kapitel beschränken lässt sehr hilfreich.

Zusammenfassend lässt sich feststellen, dass dieses Paket eine gelungene Verbindung von Kommentar und Urteilssammlung ist.

Abel, Dr. Horst G.: Praxiskommentar Bundesdatenschutzgesetz und Teledienstegesetze (Praxishandbuch), Interest Verlag, Kissing 2003, ISBN 3-8245-1109-6, Fachbuch mit 626 Seiten und CD-ROM, und Kommentierte Urteilssammlung zu den Datenschutzgesetzen (Loseblattsammlung), ISBN 3-8245-4150-5 Loseblattsammlung mit ca. 500 Seiten und CD-ROM

Praxishandbuch IT-Know-How für den Datenschutzbeauftragten

Bei der Suche nach einem oder einer geeigneten betrieblichen Datenschutzbeauftragten stellt sich häufig das gleiche Dilemma. Entweder gibt es eine Mitarbeiterin oder einen Mitarbeiter mit fundierten juristischen Kenntnissen und nahezu vernachlässigbaren technischen Kenntnissen oder aber es ist genau umgekehrt. Und selbst wenn der Glücksfall eintreten sollte, dass sich eine Diplom-Informatikerin mit Nebenfach Datenschutzrecht und entsprechender Berufserfahrung in beiden Bereichen oder ein Jurist mit Fachgebiet Datenschutzrecht und Zweitausbildung Informatik findet, so wird sie bzw. er sich sicher nicht in *allen* technischen Systemen auskennen. Ziel dieses Werkes ist es, dieses Dilemma zu überwinden und den datenschutzrechtlich ausgebildeten Datenschutzbeauftragten das notwendige technische Grundwissen an die Hand zu geben.

Allein schon der erste Teil mit Stichwortverzeichnis, ausführlichem Glossar und umfangreichen Musterformularen vom Verfahrensverzeichnis über die Verpflichtung auf das Datengeheimnis bis hin zu Betriebsvereinbarungen und Dienstanweisungen hat einen großen Nutzwert. Im zweiten Teil werden die technischen und organisatorischen Maßnahmen nach § 9 Bundesdatenschutzgesetz (BDSG) sowie die Aufgaben der betrieblichen Datenschutzbeauftragten erläutert. Der dritte Teil enthält Prüfungsansätze und –checklisten.

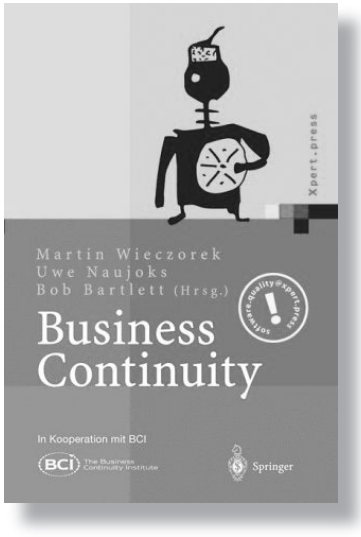
Im vierten Teil werden die Prüfungsmöglichkeiten sowohl im Mainframe-Bereich (IBM- und BS-2000-Welt als auch im Client/Server-Bereich (Unix/LINUX, sowie WindowsNT/2000) dargestellt. Der fünfte Teil setzt sich mit Netzwerken auseinander und beschreibt einige Sicherheitskomponenten. Das Thema der Datenbanken wird im sechsten Teil behandelt, während sich der siebte Teil mit E-Mail und Messaging beschäftigt. Diesen Abschnitten ist eines gemeinsam: sie stellen die jeweiligen technischen Grundlagen ausführlich dar.

Zwar wird es auch mit dem Praxishandbuch in manchen Fällen nötig sein, technische Experten oder Expertinnen hinzuzuziehen, aber selbst in diesen Fällen hilft der Inhalt des Praxishandbuches Datenschutzbeauftragten die Aussagen der Expertinnen und Experten zu verstehen und einzuordnen. In vielen Fällen wird an Technik interessierten Datenschutzbeauftragten mit diesem Handbuch das Know-How zur Verfügung gestellt, um die tägliche Arbeit zu meistern und fundierte Gespräche mit den Mitarbeiterinnen und Mitarbeitern der EDV-Abteilung führen zu können.

Abel, Dr. Horst G.: Praxishandbuch IT-Know-How für den Datenschutzbeauftragten – Rechtssichere Beurteilung von Netzwerken, Datenbanken und E-Mail-Systemen, Interest Verlag, Kissing 2003, ISBN 3-8245-7530-2, Loseblattsammlung, ca. 600 Seiten mit CD-ROM

Nachschlag zur IT-Sicherheit in der FIfF-Kommunikation 2/2003

Business Continuity – Notfallplanung für Geschäftsprozesse



Die Wirtschaft und damit auch das gesellschaftliche Leben werden immer abhängiger von funktionierenden IT-Systemen. EDV-Ausfälle kann – bei ungenügender Notfallvorsorge – kein Unternehmen über eine längere Zeit überstehen.

Daher stellen das Risiko-Management und Planung für den Wiederanlauf nach einem Notfall in der heutigen Zeit der Hochverfügbarkeit von Technik und Dienstleistungen eine elementare Voraussetzung für die Wettbewerbs-Fähigkeit und

meist auch den Fortbestand eines Unternehmens dar. Das Buch bietet durch die Beleuchtung dieser hochinteressanten Thematik aus den unterschiedlichsten Facetten allen interessierten Lesern sowohl mit praktischen als auch theoretischen Schwerpunkten eine Fülle von Informationen, sei es für die Konzeption eigener Projekte oder die Vorbereitung von internen und externen Revisionen. Als Beispiel wird eine internationale Bank mit Sitz in Deutschland herangezogen. Auch wenn die IT-Verfügbarkeit in der Finanzbranche noch wichtiger für das Überleben des Unternehmens ist als vielleicht in manch anderer Branche, so sollten es sich insbesondere die Verantwortlichen der 2/3 der IT-Unternehmen zu Gemüte führen, bei denen kein Risikomanagement angewendet wird.

Bartlett, Bob; Naujoks, Uwe, Wieczorek, Martin (Hrsg.): Business Continuity – Notfallplanung für Geschäftsprozesse, Springer-Verlag Berlin, Heidelberg New York, 2001, ISBN 3-540-44285-5, 232 Seiten

Angewandte Kryptographie

Die angewandte Kryptographie spielt im Zeitalter der Vernetzung und des E-Commerce eine zentrale Rolle beim Schutz von vertraulichen Daten und persönlicher Identität. Sie umfasst die Themen Verschlüsselung, Public-Key-Kryptographie, Authentifikation, digitale Signatur, elektronisches Bargeld und sichere Netze.

Ziel des Buches ist es, Grundwissen über Algorithmen und Protokolle zu vermitteln und kryptographische Anwendungen aufzuzeigen. Als Beispiele dienen neueste Entwicklungen wie der Advanced-Encryption-Standard (AES) oder wichtige aktuelle Angriffe gegen das Public-Key-System PGP bzw. gegen Krypto-Chipkarten.

Mit so wenig Mathematik wie nötig, aber vielen Beispielen, Übungsaufgaben und Musterlösungen wird der Schritt von der Theorie zur aktuellen Praxis vereinfacht. Zusätzlich sind auf der Webseite zum Buch aktuelle Links, Literatur und Präsentationsmaterial für Dozenten zu finden. Die zweite überarbeitete Auflage enthält Musterlösungen zu den Übungsaufgaben. Neben vielen Ergänzungen wurden aktuelle Entwicklungen wie zum Beispiel das Signaturgesetz oder die biometrische Identifikation aufgenommen.
Neben einem geschichtlichen Überblick über die Kryptographie und die klassischen Chiffren sowie der Darstellung der erforderlichen mathematischen Grundlagen enthält das Buch viele aktuelle Beispiele und Übungen. Konkret werden elektronisches Bargeld und elektronische Zahlungssysteme dargestellt. Auch die politischen Randbedingungen der Kryptographie werden angesprochen.

Auch wenn in diesem Lehrbuch nicht auf mathematische Grundlagen verzichtet werden kann, so ist zum Verständnis kein erfolgreich absolviertes Mathematikstudium erforderlich, Mathematikkenntnisse der Oberstufe werden allerdings vorausgesetzt. Wer diese mitbringt und sich selbst oder anderen fundiertes Wissen über Kryptographie beibringen will, hat mit diesem Buch ein gutes Werkzeug hierzu in der Hand.

Ertel, Wolfgang: Angewandte Kryptographie, Fachbuchverlag Leipzig im Carl Hanser Verlag, München, Wien, 2003, ISBN 3-446-22304-5, 221Seiten

Internet-Sicherheit – Browser, Firewalls und Verschlüsselung

Dieses umfassende Werk richtet sich sowohl an private Nutzerinnen und Nutzer, die möglichst gefahrlos im Internet surfen wollen als auch an Systemverantwortliche, die ein Firmennetz sicher betreiben wollen. Die Grundlagen des Internet werden detailliert aber nicht zu umfangreich erläutert und die verschiedenen Sicherheitsrisiken bei der Nutzung des Internet dargestellt und bewertet. Dies ist die Basis für die Einschätzung des eigenen Risikos durch die Leserinnen und Leser.

Weiterhin werden in dem Buch die notwendigen Schutzmechanismen erläutert. Hierzu gehören insbesondere Kryptographie, also Verschlüsselungsverfahren, und für den professionellen Einsatz Firewall-Systeme sowie Intrusion-Detection-Systeme (IDS). Dabei wird auch die Problematik *Firewalls und verschlüsselte Datenübertragung* angesprochen. Mögliche Anordnungen und Konfigurationen des Firewall-Systems werden in Abhängigkeit von den zu nutzenden Diensten diskutiert. Bei der Beschreibung der Sicherheit von Webservern werden beide „Welten", also Linux und Windows berücksichtigt. Auch bei der Darstellung der Sicherheitsaspekte bei den Browsern werden neben dem Internet Explorer auch verschiedene Versionen des Netscape Communicator, sowie Mozilla, Opera und Konqueror berücksichtigt. Für die private Internetnutzung werden zusätzlich Personal Firewalls besprochen. Kapitel über Gefährdungen und Sicherheitsanforderungen beim Einsatz von Telearbeit, Anonymität, Privatsphäre und Recht im Internet sowie über Electronic Commerce runden das Buch ab.

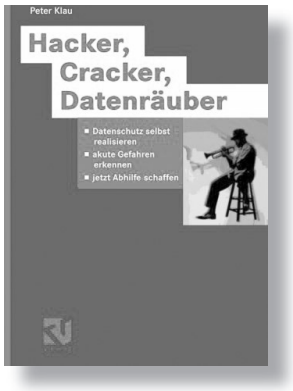
Leider hat dieses Buch ein kleines Manko: Bedingt durch das Alter (immerhin ist die letzte Auflage 2001 erschienen) konnten die aktuellsten Softwareversionen bei Servern und Browsern bei der Darstellung der sicherheitsrelevanten Einstellungen nicht berücksichtigt werden. Allerdings gelten die meisten der hierzu gemachten Aussagen auch für die neueren Versionen. Trotz dieses Mankos ist das Buch ein wichtiges Werk für alle, die sich dem Thema Internetsicherheit annähern wollen oder müssen.

Fuhrberg, Kai; Häger, Dirk, Wolf, Stefan: Internet-Sicherheit – Browser, Firewalls und Verschlüsselung, Carl Hanser Verlag München, Wien, 2001, ISBN 3-446-21725-8, 494 Seiten

Hacker, Cracker, Datenräuber

Alle, die moderne Kommunikationsmittel nutzen, vom PC bis zum Handy, sollten Interesse daran haben, dass ihre Daten nicht Freiwild für andere werden. Dies gilt nicht nur für geschäftliche Daten, sondern hier geht es auch um den Schutz der Privatsphäre. Ziel des Buches ist es zu zeigen, worauf es an kommt und dies in klarer, lockerer Darstellung. Zielgruppe sind die pri-

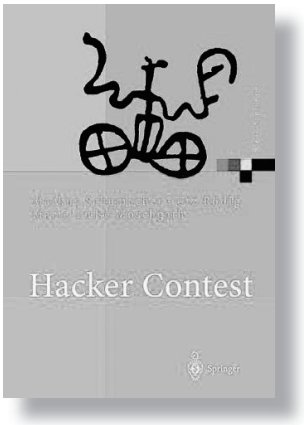
vaten Nutzer und Nutzerinnen von PC-Systemen mit Windows-Betriebssystemen.



Das Buch zeigt die konkreten Gefährdungen der Internetnutzung am persönlichen Computer. Hierzu gehören u.a. Viren, Würmer, Dialer, Hoaxes, Kettenbriefe, Also all die Gefährdungen, die zu Hause beim Surfen bestehen und noch häufig unterschätzt werden. Ebenso werden mögliche Maßnahmen zum Schutz dargestellt, wie Virenscanner, Personal Firewall, Dialer-Schutzprogramme und Verschlüsselung von E-Mails. Wer für den privaten Hausgebrauch seinen PC sicherer machen möchte, findet in diesem Buch nützliche Hinweise und Anleitungen. Wer allerdings wirklich sensible Daten – und seien es nur die Buchhaltungsdaten seines Gewerbebetriebes verarbeitet – tut gut daran, weitergehende Sicherheitsmassnahmen zu ergreifen.

Klau, Peter: Hacker, Cracker, Datenräuber – Datenschutz selbst realisieren, akute Gefahren erkennen, jetzt Abhilfe schaffen; Friedrich Vieweg & Sohn Verlags-GmbH, Braunschweig, Wiesbaden, 2002, ISBN 3-528-05805-6, 268 Seiten

Hacker Contest



Diese Buch richtet sich vor allem an technisch Interessierte und IT-Fachleute, die einen seriösen Einstieg in die Materie „IT-Sicherheit“ suchen. Es beschreibt die meisten Konzepte Betriebssystem-unabhängig und ist so eine gute Grundlage für spezifischere Fachbücher. Im Gegensatz zu vielen anderen Büchern zur IT-Sicherheit ist es dabei weder Gebrauchsanleitung für Systemadministratoren oder Entwickler noch ein Lehrbuch für das Informatikstudium, sondern ein Grundlagenwerk, um den Stellenwert von Computersicherheit einschätzen zu lernen.

In den drei Kapiteln des ersten Abschnitts wird ein historischer Abriss über bekannte Hacker und Cracker aufgezeigt sowie eine kurze Einführung in die rechtliche Situation gegeben. Im zweiten Abschnitt werden viele Bereiche der IT-Sicherheit angesprochen und dabei ausführlich die Grundlagen der IT-Sicherheit wie die Authentifizierung oder das Erkennen von Angriffen erläutert. Die Probleme werden generalisiert dargestellt, es geht also nicht um den konkreten Einzelfall, sondern um die grundlegenden Verhaltensrichtlinien der IT-Sicherheit. Auch im dritten Abschnitt versuchen die Autoren in allgemeiner Form darzustellen, was man in welchen Fällen unternehmen muss: Die Probleme werden abstrahiert und verschiedene Lösungsansätze vorgestellt.

Das Werk bietet als eines der wenigen vergleichbaren Bücher außerdem einige Informationen über Täterprofile. So erfahren die Leserinnen und Leser, mit wem und mit welcher Altersgruppe aus welchen geografischen Regionen sie es bei Angriffen vermutlich zu tun haben. Durch die abstrakte Darstellung der Probleme wird das unvermeidliche Problem der Aktualität elegant gelöst. Dieses stellenweise fast zum Schmökern geeignete Werk ist wichtig und interessant, nicht nur für alle, die sich das erste Mal mit Internetsicherheit befassen müssen.

Moschgath, Marie-Luise; Rödig, Utz; Schumacher, Markus: Hacker Contest; Springer-Verlag Berlin, Heidelberg New York, 2003, ISBN 3-540-41164-X, 301 Seiten

Web-Administration – Administration von Web- und Internet-Servern unter UNIX/Linux und Windows

Auch wenn dieses Werk sich ganz allgemein mit der Administration von Web- und Internet-Servern beschäftigt, so enthält es doch wesentliche Abschnitte, die sich mit der Sicherheit der jeweiligen Systeme und Server auseinandersetzen. Das scheint mir Grund genug, dieses Werk unter der Rubrik IT-Sicherheit aufzunehmen.

Bereits das erste Kapitel, das sich mit der Auswahl der Hard- und Softwarekomponenten beschäftigt, legt großen Wert auf die Verfügbarkeit der Dienste. Es wird der Leserin oder dem Leser zwar nicht die Entscheidung zwischen Linux und Windows abgenommen, aber die Vor- und Nachteile beider Betriebssysteme kurz dargestellt. Der Tatsache, dass die Administration von Linux- und Windows-Systemen nicht vergleichbar ist, wird dadurch Rechnung getragen, dass für beide Betriebssystemvarianten eigene Kapitel für die unterschiedlichen Komponenten erstellt wurden. Linux-Administratoren und Administratorinnen werden so nicht mit Windows-Spezifika belästigt und umgekehrt. Wer mit den Informationen „der anderen Seite“ gar nicht in Berührung kommen will, kann sich – zumindest beim derzeitigen Umfang – die Ordner so zusammenstellen, dass ein Ordner nur die allgemeinen Teile wie Hard- und Softwareauswahl, Tabellen und die Grundlagen, Formate und Protokolle des Internet sowie die Kapitel zum eigenen Betriebssystem enthält und der andere Ordner die Kapitel des anderen Betriebssystems.

Da auch ein aus Open-Source-Komponenten bestehender Server nicht per se sicher ist und auch ein auf Windows basierender Internet-Server relativ sicher betrieben werden kann, werden in beiden Hauptteilen viele sicherheitsbezogene Themen angesprochen. Nur der Datenschutz kommt etwas kurz. So fehlen – wie in den meisten anderen vergleichbaren Werken auch – Hinweise auf die datenschutzkonforme Gestaltung der Logfiles. Alles in allem bietet dieses Werk aber die Informationen, die zum sicheren Betrieb eines Webservers erforderlich sind.

Padberg, Dr. Anja (Hrsg.): Web-Adminsitration – Administration von Web- und Internet-Servern unter UNIX/Linux und Windows; Interest-Verlag, Kiesling, 2003, ISBN 3-8245-9101-4, Loseblattsammlung, ca. 1.600 Seiten

Dagmar Boedicker

Symposium „Trusted Computing Group (TCG)“
am 2. und 3. Juli 2003 in Berlin im BMWA

Bei der Trusted Computing Group (TCG) handelt es sich um ein Gremium, in dem sich 30 Firmen, unter anderem AMD, HP, IBM, Intel und Microsoft, zusammengeschlossen haben, um offene Standards für Trusted Computing *zu spezifizieren. Vorläufer der TCG in anderer Zusammensetzung war die* Trusted Computing Platform Association (TCPA) *mit etwa 200 Mitgliedern. Ein vorläufiges Ergebnis entfachte unter dem Namen* Palladium *heiße Diskussionen. Microsofts Weiterentwicklung heißt* Next Generation Secure Computing Base (NGSCB).

Das Bundesministerium für Wirtschaft und Arbeit (BMWA) *hatte zu einem zweitägigen Symposium geladen, um die wettbewerbs- und datenschutzrechtlichen Aspekte zu diskutieren und die „bislang höchst kontrovers geführte[n] Diskussion über die tatsächlichen Inhalte und Auswirkungen“ (Ankündigungstext des Bundesministeriums für Wirtschaft und Arbeit) zu versachlichen.* Nach eigener Aussage ist das BMWA am Thema IT-Sicherheit sehr interessiert, vermisst aber zur Zeit volkswirtschaftliche Impulse aus dem IKT-Bereich. Zeitweise schlugen die Wellen hoch, woran der Chaos Computer Club (CCC) natürlich nicht ganz unschuldig war. Sicher hätte auch das FIfF dazu etwas zu sagen gehabt, es war aber nicht geladen, um nicht zu sagen: Es wurde ausgeladen. Dazu aber mehr im Fazit. Zunächst ein möglichst knapper Bericht über die wesentlichen Aspekte des Symposiums, eingeleitet von einer Darstellung des Sicherheitskonzepts der Trusted Computing Group. Wer sich darin schon auskennt, kann das überspringen und gleich weiter lesen, was die Kritiker dazu sagen.

Das Sicherheitskonzept

Trusted Computing wie von der TCG spezifiziert ist ein integriertes Hardware-Software-Konzept. Ein vom Hersteller zertifizierter Chip[2], ein veränderter Chipkarten-Controller, wird fest mit der Platine des PCs, PDAs oder Mobiltelefons[3] verbunden. Dieses *Trusted Platform Module (TPM)*

- erzeugt asymmetrische Schlüssel und Zufallszahlen für die Verschlüsselung,
- speichert Hash-Werte über die Konfiguration in *Platform Control Registers (PCR),* die vor dem und beim Booten eine *Chain of Trust* erzeugen,
- erzeugt einen Genehmigungsschlüssel *(Endorsement Key, EK),* mit dem die Nutzer ihre Schlüssel als vom Trusted Platform Module generiert bestätigen. Auf der Basis des Endorsement Key können *Attestation Identity Keys (AIKs)* von einer externen Zertifizierungsstelle zertifiziert werden. Mit diesen AIKs lassen sich die Schlüssel des Nutzers anonym signieren.
- initialisiert und verwaltet weitere Funktionen wie das Ein- oder Ausschalten des Trusted-Computing-Modus durch den *Eigentümer* (der nicht mit dem *Nutzer* identisch sein muss).

Die Schnittstelle zu den Funktionen des Trusted Platform Module bildet der *TCG-Software-Stack (TSS),* beispielsweise für die Entwicklung standardisierter Verschlüsselungs-APIs[4], Schlüssel-Backup und -Migration, Authentifizierung der Plattform usw.

Beim Start des BIOS und beim Booten prüft das Trusted Computing Module schrittweise den Zustand des PCs und speichert *integrity metrics,* Plattform-abhängige Informationen zum Zustand der Software. Stück für Stück werden die Komponenten des Betriebssystems, die Hardware und die Software geladen und geprüft. Entsprechen die Hash-Werte dem Soll, kann es weitergehen. Wenn sich die Konfiguration deutlich geändert hat, ist eine neue Zertifizierung nötig. Eine Aussage lautet, dass der Benutzer sie selbst durchführen kann, Kritiker behaupten, dass die Änderungen online *abgesegnet* werden müssen und der PC eine neue Zertifizierung braucht.[5] Wenn Inhalte abgerufen werden, haben Anbieter die Möglichkeit, ihre verschlüsselten Inhalte nur in Abhängigkeit von ihren Sicherheitsrichtlinien abzugeben und können dazu verlangen, dass der Rechner sich als vertrauenswürdig gemäß TCG-Attestierung ausweist. Weil wahrscheinlich nur bestimmte Software als vertrauenswürdig anerkannt sein wird, können die Inhalte-Anbieter und Inhaber der digitalen Rechte natürlich Auflagen für die Software machen, beispielsweise einen bestimmten Abrechnungsmodus, Kopierschutz usw.

Das TPM kann nicht vor Hardware-Angriffen schützen, auch nicht vor Spam oder Viren-Attacken. Mit dem TPM wird ein Gerät authentifiziert, nicht die Person, die es nutzt.

Spezifikationen der TCG

Die TCG spezifiziert die Komponenten des Sicherheitskonzepts und außerdem Zertifizierungsanforderungen für spezifische Implementierungen. Als Spezifikationsinstrument werden *Protection Profiles* gemäß der *Common Criteria (IS 15408)* genutzt.
M. Waidner, vom *IBM Privacy Research Institut*, beschrieb auch, was die Trusted Computing Group *nicht* tut:

- Sie zertifiziert weder Anwendungen noch andere Software oder Schlüssel,
- sie nimmt keinen Einfluss auf die Auswahl der Software, die Benutzer auf der Trusted Platform einsetzen,
- und sie implementiert weder Dienste noch Server von Dritten.
- Sie unterhält keine Datenbanken
- und fungiert nicht als *Trusted Third Party,* die die Vertrauenswürdigkeit kommunizierender Geräte attestiert.

Die Kritik

Der wohl polemischste Kritiker war Ross Anderson, Universität Cambridge, UK. Mit handgeschriebenen Folien statt geschniegelter Powerpoint-Präsentationen feuerte er gezielte Salven auf die Versuche der Konzerne, die Selbstbestimmung der IT-Beschäftigten und -Nutzer mit technischen Kniffen einzuschränken. Aber auch Christian Koenig vom Zentrum für Europäische Integrationsforschung nahm kein Blatt vor den Mund. Wo Anderson und verschiedene CCC-Mitglieder Kritik aus technischer Sicht vorbrachten, hatte Koenig eher das Kartellrecht im Blick. Er äußerte den Verdacht, die TCG wolle misstrauischen Juristen möglichst wenig Einblick in die Technik geben: *Security by obscurity.* Gerade dann aber, wenn Juristen etwas obskur erscheine, kontrollierten sie besonders genau – vor allem im Wettbewerbsrecht.

Koenig verwies auf Artikel 81 EG-Vertrag, das Kartellverbot: Es bezieht sich auf abgestimmte Verhaltensweisen, die eine Verfälschung des Wettbewerbs bewirken. Ein Wille der Beteiligten ist dazu nicht nötig, der Effekt kann beispielsweise durch Standards entstehen, die Kompatibilität, Austauschbarkeit, und Interoperabilität regeln. Koenig warnte davor, Wettbewerbskommissar Monti zu unterschätzen: Im Gegensatz zu US-Wettbewerbsschützern, die gern abwarten und erst bei Fehlverhalten zuschlagen, beobachteten die Hüter des EU-Wettbewerbsrechts sehr viel genauer und ließen sich vorab, oft vertraulich, informieren. Microsoft und Intel seien wenig proaktiv in diesen Kontakten, sie schienen Angst wegen vergangener Vorfälle zu haben. Koenig gab die Empfehlung, die Kommission auf dem Laufenden zu halten, meinte aber, das könne im Fall TCG auch schon vertraulich passiert sein.

Informationsfreiheit und informationelle Selbstbestimmung

Ein Schwerpunkt der Kontroverse war das Zusammenspiel zwischen TPM und dem *Digital Rights Management (DRM):* DRM soll die grundgesetzlich verankerten zustimmungsfreien, pauschal vergüteten Nutzungsmöglichkeiten, die das Urheberrecht vorsieht, ersetzen durch individuell lizensierte Nutzungen, es würde damit die Sozialbindung des geistigen Eigentums abschaffen (V. Grassmuck, HU Berlin). Was im real gestorbenen Sozialismus beliebtes Zensurmittel war, die Kontrolle über Vervielfältigungsgeräte aller Art, findet im übrig gebliebenen Kapitalismus einen würdigen Nachfolger. Eine Technik wie TPM ist eine mögliche Basis dafür.

Das Trusted-Computing-Konzept bietet sich natürlich nicht nur für Unternehmen an, auch staatliche Einrichtungen sind sehr interessiert: Anwendungen können Dokumente für einen bestimmten Adressatenkreis ausschließlich verschlüsselt und mit eingeschränkter Nutzung erstellen. Eine solche erzwungene Zugangskontrolle schaltet den Menschen als wichtigsten Unsicherheitsfaktor weitgehend aus, unerwünschte Lecks beispielsweise in Richtung Medien können kaum noch vorkommen. Sollte die organisierte Kriminalität diese Funktionen nutzen wollen (und das wird sie sicherlich), lässt sich vorbeugen: Die *Hintertür* für die Sicherheitsbehörden kann gesetzlich erzwungen werden, auch wenn Firmenvertreter von Microsoft derartige Absichten eindeutig verneinten.

Die informationelle Selbstbestimmung als das Recht, selbst zu entscheiden, wer was über uns weiß, sahen mehrere Teilnehmer bedroht. Sie könnte auch laut BITKOM-Erläuterungen gefährdet sein:

> *„... besteht die Befürchtung, es könnten Konfigurationsdaten des Computers, die beim Zugriff auf Web-Angebote auf einem externen Server abgeglichen werden, von Dritten eingesehen und missbraucht werden."*

Für BITKOM aber kaum Grund zur Beunruhigung:

> *„Die Weitergabe von Konfigurationsdaten an externe Server ist jedoch vom TCPA-Konzept nicht vorgesehen. Ohnehin würden Gefahren, die sich für die informationelle Selbstbestimmung des Nutzers ergeben könnten, durch die bestehenden datenschutzrechtlichen Regeln abgefangen."*[6]

So optimistisch waren die Kritiker nicht. – Ein Diskussionsbeitrag sah die Freiheit der Nutzer durch die kommende Infrastruktur eingeschränkt: Zwar können die Nutzer das Trusted Platform Module abschalten, wenn sie aber bestimmte Webdienste in Anspruch nehmen möchten, entscheidet deren Anbieter über die Verwendung des TPM. In diesem Fall können die Nutzer also lediglich zwischen verschiedenen Anbietern auswählen und das nur solange der Wettbewerb funktioniert. Datenschützer[7] betrachten eine zwangsweise online-Registrierung als rechtswidrig und die Kontrolle von Nutzungsverhalten im privaten Bereich als illegal. Einen Anforderungskatalog haben sie der TCG bereits übergeben. Koenig stellte die berechtigte Frage, welchen Einfluss die Forderungen der Datenschutz-Beauftragten auf die Spezifikationen der TCG haben und erwartet *protokollfeste Ergebnisse.*

Datensicherheit

Eine Gruppe von Studierenden an der TU Berlin, Institut für Informatik und Gesellschaft, sieht folgende Schwierigkeiten:

> *„Das Hauptproblem ‚Break-once-run-everywhere' […] ist noch nicht beseitigt. Um zu verhindern, dass Datenübertragungen [...] abgefangen werden, bevor sie plattformabhängig verschlüsselt werden und so nur noch auf einem bestimmten Computer oder Handy laufen, müsste [...] viel mehr getan werden als das TPM leisten kann."*[8]

Und zum Thema Datensicherung:

> *„Sicherungskopien von unternehmenskritischen Daten, die an die TPMs der entsprechenden Datenserver gebunden sind, könnten im Falle eines Hardwaredefekts unwiederbringlich verloren sein."*[9]

Zu diesem Argument, das auch der CCC anführt, wandte Dirk Kuhlmann, HP, ein, dass die *Sealed Storage* (sicherer Speicherbereich) als geschützter Ort für sensible Daten wie Schlüssel sich auf einem Firmenserver kontrolliert duplizieren lässt. Ein Backup der Schlüssel sei nur für Einzelplatz-Rechner ausgeschlossen. – Die Gruppe von der TU Berlin fordert kundenfreundliche, durchsetzbare Datenschutzbestimmungen und empfindliche Strafen für Datenmissbrauch, damit Kunden dem TCPA-Ansatz vertrauen könnten.

Der CCC brachte weitere Probleme ins Gespräch: *verborgene Kanäle,* über die geheime Schlüssel der Nutzer übertragen werden könnten und die damit den Zugriff auf alle damit verschlüsselten Informationen möglich machen, und die bisher unvollständige Kontrolle der Nutzer über alle auf ihrem Rechner verwendeten Schlüssel.

Wettbewerbsrechtliche Einwände

Zwei Einschränkungen der Nutzer-Autonomie beanstandete Anderson besonders: *Locking-in* und *Product-Tying*. Locking-in bezieht sich auf die Bemühungen der Quasi-Monopolisten, ihre Kunden mit proprietären Formaten, De-facto-Standards und Software-Architekturen am Herstellerwechsel zu hindern. Product-Tying bezieht sich auf Zubehör, das einen wesentlichen Beitrag dazu leistet, bestimmte Produkte wie Drucker oder Handies unter Preis zu verkaufen, weil das Zubehör überteuert angeboten wird und billigere Konkurrenzprodukte ausgesperrt werden. Ein gutes Beispiel sind die Akkus für Handies, die zum Aufladen einen Authentifizierungscode des Herstellers abfragen. Billigere Konkurrenz-Akkus lassen sich mit dem zugehörigen Ladegerät nicht aufladen. Mit der Einführung des Trusted Computing wird nach Andersons Ansicht die Kontrolle der Nutzer nach dem Kauf aber noch einfacher.

Anderson wurde deutlich in Bezug auf Palladium und TCPA. Seine Kritik besagt, dass der Begriff „trusted" mit Vertrauen nichts zu tun hat und lediglich bedeutet, dass ein Programm auf einem PC für Dritte vertrauenswürdig wird, denn sie können dann feststellen, ob es verändert wurde, eine für das *Digital Rights Management* entscheidende Voraussetzung. Nur dann können die Anbieter von Inhalten entscheiden, auf welchen Plattformen und mit welcher Software ihre Waren genutzt werden dürfen. Sie können unlizensierte Software aussperren, über die Art oder Häufigkeit der Nutzung von Inhalten bestimmen und den Preis entsprechend gestalten, über kurz oder lang direkt von ihren Servern aus. Regierungen können mit Hilfe gestaffelter Sicherheitsebenen (*Multi-Level-Security-Levels*, *MLSL)* den Zugang zu ihren Informationen regeln. Auch für den Mail-Verkehr lassen sich Einschränkungen vorab festlegen: Mails sind druckbar oder nicht, Lesbarkeit nur bis zu einem bestimmten Datum, Weiterleitung erlaubt oder nicht, ... Ob solche Einschränkungen sich mit nationalem Recht vereinbaren lassen, ist mehr als fraglich, oft stehen Aufbewahrungsfristen dem entgegen.

Aus wettbewerbsrechtlicher Sicht entscheidend ist aber die Kontrolle der Anbieter über das Nutzungsverhalten nach einem Kauf. Quersubventionierungen von Hardware durch Software-Verkäufe ist das eine Problem, die Bindung der Nutzer an bestimmte Produkte und Plattformen das andere, wenn die Kosten für einen Wechsel zur Konkurrenz *(Switching Costs)* so hoch werden, dass der sich fast automatisch ausschließt. Zur Zeit entstehen bei einem Wechsel Kosten für Schulungen, die Konvertierung der Datenbestände, möglicherweise inkompatible Prozesse. Beim Wechsel von MS-Office zu einer Open-Source-Plattform wie Linux sind diese Kosten etwa vergleichbar mit den geltenden Lizenzgebühren. Sollte Trusted Computing sich als Standard durchsetzen, könnte der Wechsel nicht nur teurer werden sondern womöglich undurchführbar, weil sich beispielsweise die Zugriffsrechte auf verschlüsselte Dokumente durch eine andere Anwendung nur nach Genehmigung durch den Eigentümer (Ersteller) ändern ließen, was nach vielen Jahren der Geschäftsbeziehungen mit unzähligen Kunden ein gewaltiger Aufwand wäre.[10]

Heftige Debatten entspannen sich auch über die Spezifikationen der TCG, über Patente auf einzelne Komponenten und darüber, dass diese Rahmenbedingungen viele kleine und mittlere Software-Anbieter (KMU) und die gesamte Open-Source-Gemeinde ausschließen könnten. So ist die Mitgliedschaft in der TCG teuer, selbst Mitglieder ohne Entscheidungsrecht *(adapters)* zahlen mit 7.500 $US einen hohen Beitrag.

Die Spezifikation ist laut Koenig zwar für ITler, nicht aber für Juristen transparent; das Verfahren ist es überhaupt nicht. In Fällen einer möglichen Marktdominanz durch abgestimmte Verhaltensweisen stellt das Wettbewerbsrecht erhöhte Anforderungen an eine Mitgliedschaft im Standardisierungsprozess. – Die Lizensierung der TCG gilt aber nur gegenüber Mitgliedern, auch die Vereinbarungen für Patente nach *RAND (Reasonable and non-discriminatory licensing)* gelten nur für Mitglieder und der tatsächliche Umgang mit den Patenten bleibt abzuwarten. Nichtmitglieder der TCG haben keinerlei Einfluss und werden in ihrem Wissen über die Entwicklungsvorgaben nachhinken. Eine Ausnahme von kartellrechtlichen Auflagen (Freistellung) kann es übrigens bei angemessener Beteiligung der Verbraucher geben, oder wenn das Gremium den technischen oder wirtschaftlichen Fortschritt besonders fördert. Es darf dann aber keine Beschränkungen durch die beteiligten Unternehmen geben oder Möglichkeiten für sie, für einen wesentlichen Teil der betreffenden Waren den Wettbewerb auszuschalten.

Konstruktive Vorschläge

Eberhard Becker von der Universität Dortmund, Moderator der Arbeitsgruppe „Medienwirtschaft, DRM und Trusted Computing Group" (Section 4) gab einige Hinweise, wohin die TCG sich bewegen sollte: Sie sollte in ihre Reihen auch Non-profit-Organisationen und Vertreter der Open-Source-Gemeinde aufnehmen, wirklich durchsetzbare Sicherheitspolitiken implementieren und die Haftung der Hersteller verbessern, damit könne sie öffentliches Vertrauen erringen.

Von verschiedenen Seiten, besonders den Datenschützern, wurde die Forderung nach überprüfbarem offenem Code ge-

stellt, aber auch weitere konkrete Anforderungen. So müsse der Zugriff auf Daten ohne Protokolle möglich sein. Der Schutz der Urheberrechte lasse sich auch ohne Protokollierung erreichen, dafür sind die Verwertungsgesellschaften einzubeziehen. Die Nutzung müsse auch ohne Internet-Zugang möglich sein, und Updates ohne Einwilligung der Nutzer ausgeschlossen. Es müsse Wahlfreiheit geben: Jede und jeder müssten ihre vertrauenswürdige Instanz selbst aussuchen können, denn wenn dabei ein faktischer Zwang vorhanden sei, könne kein Vertrauen entstehen.

In der Diskussion wurde auch eine *vorlaufende* Regulierung durch EU und nationale Regierungen gefordert. In manchen Bereichen ergibt sich eine Deckung von Wettbewerbs- und Datenschutz-Recht, Vertreter beider Rechtsgebiete sollten also zusammenarbeiten.

Die TCG machte Angebote: Sie will ihre Öffentlichkeitsarbeit verbessern und mit den Kritikern zusammenarbeiten. Auch wenn es bisher bei der TCG keine kostenlose Mitgliedschaft gibt, kündigten ihre Vertreter doch an, zwei beitragsfreie Liason-Mitgliedschaften anzubieten.

Fazit

Ein Problem zog sich durch die gesamte Diskussion auf dem Symposium – die fehlende Trennung zwischen den Nutzer-Gruppen. Anvisierte Nutzer der Trusted Computing Group sind vor allem die Unternehmen *(business user).* Unternehmen, die für eine große Gruppe von Mitarbeiterinnen und Mitarbeitern sichere PCs einsetzen und die Anwendungen oder Dienste kontrollieren möchten, haben ein legitimes Interesse daran, dass diese Mitarbeiter an stabil konfigurierten PCs arbeiten und dort nur die Software einsetzen, die Dienste nutzen und die Inhalte abrufen, die für ihren Aufgabenbereich im Unternehmen erforderlich sind. Privatkopien von urheberrechtlich geschützten Inhalten spielen kaum eine Rolle, der Wunsch der Nutzer, von ihrem PC vielseitig Gebrauch zu machen, ebenso wenig. Informationelle Selbstbestimmung ist zwar ein Grundrecht der Mitarbeiterinnen und Mitarbeiter, wird im betrieblichen Alltag aber leider klein geschrieben.

Privatpersonen dagegen, die ihren PC als Allzweck-Computer schätzen, die eine Film- oder Musiksammlung auf der Festplatte anlegen wollen, ihre Anwendungen beliebig oft ergänzen, umkonfigurieren oder deinstallieren wollen, haben naturgemäß massive Vorbehalte gegenüber einer Sicherheitssoft- und -hardware, die ihre Autonomie einschränkt. Wie betriebliche Nutzer wollen sie selbst entscheiden, was sie im WWW nutzen, herunterladen, weiterleiten, kopieren, usw. – aber sie unterliegen keiner Abwägung von Interessen mit einem Arbeitgeber. Sie haben den Wunsch und legitimen Willen, sich nicht von einer angeblich sicheren Plattform bevormunden zu lassen. Daran könnte das Konsortium sich noch die Zähne ausbeißen, denn Microsofts Ruf ist durch eigene Schuld so beschädigt, dass seine friedlichen Kompromissangebote und Zusagen, Kritik zu berücksichtigen, während des Symposiums regelmäßig auf deutliche Zweifel stießen. Auch Intel hat bereits mit dem Pentium III schlechte Erfahrungen gemacht, und hatte darüber gelogen, auch das wurde ihm zu Recht vorgeworfen. Immer wieder machten die Hersteller zu Datenschutz-relevanten Themen Aussagen des Inhalts, dass sie dieses oder jenes sowieso nicht vorhätten. Hat sich damit der Zweck des Symposiums erfüllt oder handelt es sich um eine Ausrede, weil die Technik noch nicht besteht? Es fragt sich, ob es der TCG gelingen wird, ein eigenes Image aufzubauen, unbeschädigt vom lädierten einiger Mitglieder?

Ein weiteres Problem für die Verständigung unter den Teilnehmern war deren unterschiedliche fachliche Herkunft: Bit-Fiesler und Vertreter von Organisationen der Zivilgesellschaft, Behördenvertreter oder Marketing-Experten, Anwälte und andere Mitglieder der juristischen Fakultät, Informatikerinnen und Informatiker, alle versuchten, aus ebenso verschiedenenartigen Vorträgen Honig zu saugen. Diese (seltene) Art von Experiment ist sicher sehr zu begrüßen, zumal sich der Moderator des ersten Tages, Christian Koenig, zum Anwalt des Publikums machte und Zeit für die Diskussion freizuschaufeln versuchte, wo es nur irgend ging. Ein Diskurs zwischen unterschiedlichen Mitgliedern der Gesellschaft also, der sicher lohnte.

Zu kritisieren ist allerdings der Veranstalter TimeKontor AG, der nicht nur einen besonderen Beleg für IT-Sicherheit lieferte, indem er meine Teilnahmebestätigung zunächst an ein Berliner Unternehmen faxte, bevor er es mir dann mit handschriftlicher Notiz des Erst-Empfängers richtig zustellte. Trotz seiner Aussage, dass die Teilnehmer „nach zeitlichem Eingang der Anmeldungen“ ausgewählt würden, wählte er das FIfF e.V. komplett aus der Teilnahme heraus: zwei seiner Vertreter hatten sich vor mir angemeldet, wurden aber abschlägig beschieden.

Was Ross Anderson feststellt, scheint mir eine gute Zusammenfassung des Symposiums. IT-Sicherheit nähert sich einer ethischen und politischen Krise; sie wird nicht zum Schutz der Privatsphäre genutzt, sondern um Investitionen, Businesspläne u.a. zu schützen. Die Krise allerdings ist nicht wirklich neu, der Dualismus zwischen wirtschaftlichen und grundrechtlichen Interessen auch nicht. Regierungen haben dafür zu sorgen, dass es weiterhin Wettbewerb zwischen den Hard- und Software-Anbietern gibt. Das kann keine rein rechtliche, sondern muss auch eine ökonomische Diskussion sein.

1 *www.trustedcomputinggroup.com*
2 *auch Fritz-Chip genannt, zu Ehren des US-Senators Fritz Hollings, der TCPA als zwingenden Bestandteil sämtlicher Konsumelektronik propagiert (http://moon.hipjoint.de/TCPA-paladium-faq-de.html, Stand 18.5.2003)*
3 *weitere Geräte der Konsumelektronik könnten folgen*
4 *Application Programming Interface*
5 *So eine auf dem Symposium ausliegende FAQ von R. Anderson in Übersetzung von Moon vom 18.5.2003, http://moon.hipjoint.de/tcpa-palladium-faq-de.html. Diese Aussage ließ sich aber nicht bestätigen.*
6 *Bundesverband Informtaionswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM): Erläuterungen – Trusted Computing Platform Alliance (TCPA); vorgelegt beim Symposium*
7 *Alexander Dix, Landesbeauftragter für Datenschutz in Brandenburg*
8 *Luther, Katja et al: TCPA = DRM? Beitrag zum Symposium „Trusted Computing Group“ im BMWA, 2. und 3. Juli 2003*
9 *a.a.O.*
10 *Upgrade IV, 6/2003, S. 38*

Peter Bittner

Videoüberwachung und Bürgerrechte
Ein Jahr überregionaler Arbeitskreis

Seit der Konstituierung des Arbeitskreises im Rahmen des Kongresses „Save Privacy – Grenzverschiebungen im digitalen Zeitalter" am 7. Juni 2002 ist mehr als ein Jahr vergangen. Zeit also, über das bisher Geschehene und Erreichte zu berichten und die nähere Zukunft in den Blick zu nehmen.

Workshops

Neben der Gründungsveranstaltung auf dem *Save-Privacy*-Kongress hat der Arbeitskreis mittlerweile drei Workshops veranstaltet. Sie waren allesamt stark interdisziplinär zusammengesetzt – wie der AK selbst. Der erste Workshop fand am 16. August 2002 in Bielefeld statt. Dort wurden neben ersten thematischen Fragen (Städtebau, Recht, Gegenwehr) v.a. auch Fragen der inneren Organisation des AK und möglicher Projekte (FAQ, Buch) diskutiert.

In Freiburg gab es im Rahmen der FIfF-Jahrestagung am 19. Oktober 2002 einen eher allgemeinen Workshop zur breiten thematischen Bestandsaufnahme, Analyse und Gegenwehr. So berichtete Leon Hempel aus dem EU-Projekt *Urbaneye,* Nils Leopold zeigte aktuelle politische und juristische Entwicklungen auf, Francisco Klauser führte in seine humangeographischen Forschungen ein und zeigte sozialräumliche Konsequenzen von Videoüberwachung (VÜ) auf.

Der dritte Workshop in Berlin fand am 11. April 2003 in Kooperation mit dem *Zentrum Technik und Gesellschaft* der TU Berlin statt. Unter dem Thema „Bild – Raum – Kontrolle" fanden sich etwa 30 Teilnehmende zusammen, um sich über Analyseansätze zur Videoüberwachung auszutauschen. Dabei ging es in insgesamt sieben Beiträgen um die Frage, inwieweit bestimmte Aspekte, wie die Bedeutung der Bilder oder die Veränderung von Räumen durch die Videoüberwachung neue Strategien der (Selbst-)Kontrolle herbeiführen. Im Vordergrund standen medien-, sozialwissenschaftliche und geographische Ansätze.

Der vierte Workshop am 22. November 2003 findet wieder im Rahmen der FIfF-Jahrestagung statt (siehe AG e-identity) und widmet sich der Frage biometrischer Daten in Ausweispapieren. Diese Frage hängt eng mit der der Videoüberwachung zusammen, denn mit der *biometrischen Verdatung* wird auch gleich eine Referenzdatenbank entstehen, die zum Abgleich von Gesichtern sehr nützlich sein dürfte.

Auch für das Frühjahr 2004 gibt es schon erste Planungen: Im dann schon fünften Workshop soll die Frage der Evaluation von polizeilicher Videoüberwachung im Mittelpunkt stehen.

Publikationen und Interviews

Das mit der FIfF-Kommunikation 1/2002 (Schwerpunkt Videoüberwachung) avisierte Buchprojekt verzögert sich, es ist beileibe nicht so, dass wir nicht auf hinreichend Material zählen könnten. Momentan fehlt es an der Zeit, die Konzeption des Buches voranzutreiben. Dass wir damit den Beitragenden viel Geduld abverlangen, ist den Herausgebenden bewusst.

In der Zwischenzeit sind dafür aus dem AK heraus einige Beiträge (ohne Anspruch auf Vollständigkeit) entstanden, auf die ich aufmerksam machen möchte:

- Leopold, Nils (2003): Videoüberwachung auf Straßen und Plätzen – aus rechtlicher Sicht. Deutsches Polizeiblatt, 1/2003, S. 13-16.
- Hempel, Leon; Bittner, Peter (2003): Zur Evaluation von Videoüberwachung. Deutsches Polizeiblatt, 1/2003, S. 27-32.
- Hempel, Leon; Töpfer, Eric (2003): Videoüberwachung in Berlin. CILIP 74, 1/2003.
- Hempel, Leon (2003): Verdrängen statt Vorbeugen. Zur mobilen Videoüberwachung in Deutschland. Telepolis, 15.01.2003; *http://www.heise.de/tp/deutsch/inhalt/co/13928/1.html*

In zahlreichen Interviews haben sich die Aktiven des AK zu Fragen der Videoüberwachung geäußert, was sich in diversen Presseveröffentlichungen niederschlägt.

Peter Bittner

Peter Bittner, Diplom-Informatiker, arbeitet als wissenschaftlicher Mitarbeiter im Bereich *Informatik in Bildung und Gesellschaft* an der Humboldt-Universität Berlin. Arbeitsschwerpunkte sind u. a.: *Theorien der Informatik, Profession und Verantwortung, Informatik in Überwachungskontexten.* Er ist seit 1995 im FIfF-Vorstand.

Prozesse und Projekte

Aufmerksamkeit erhielten wir dabei immer wieder durch die von den Juristen unter unseren Mitgliedern begleiteten Prozesse, sowohl verwaltungsrechtlicher Art, wie im Falle „Ravensberger Park" in Bielefeld, als auch zivilrechtlicher Art, wie im Falle „Kulturkaufhaus Dussmann" oder „Humboldt-Universität" in Berlin.

Neben der Verfolgung der Prozesse und der Dokumentation der Rechtsnormen zur Videoüberwachung haben wir uns für die nächste Zeit vorgenommen, die Pilotversuche in Deutschland gesammelt zu dokumentieren. Mittlerweile gibt es ja in zahlreichen Städten Tests oder gar einen *Normalbetrieb*. Für dieses Vorhaben benötigen wir aber eure Unterstützung: Bitte schickt uns Belege von lokalen Publikationen, die über Videoüberwachung berichten. Diese Bitte betrifft auch Unterlagen, die den politischen Entscheidungsprozess pro/contra Videoüberwachung darstellen ... oder Hinweise auf Kosten, Verfahrensweisen etc. geben. Die Adresse findet ihr beim folgenden Beitrag, dem Schreiben an die *Art. 29 Datenschutzgruppe der EU*.

Web und Mailing-Listen

Nachdem leider die Mailing-Listen zu sehr mit Spam bedacht wurden (was nicht am bisherigen Provider lag) und sich die moderierte Liste für Diskussionen als wenig brauchbar erwiesen hat, haben wir diese eingestellt. Mit dem im Juli/August vollzogenen Providerwechsel gibt es neue Mailing-Listen; gegen Ende August erfolgt dann auch ein Relaunch der Webseiten; sie werden dann direkt unter http://www.ak-videoueberwachung.de erreichbar sein, also ohne Umleitungen. Bei dieser Gelegenheit soll auch bei den Inhalten kräftig nachgelegt werden. Über Einsendungen, die wir auf der Website veröffentlichen dürfen, würden wir uns sehr freuen.

Zu guter Letzt ...

haben wir uns auch international in Sachen Videoüberwachung und Bürgerrechte eingemischt.

Die *Art. 29 Datenschutzgruppe der EU,* die gemäß Artikel 29 der Richtlinie 95/46/EG zum Schutz der persönlichen Daten eingesetzt wurde und aus Vertretern der europäischen Datenschutzbeauftragten und -kommissare besteht, hat ein Arbeitsdokument (http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp67_de.pdf) mit einer ersten Analyse der Anwendung der Datenschutzrichtlinie im Bereich Videoüberwachung erstellt. Mit einer öffentlichen Anfrage (http://europa.eu.int/comm/internal_market/privacy/workingroup/consultations/consultation_de.htm) wollte die Datenschutzgruppe einen Überblick über die Meinungen der verschiedenen Interessengruppen hierzu bekommen.

Da in einer zweiten Phase die Gruppe der europäischen Datenschutzkommissare möglicherweise eine Empfehlung zu diesem Thema annehmen wird, haben wir uns entschlossen, einen Beitrag zur Diskussion zu leisten. Pünktlich ging deshalb ein Papier des AK mit zahlreichen unterstützenden Unterschriften an die Art. 29 Datenschutzgruppe. Es folgt diesem Bericht.

Arbeitskreis Videoüberwachung & Bürgerrechte
c/o Peter Bittner
Humboldt Universität zu Berlin
Institut für Informatik
Unter den Linden 6
D - 10099 Berlin, Germany

Fax: +49-(0)30-2093-3168
Email: *cctv@fiff.de*
Internet: *www.ak-videoueberwachung.de*

30 May 2003

Consultation of the Art. 29 Data Protection Working Party on Video Surveillance

Opinion of the Working Group on Video Surveillance and Civil Rights

Experiencing video surveillance almost every day, we welcome the initiative taken by the Article 29 Data Protection Working Party to address the issue at a European level. As a network of concerned citizens and interested researchers we are grateful for the opportunity to help the efforts to develop a "general viewpoint" on how to prevent "unjustified restrictions in the citizens' rights and fundamental freedoms" in face of the rapid proliferation of CCTV, Intranet and Internet cameras that accompanies a rising culture of risk, suspicion and control.

In Germany hundreds of thousands cameras monitor every day life in a growing number of publicly accessible spaces – many of them nearly covert and without signage. Police forces in around 20 cities operate open-street CCTV systems at public areas said to be "crime hotspots".. Moreover, the police observe demonstrations and other crowds by mobile means, and covert cameras are deployed for criminal investigation purposes. There is clear trend towards interconnection of already existing camera systems. Public-private partnerships blur the line between state and corporate surveillance. Most of the recently installed systems operate on a digital basis, and first major pilot projects with automatic facial or licence plate recognition are underway at border points and airports.

In total, nearly 40 acts regulate without effectively limiting the use of video surveillance in Germany. Among others 16 state police acts, two federal police acts, the code of criminal procedure, the federal data protection act and 16 state data protection acts govern the deployment of video surveillance in different ways depending on who is the data controller and what type of monitored location. This may serve as to illustrate the difficulties of adopting a "systematic and harmonised approach".

The use of video surveillance is representing a peculiar social technique with exceptional consequences which barely seem to be met by common data protection laws. In contrast to many other forms of data processing that require the informed con-

sent of the data subject, video surveillance allows to collect, store and process personal data covertly and without interaction between the controller and the data subject . The only way to opt out of this form of data processing is to avoid locations under surveillance. Clearly the right of the data subjects to object to being filmed as laid down in Article 14 of the Directive cannot be applied effectively. Moreover, the more or less opaque character of the collection, storage and processing of personal data by the means of video surveillance threatens to undermine the ability of the observed to make an informed and autonomous decision on the acceptance or avoidance of such data processing by video surveillance. The mere existence of a camera – even if notified – does hardly tell the relevant details. Whether it is a dummy camera, a single camera system without storage capacity, or a camera of a large and sophisticated system additionally linked to third parties remains unknown to the citizens which happen to be affected in large quantities and for no apparent reason but broadly alleged prevention purposes. Thus, we see the relation of information that the observers hold on the observed and vice versa – which in fact is an asymmetric relation of power – as crucial for the systematic assessment and regulation of video surveillance.

Having said this, we would like to point out the following issues.

- Since data controllers cannot assume informed consent of the data subjects per se the employment of video surveillance in public and publicly accessible space should only be allowed for a limited set of clearly defined purposes. Art. 6b and Art. 7 should of Directive 95/46/EC should help to prevent both the exhaustive spread of video surveillance systems and the expandable mutability that characterises their use at the moment.

- Pictures in a way seem to be more open to interpretation by the individual controller. Therefore the regulatory approach must also address problems of this "openness" coming with pictures which also seem to undermine the principle of purpose specification. In order to ensure both compliance with Art. 6b and Art. 7 and the proportionality of video surveillance which is a socio-technical rather than simply a technical device the operators of video surveillance systems, in particular control room staff, must be trained and managed in an appropriate manner. This may serve as to limit the possible discriminating use and misleading conclusions drawn from picture materials.

- The commandment of information should be enhanced as a balance weight against the asymmetric relationship of vision between the data controllers and the data subjects. In line with Art. 10 and Art. 11 data subjects should not only be informed about the operation of video surveillance, the identity of the data controller and its purpose but also about the core features of systems such as storage of footage or possible linkages to third parties.

- Given the definition of personal data as "any information relating to an identified or identifiable natural person" by Art. 2 it should be clarified if and how the oral exchange of information drawn from the processing of image data is touched by the Directive. Such practices are evident for technical and social networks of video surveillance systems and their operators for instance within police-private-partnerships. If not addressed, this problem could easily lead to an arbitrary practice of networks informally exchanging information referring to identifiable persons.. This problem in a way seem to have been met by German laws through specific data controller obligations of keeping gathered knowledge on single persons secret.

Finally, we wish to address the following issues going beyond the scope of the Directive but which, however, are closely related to it.

- Privatisation and securitisation are not just catchwords. Although the Directive does not apply to video surveillance carried out by public crime control and national security authorities, we observe – as mentioned above – that the lines between the work and the specific tasks of these public bodies and other private data controllers where the Directive is wholly applicable are increasingly blurring. Thus, these hybrid areas of surveillance activities need increased attention and eventually regulation. We expect the Working party therefore to promote an understanding of the Data Protection Directive which strengthens its decisive meaning and impact as the common aquis also within the remaining third and second pillar of the European Union. The current discussion of a growing "European space of freedom, security and rule of law"(Constitutional Convention draft papers) should consequently be enriched by stressing the legal achievements of the EU in its first pillar activities.

- To support the assessment of the proportionality of video surveillance in general and the deployment of advanced applications in particular, professional but independent evaluations of their effectiveness in terms of declared purposes and other possible impacts and consequences, especially with respect to the basic prerequisites of open and democratic societies are necessary.

- Last but not least, the wide gap between the provisions of the Directive and the current reality in the practices and use of video surveillance show that the Directive is an important but rather weak framework if not completed by an efficient regime of control and penalties.

Signatories for the Working Group

1. Ralf Bendrath, political scientist, University of Bremen
2. Peter Bittner, computer scientist, Humboldt-University at Berlin, Vice Chairman FIfF e.V. (Computer Professionals for Peace and Social Responsibility)
3. Leon Hempel, research assistant, Technical University Berlin
4. Nils Leopold, lawyer, Managing Director Humanistische Union e.V.
5. Eric Töpfer, political scientist, Technical University Berlin

Marie-Theres Tinnefeld

Der Bundesbeauftragte für den Datenschutz

Denkanstöße zur Wahl des neuen Bundesbeauftragten

Die Einführung der parlamentarischen Wahl des Bundesbeauftragten für den Datenschutz gehört zu den markantesten Neuerungen der BDSG-Novellierung von 1990. Am Ende dieser Legislaturperiode läuft die Amtszeit des bisherigen Amtsinhabers Dr. Joachim W. Jacob aus. Aus diesem Grunde ist es sinnvoll, sich mit der bedeutendsten Kontrollinstanz in Deutschland zu beschäftigen.

Im Volkszählungsurteil von 1983 formulierte das Bundesverfassungsgericht flankierende verfahrensmäßige Schutzvorkehrungen wie Informations-, Korrekturrechte und Schadensersatzansprüche zugunsten von Bürgerinnen und Bürgern. Sie sind in Einzelfällen von beträchtlicher Bedeutung und sollen vor Machtmissbräuchen schützen. Sieht man indessen etwas näher hin, so kann es für die Betroffenen angesichts der komplizierten gesetzlichen Regelungen schon sehr schwierig sein, ihre Rechte wahrzunehmen. Das Bundesverfassungsgericht hat diese schwache Position des Einzelnen gesehen und daher die Einrichtung und Beteiligung von unabhängigen Datenschutzbeauftragten verlangt. Die Chancen, welche das Grundrecht auf Datenschutz derzeit bietet, rechtfertigen keine optimistische Einschätzung, wenn man die zunehmende Telefonüberwachung, Lauschangriffe und Videokontrolle, unbemerkte Fernüberwachung am Arbeitsplatz usw. betrachtet. Um so wichtiger sind Datenschutzbeauftragte, die als ein *Stück vorgezogenen Rechtsschutzes* für die Einhaltung der Vorschriften zum Schutz der Bürgerinnen und Bürger Sorge zu tragen haben.

Die EG-Datenschutzrichtlinie von 1995 fordert gleichfalls, dass in den Mitgliedstaaten eine oder mehrere unabhängige öffentliche Stellen mit der Kontrolle des Datenschutzes beauftragt werden. Entsprechend der föderalen Struktur in Deutschland wurden im Bund und in den Ländern mittlerweile überall staatliche Datenschutzbeauftragte eingerichtet. Sie tragen eine besondere Verantwortung, weil sie im Interesse des Einzelnen einen vorgezogenen Rechtsschutz durchsetzen müssen. Zu ihrem Aufgabengebiet gehört also die präventive Umsetzung und Anwendung rechtlicher Grundsätze, verbunden mit einem besonderen Blick für ihre technischen Rahmenbedingungen! Eine herausragende Stellung unter den Kontrollinstanzen hat der Bundesbeauftragte für den Datenschutz (BfD).

Der BfD ist nach dem BDSG 2001 (§§ 22-26) auch zuständig für die Bundesbehörden und andere öffentliche Stellen des Bundes, für Telekommunikationsunternehmen, die deutsche Post AG und andere Unternehmen, soweit diese geschäftsmäßig Postdienstleistungen erbringen. Er wird nicht nur vom Parlament in Berlin gewählt, sondern ist auch Berater der Volksvertretung von erheblichen politischen Gewicht. Anders und präziser formuliert nach den Worten des ehemaligen Mitglieds des Bundestages Dr. Burkhard Hirsch (StenBer. Vom 31. 5. 1990, 12/16783 f.): Er ist „der verlängerte Arm, das Ohr und Prüfungsinstrument des Parlaments". Dem BfD kommt somit eine herausragende Stellung innerhalb der Kontrollinstanzen in Deutschland zu. Die Bundesregierung sieht in der am 26. 7. 2000 beschlossenen neuen Geschäftsordnung der Bundesministerien (GGO) ausdrücklich eine frühzeitige Beteiligung des BfD bei allen Vorhaben vor, die seine Aufgaben berühren. Der BfD hat außerdem eine wichtige Koordinationsaufgabe, da er zwischen den Datenschutzbeauftragten der Länder und den Aufsichtsbehörden auf konstruktive Abstimmungen im Feld des Datenschutzes hinzuwirken hat. Er hat zudem eine integrative Aufgabe bei der Mitwirkung in überregionalen (*Ständige Konferenz der Datenschutzbeauftragten des Bundes und der Länder* und *Düsseldorfer Kreis* der Aufsichtsbehörden der Länder) sowie bei internationalen Zusammentreffen im Rahmen des europäischen Gemeinschaftsrechts. Während der deutschen Präsidentschaft im Jahre 1994 hatte der deutsche BfD Dr. Joachim Jacob den Vorsitz in der *Ratsgruppe Wirtschaftsfragen,* die die Fertigstellung der gemeinschaftsrechtlichen Datenschutzrichtlinie 95/46/EG entscheidend voranbrachte. Helmut Heil (Computer und Recht 199, S. 274) spricht von „The happy coincidence of a German Presidency". Der BfD benötigt also besondere kommunikative und integrative Fähigkeiten, wenn er seine Aufgaben effizient wahrnehmen soll!

Für die Tätigkeit des BfD sind die Mittel der Information, der Aufklärung, Anregung und der Kritik bis zur Ebene des Parlaments von besondere Bedeutung. Hier spielt die Musik in den Tätigkeitsberichten, also der Veröffentlichung seiner Kontrollergebnisse. Sie gelten als eine wichtige Erkenntnisquelle und authentische Interpretation des geltenden Rechts und enthalten zugleich technische datenschutzrelevante Lösungsansätze. Das bedeutet, dass der BfD über juristische, insbesondere über menschen- und grundrechtliche Datenschutzkenntnisse verfügen muss sowie ein Gespür für eine entsprechende Technikgestaltung!

Prof. Dr. Marie Theres Tinnefeld

Prof. Dr. Marie-Theres Tinnefeld ist Juristin und Publizistin mit Schwerpunkt Datenschutz- und Wirtschaftsrecht. Sie ist verantwortlich für die Ausbildung für betrieblichen Datenschutz an der Fachhochschule München und Mitglied im wissenschaftlichen Beirat des FIfF.

Der herausgehobenen Funktion des Bundesbeauftragten gegenüber der Bundesregierung bzw. Bundesverwaltung entspricht die seit der Novelle 1990 gesetzlich geregelte Wahl des Bundesbeauftragten durch den Deutschen Bundestag. Sie wurde auf Betreiben des Innenausschusses in das Gesetz aufgenommen und unterstreicht den Willen der Volksvertretung, den Bundesbeauftragten demokratisch zu legitimieren und sein politisches Gewicht zu erhöhen: Der BfD muss danach auf Vorschlag der Bundesregierung mit mehr als der Hälfte der gesetzlichen Zahl der Mitglieder gewählt werden (§ 22 Abs. 1 Satz 1 BDSG). Derzeit verfügt das Parlament über 603 Abgeordnete. Zur Wahl des BfD würden daher 302 Stimmen genügen. Die rot-grüne Koalition verfügt über 306 Stimmen, also über vier Stimmen mehr als für die Wahl mindestens erforderlich sind.

Bei dem Amt des BfD handelt es sich jedoch um ein parteipolitisch neutrales Amt mit einer verfassungspolitischen Signalwirkung. Es wäre daher wünschenswert, wenn die Bundesregierung eine Kandidatin/einen Kandidaten vorschlagen würde, die/der sich auf eine breite Mehrheit im Parlament stützen könnte. Eine vorherige Abstimmung mit der Opposition wäre nicht ungewöhnlich, wie die Ergebnisse der letzten beiden Wahlen zeigen: Der amtierende BfD Dr. Joachim Jacob wurde bereits bei seiner ersten Wahl 1993 mit einer breiten Mehrheit von 459 der 482 abgegebenen Stimmen und bei seiner Wiederwahl 1998 mit 562 von 618 Stimmen gewählt. Es bleibt zu wünschen, dass die Bundesregierung dem Parlament eine Nachfolgerin bzw. einen Nachfolger vorschlägt, die/der den erfolgreich beschrittenen Weg weiterführt und als unabhängige Instanz das Grundrecht auf Datenschutz regional und international, im staatlichen und wirtschaftlichen Bereich mit Augenmaß vertritt.

Einladung zur FIfF-Jahrestagung 2003

Die e-lektrisierte Gesellschaft

Nachstehend ist das vorläufige Programm der diesjährigen FIfF-Jahrestagung abgedruckt, ferner Kurzbeschreibungen einiger Arbeitsgruppen. Aktuelle und erweiterte Informationen finden sich auf der Homepage der Tagung:

http://www.fiff.de/2003

Hier werden in Kürze auch nähere Informationen zu den Tagungsgebühren und zur Anmeldung veröffentlicht. Im Tagungsbüro (*2003@fiff.de*) kann der Tagungs-Flyer angefordert werden.

Die Tagung findet statt im „Bildungszentrum des Bundesverbands der Unfallkassen“ in Bad Hersfeld. In der Tagungsgebühr sind Unterkunft im Tagungshaus und Verpflegung enthalten.

Tagungsbüro / Kontakt:

Tagungsbüro FIfF 2003
Forum InformatikerInnen für Frieden
und gesellschaftliche Verantwortung (FIfF) e.V.
Goetheplatz 4
D-28203 Bremen
Tel.: 0421 / 33 65 92 55
Fax: 0421 / 33 65 92 56
E-Mail: *2003@fiff.de*
WWW: *http://www.fiff.de/2003*

Vorbereitungsteam FIfF 2003:

Dagmar Boedicker (München)
Werner Hülsmann (Mörgen)
Klaus Köhler (München)
Uli Moser (Gottmadingen)
Michael Riemer (Bremen)
Ralf E. Streibl (Bremen)
Werner Winzerling (Fulda)

Freitag, 21. November 2003	
nachmittags	*Das Tagungsbüro im Tagungshaus ist ab Nachmittag geöffnet.*
17.00 Uhr	Eröffnung der Tagung
17.15 Uhr Plenumsvortrag	e-fitness. Dauerlauf und Durchschlagskraft - kompetent, kommunikativ, konnektiv. Rede von der Beweglichkeit und Standhaftigkeit in der schimmernden Welt, ironische Untertöne nicht verbergend, doch heiter sich einlassend aufs Unvermeidliche, vorgebracht von **Frieder Nake** (Bremen)
18.30 Uhr	Abendessen
20.00 Uhr Plenumsvortrag	More e-work - ArbeitnehmerInnen im 21. Jahrhundert **Jürgen Ditz Schroer** (München)
anschl.	Gespräche und Getränke in der „Stube“

Samstag, 22. November 2003	
8.30 Uhr	Frühstück
9.30 Uhr parallele Arbeitsgruppen (Ankündigungstexte zu den AGs siehe Seite 55)	AG 1: e-learning Organisation: *Werner Sesink* (Darmstadt) und *Reinhard Keil-Slawik* (Paderborn) AG 2: e-rights (insb. Urheberrecht) Organisation: *Volker Grassmuck* (Berlin) AG 3: e-identity: Wenn der Körper vermessen zur Information wird! (Biometrie, insb. Gesichtserkennung) Organisation: *Peter Bittner* (Berlin) AG 4: e-libraries Organisation: *Julia Stoll* (Darmstadt) AG 5: e-privacy Organisation: *Werner Hülsmann* (Mörgen), *Uli Moser* (Gottmadingen) AG 6: e-enemy: Feindbild-Manufaktur und Kriegspropaganda Organisation: *Ralf E. Streibl* (Bremen), *Markus Hoff-Holtmanns* (Baesweiler)
12.30 Uhr	Mittagessen
14.30 Uhr Plenumsvortrag	Jefferson revised: Demokratische Technologie und Softwarepatente sind ein Widerspruch! **Bernd Lutterbeck** (Berlin)
16.00 Uhr	FIfF-Mitgliederversammlung (Tagesordnung siehe FIfF-Kommunikation 2/2003, S.7)
18.30 Uhr	Abendessen
19.30 Uhr	„Sentimentalitäten in Echtzeit“ - ein kleines Kulturprogramm
anschl.	Gespräche und Getränke in der „Stube“

Rahmenprogramm: Konrad-Zuse-Museum

Es ist geplant, am Freitagnachmittag für interessierte früh Anreisende eine gemeinsame Fahrt zum *Konrad-Zuse-Museum* nach Hünfeld zu organisieren. Details werden noch bekannt gegeben - bitte ggf. beim FIfF-Büro nachfragen!

Sonntag, 23. November 2003	
8.30 Uhr	Frühstück
9.30 Uhr Plenumsvortrag	Das Internet als Probebühne alltagsästhetischer Inszenierungen? Eine kritische Analyse medialer Selbstdarstellung im Netz **Barbara Becker** (Paderborn)
11.00 Uhr Podiumsdiskussion (Ankündigungstext zur Podiumsdiskussion siehe unten)	e-democracy/e-government mit Wolfgang Kleinwächter, Annette Mühlberg und Ralf Klischewski Moderation: Dagmar Boedicker
12.30 Uhr	Mittagessen
anschl. Abreise	

Änderungen vorbehalten!

Podiumsdiskussion

e-democracy/e-government

Worum wirds auf dem Podium gehen?

Am 23. November werden wir eine Podiumsdiskussion veranstalten, bei der sich ausgewiesene Experten in Sachen Demokratie und ihres e-Potenzials *über deren Ziele, Wege und bisherige oder zu erwartende Ergebnisse unterhalten werden. Die Podiumsgäste sind Annette Mühlberg von ver.di, Wolfgang Kleinwächter von der Universität Aarhus und Ralf Klischewsi von der Universität Hamburg.*

Was ist was?

Die beiden Begriffe *e-democracy* und *e-government* werden häufig vermischt, tatsächlich haben sie eine gemeinsame Schnittmenge im Bereich der Bürgerkontakte mit der Exekutive. Immer dann, wenn die Bürger von ihrer Verwaltung eine Dienstleistung brauchen, oder wenn die Exekutive Stimmungen oder Interessen abfragt, sind die selben Regeln anzuwenden: Es sind vorwiegend Regeln, die auch für die IT-Sicherheit allgemein gelten. Authentifizierung und Sicherheit und Schutz der personenbezogenen Daten bei der Übertragung und der verarbeitenden Stelle.

Ziele und Versprechungen

Die Ziele freilich unterscheiden sich: e-government soll Verwaltungsprozesse beschleunigen und Kosten reduzieren. Flexibilität von Ort und Raum als klassische Merkmale der Internet-Kommunikation sollen im Dienst des Staates und seiner Bürger stehen. Von der Ebene der Europäischen Union bis zu den Kommunen erwarten alle Akteure vor allem mehr Effizienz vom e-government. Soweit, so relativ unproblematisch.

Die Ziele der e-democracy dagegen sind hochfliegend und gewaltig, sie versteht sich als elektronische Demokratieförderung. Bürgersinn soll geweckt und Teilhabe angeregt werden, Politikverdrossenheit ausradiert und Parteimüdigkeit umgangen werden. Sie ist das virtuelle Allheilmittel für die Krankheiten des politischen Systems, egal ob in England, Deutschland, den USA oder Australien. So sehen sie zumindest ihre Propagandisten.
Empowerment – Befähigung – heisst das Zauberwort. Und als Käse in der Mausefalle hat es gewisse Ähnlichkeiten mit der Eigenverantwortung, in deren Namen unsere Sozialsysteme skelettiert werden. Anscheinend sollen diejenigen unter uns, die es nicht längst leid sind, sich doch bitte ihre Informationen selbst holen, in der spärlichen Freizeit, die ihre stressigen Jobs ihnen noch lassen. Sie sollen selbst die Spreu vom Weizen trennen – wirklich eine sinnvolle Alternative zum medialen Mainstream, der sich sein neo-liberales Flussbett beständig tiefer gräbt?
Laut *Institute for Public Policy Research (IPPR)* kann e-democracy im lokalen Bereich folgenden Gefahren begegnen:

- Dem Sich-Abwenden der Bürger vom politischen Prozess
- Technologischer Stagnation, da die Bürger im Internet keine lokalen Politik-Inhalte oder -Foren finden

... und dabei die folgenden Chancen wahrnehmen:

- die Fähigkeit der Behörden stärken, eine führende Rolle in der kommunalen Gemeinschaft zu spielen
- die positive Wirkung von e-government verstärken
- die Bürger vermehrt in Prozesse einbinden, in denen durch eine allgemeine Interessenvertretung der allgemeine Nutzen maximiert wird
- Chancen neuer politischer Strukturen vertiefen und erweitern

Vor einem Jahr hat *IPPR* allerdings noch feststellen müssen, dass diese Chancen noch kaum genutzt werden – und damit wohl auch die Gefahren kaum gebannt sind. Hier und da eine lokale Abstimmung, gelegentliche Online-Befragungen der Bürger zu aktuellen Themen der Stadt- oder Gemeindeverwaltung, viel tut sich nicht auf diesem Gebiet. Nicht einmal diejenigen Potenziale sind verwirklicht, die FIfF e.V. und DVD bereits 1995 in ihrem Bericht für das Europäische Parlament[1] ausgemacht hatten.

Welche Erwartungen an e-democracy sind denkbar?

Die Akteure der e-democracy sind andere als die des e-government: Im Bereich e-democracy trifft sich eine bunte Mischung aus Wissenschaft, Kommerz, Parteipolitik, Bürgerinnen und Bürgern. Sie alle haben Interessen, die für die politischen Entscheidungsträger bedeutsam sein können.

Was könnte e-democracy bieten?

1. Vernetzung eigenständiger Bürger-Initiativen und Nicht-Regierungs-Organisationen
2. Information der Bürger über politische Prozesse
3. Kommunikation zwischen den Abgeordneten und ihren Wählern
4. Kommunikation zwischen der Exekutive und den Bürgern
5. Kontrolle der Exekutive durch Fachleute und andere Bürger
6. Befragungen und Abstimmungen
7. öffentliche Debatten
8. partizipative Entscheidungsfindung zu Themen allgemeiner Relelevanz, insbesondere da, wo Menschen direkt betroffen sind, wie beispielsweise im Gesundheitswesen und den sozialen Sicherungssystemen

In unserer Diskussion wird es darum gehen, die Erwartungen darauf zu untersuchen, wie realistisch und für die Bürger erstrebenswert sie sein können und welche Hindernisse sich ihnen in den Weg stellen.

Kontakt: Dagmar Boedicker, *db@fiff.de*

[1] Ingo Ruhmann et al: "An Appraisal of Technical Instruments for Political Control and to Improve Participation in the Information Society", 1995

Beschreibung der Arbeitsgruppen

Wie jede FIfF-Jahrestagung, so bietet auch die diesjährige ein breites Angebot von Arbeitsgruppen zu alten und neuen FIfF-Themen. Neben aktuellen Informationen zu den Themen stehen Austausch und Diskussion darüber im Vordergrund.

Für folgende Arbeitsgruppen lagen bei Redaktionsschluss Kurzbeschreibungen vor - aktualisierte Ankündigungen der AGs finden sich auf der Homepage der Tagung unter *http://www.fiff.de/2003* .

AG 3: e-identity: Wenn der Körper vermessen zur Information wird

„Die Menschen machen sich endlich auf, die Einzigartigkeit jedes Menschen anzuerkennen – eine Utopie wird Wirklichkeit. So könnte man meinen. Aber in einem völlig anderen Kontext, als [wir] dies vielleicht in unserem humanistischen Ideal und unseren vielleicht naiven Vorstellungen erwartet haben: statt um konkrete zwischenmenschliche Anerkennungsverhältnisse auf gleicher Augenhöhe geht es um die Feststellung der Einzigartigkeit in einem hochabstrakten und hochkomplexen technischen Verfahren: und erst wenn das technologische Verfahren die behauptete Identität verbürgt, kann ich – vielleicht – auf die freie Entfaltung meiner Ich-Behauptung hoffen und meiner Wege ziehen."[2]

Nach einer kurzen Reise in die Geschichte biometrischer Verfahren (Bertillonage, Daktyloskopie) soll es um die Prinzipien und Grenzen moderner biometrischer Verfahren gehen. Dies soll am Beispiel der Gesichtserkennung verdeutlicht werden.

In einem zweiten Teil des Workshops wird es um den Einsatz von biometrischen Merkmalen in Ausweispapieren gehen. Die sogenannten *Antiterror-Gesetze* vom Januar 2002 ermöglichen es, durch die entsprechenden Änderungen des Pass- und des Personalausweisgesetzes (bei letzterem noch mit Gesetzesvorbehalt) biometrische Merkmale in hiesige Ausweispapiere einzubringen. Induziert durch den *US Enhanced Border Security and Visa Reform Act* von 2002 soll der *Rest der Welt*[3] gezwungen werden, biometrische Merkmale in Ausweispapieren bis Oktober 2004 umzusetzen. Pflichtschuldigst werkeln Standardisierungsgremien wie die ISO und vor allem die *International Civil Aviation Organization (ICAO)* an Blaupausen, wie denn die neuen Ausweise aussehen sollen[4]. Da die EU sich nicht widersetzen mochte, hat man sich im Juni 2003 auf höchster Ebene darauf verständigt, einen „coherent approach on biometric identifiers" und „harmonized solutions for documents" zu entwickeln[5].

Die Entwicklungen gehen momentan sogar dahin, dass die biometrischen Daten via RFID[6] (Radio Frequency Identifier) aus dem Ausweis ausgelesen werden können[7] – natürlich unbemerkt vom Besitzer des Ausweises. Daß man ganz sicher gehen will, sollen gleich mehrere biometrische Merkmale auf den Ausweis. Dies, kombiniert mit einer allerorten sich vernetzenden Videoüberwachung, kann einem schon einmal die Gesichtszüge entgleisen lassen – zumal die Politiker im Fahrwasser der Techniker jegliches Gespür für die Angemessenheit gesetzlicher Regelungen zu verlieren scheinen . Drum soll es im dritten Teil des Workshops nicht nur um die gründliche interdisziplinäre Analyse jener Technologien und ihrer Einsatzfelder gehen, sondern auch um die Organisation einer effektiven Gegenwehr.

Einstweilen könnte man empfehlen: „Barcode yourself!"[8]. Mit einem Barcode auf der Stirn, am besten eintätowiert, braucht es nur noch ein Gesetz zur Reglementierung der Haarlänge. Mit den Barcode-Scannern hat man ja genug Erfahrung. Das jedenfalls wäre ein bedenkenswerte Billig-Lösung und man könnte sich den Aufstand mit den neuen Ausweisen wirklich sparen ... hüstel.

Kontakt: Peter Bittner (Humboldt-Universität zu Berlin, Institut für Informatik), *bittner@informatik.hu-berlin.de*

[2] Leopold, Nils: Reader zur Fachanhörung Bündnis 90/Die Grünen vom 19.05.2003 in Berlin: „Mehr Sicherheit durch Biometrie?", gesehen am 15.07.2003 & zugänglich via http://www.humanistische-union.de/modules.php?op=modload&name=Downloads&file=index&req=getit&lid=32

[3] Jedenfalls werden ab Oktober 2004 auch den vormals visafrei in die USA Einreisenden die biometrischen Daten abverlangt!

[4] Cards and personal identification standards committee, siehe http://www.sc17.com (gesehen 16.07.2003); hier interessant z.B. das Dokument 2330 aus der Kooperation ICAO/ISO zum Thema „contact-less chip technology for machine readable passports".

[5] EU Summit: Agreement on „harmonized" biometric identification linked to EU databases, *http://www.statewatch.org/news/2003/jun/22bio.htm* (gesehen 17.07.2003)

[6] Das berührungslose Auslesen geht immerhin auch noch in Entfernungen bis an die 30 Meter, wie mir technisch Versierte versicherten!

[7] Beitrag: „Wenn die Pässe Bio-Daten funken" vom 09.07.2003 unter *http://futurezone.orf.at/futurezone.orf?read=detail&id=169869*

[8] Projekt zuletzt gesichtet unter *http://www.barcodeart.com* am 17.07.2003

AG 4: e-Libraries - wozu?

Wissenschaftliche Arbeit basiert auf dem Austausch von Ergebnissen innerhalb einer Disziplin, zwischen Disziplinen und zwischen Forschern und Forschergruppen an verschiedenen Orten. Bibliotheken und *e-Libraries* sind eine Grundlage wissenschaftlicher Arbeit. Zudem erlauben Web-Applikationen den Austausch von Informationen weltweit, zwischen beinahe jedem Ort und zu fast jeder Zeit.

Um bibliotheksorientierte Web-Dienste zu spezifizieren und umsetzen zu können, bedarf es einer Klärung des Begriffs *e-Library*. Der Begriff *e-Library* lässt die unterschiedlichsten Assoziationen zu: Programmbibliotheken, digitale und virtuelle Bibliotheken, Integration heterogener, dezentraler Informationsdienste, die ihre Daten aus einer verteilten Datenbank erhalten oder auf strukturierte Quellen aus dem Web zugreifen, hybride Bibliotheken u.v.m. Im Rahmen des Workshops wollen wir Ausprägungen verschiedenster Bibliotheken betrachten, um den Begriff einer *e-Library* zu bestimmen. Zu diskutieren sind Aufgaben, Ziele und gleichzeitig Abgrenzungen von

- web-basierten Suchdiensten zur Suche in der *globalen Bibliothek* des Web,
- traditionellen (wissenschaftlichen) Bibliotheken, die ortsgebunden sind,
- heterogenen Informationsdiensten, die in einem Portal den Zugriff auf strukturierte (Fach-)Informationen erlauben,
- oder auch von Kombinationen dieser aufgeführten (Bibliotheks- und web-basierten) Dienste.

Auch die Publikationsverfahren haben sich unter dem Einsatz von Web-Publishing-Methoden verändert. Sie sind geprägt von neuen Arbeitsweisen. Wir müssen unterscheiden zwischen

- "review-before-commit", bei ein fertiges Produkt entsteht, z. B. in Form eines Buches, einer Zeitschrift oder auch in Form einer geschlossenen, digitalen, strukturierten Quelle, wie z. B. e-magazines, über einen Verlag und
- "review-on-commit", einem Verfahren, bei dem auch ein Zwischenstand zur Diskussion gestellt werden kann.

Der Ansatz *review-on-commit* ist aus der Open Source Community entliehen. Hier werden erfolgreich andere Interessierte in eine Diskussion eingebunden, und man geht nach dem Motto „publish early, publish often" vor. Diese Arbeitsweise lässt sich auch auf andere Quellen außer Programmen übertragen. Sie wird ermöglicht durch die inzwischen weit verbreitete Trennung zwischen Syntax und Inhalt in Darstellung und Austausch von strukturierten (Hypertext-)Quellen bzw. Dokumenten. Man nutzt dabei RDF, XML, SOAP oder auch im Moment noch in Entwicklung befindliche Web Services basierend auf WSDL. Ein Dokument unterliegt damit einem offenen Entwicklungsprozess, der nicht abgeschlossen sein muss, wie bei einer Publikation über einen Verlag.

Eine klassische Definition des Begriffs *Bibliothek* besagt, dass eine Bibliothek eine Sammlung von Quellen ist, die um Dienste für eine adäquate Nutzung angereichert ist. Ist das die größte Gemeinsamkeit in den genannten Aufgaben und Zielen? Fragen, die sich anschließen, sind: Wer sammelt was? Was für Quellen sind relevant? Was heißt Nutzung, wovon? Welche Gruppen von Dienstleistern und Nutzern treffen aufeinander? Selbst wenn ein Teil der aufgeführten Fragen schnell zu beantworten scheint, liegen Gründe für die diversen Interpretationen des Begriffs *e-Library* möglicherweise tiefer? Was wird aufbewahrt; wenn ja, wie?

Der halbtägige Workshop möchte während der FIfF-Jahrestagung einige Fragen beantworten und gleichzeitig Probleme in der Umsetzung ins Bewusstsein rufen, an denen bereits gearbeitet wird.

Eine Auswahl von Quellen:

W. Arms: Digital Libraries. MIT Press, McGraw Hill, 2. Aufl. 2002.
W3C: Extended Markup Language (XML) *http://www.w3.org/*
W3C: Resource Description Format (RDF) *http://www.w3.org/*
E. Raymond: The Cathedral and the Bazar. O´Reilly, Cambridge, Köln, Paris, Sebastopol, Tokio 1999.
W3C. Simple Open Access Protocol (SOAP) *http://www.w3.org/*
W3C: Web Service Description Language (WSDL) *http://www.w3.org/*

Kontakt: Julia Stoll, *julias@acm.org*

AG 6: e-enemy: Feindbild-Manufaktur und Kriegspropaganda

Organisation: *Ralf E. Streibl* (Bremen) & *Markus Hoff-Holtmanns* (Baesweiler)

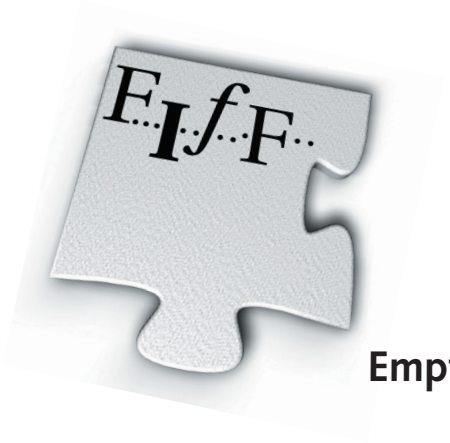
Die Welt ist nicht so einfach, wie die Gut-Böse-Schemata in manchen Computerspielen. Aber manchmal wird sie so einfach

gemacht. Mit dem richtigen Feindbild lässt sich Politik machen, Krieg führen, die Wirtschaft beleben, Überwachung und Kontrolle zur Verbesserung der inneren und äußeren Sicherheit rechtfertigen u.v.m.

In der AG soll ausgehend vom „Feindbild" als psychologischem Konstrukt ein kritischer Blick auf die Informatik und Medieninformatik geworfen werden. Angedacht sind u.a. folgende Themen:

- Feindbilder in Computerspielen
- Möglichkeiten der (technischen) Manipulation von Medieninhalten
- Funktionalisierung von Informations- und Kommunikationstechnik zur Verbreitung von Feindbildern

Die AG ist zur Zeit des Redaktionsschluss dieser FIfF-Kommunikation noch in der Planungsphase. Auf der Homepage der Tagung wird rechtzeitig vor Beginn eine aktualisierte Kurzbeschreibung veröffentlicht werden. Anregungen sowie Angebote zur aktiven Mitwirkung bitte an Ralf Streibl (*res@fiff.de)*.



Presseerklärung

der Regionalgruppe München

des FIfF e.V.

Empfehlung von Fachleuten

Die Regionalgruppe München des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e.V.) begrüßt die Überlegungen der Stadt München zum Einsatz von Open-Source-Software. Die Verwendung freier, quelloffener Software hat aus unserer Sicht viele Vorteile, auf die wir als Fachleute und als Münchner Bürgerinnen und Bürger hinweisen möchten.

Vorteile freier Software

Freie Software erleichtert das Sicherheitsmanagement:
Das Bundesamt für Sicherheit in der Informationstechnik hat sich bereits positiv zu Open-Source-Software geäußert, auch die Europäische Union erwartet Sicherheitsvorteile von ihrem Einsatz. Das ist relevant sowohl für die informationelle Selbstbestimmung der Bürgerinnen und Bürger als auch für die Daten der Verwaltung, beispielsweise bei Ausschreibungen, der Ausweisung von Baugrund usw.

München muss sparen

Freie Software hat Kostenvorteile, das gilt für das Betriebssystem, die Hardware und die Anwendungssoftware – selbst wenn man die Kosten für Schulungen und Support berücksichtigt. Es gibt viele Anbieter zu LINUX, das bedeutet das Ende der städtischen Abhängigkeit von einem einzelnen Hersteller.

In einer vielfältigen Informationstechnik bieten sich Möglichkeiten für alle:

Die Beschäftigten der Stadt erwerben nützliche Qualifikationen, die Bürger können ohne teure, ständig zu erneuernde Lizenzen mit der Verwaltung kommunizieren und im Netz partizipieren, aus technischer Monokultur wird Vielfalt, auch andere Hersteller erhalten ihre Chance. Der Wettbewerb um mehr Sicherheit und geringere Kosten wird gefördert.

Ein kluger und mutiger Stadtrat

Wir wünschen uns von den Münchner Stadträtinnen und Stadträten eine unvoreingenommene Prüfung und zukunftsweisende Entscheidung. Für uns alle erhoffen wir uns mehr Freiheit und mehr Kompetenz, und für unsere Stadt sinkende Kosten.

München, 14. Mai 2003

Für die Regionalgruppe des FIfF e.V. und V.i.S.d.P.:

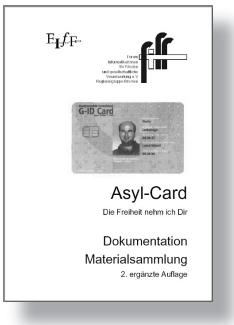
Dr. Jens Woinowski
Pöppelstraße 6, 81541 München

Ansprechpartner für diese Presseerklärung:

Prof. Dr. Klaus Köhler
Tel.: 089/1265-1626 oder 089/60019153

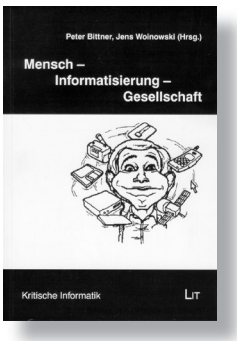
FIfF-Bibliothek

Bücher und Broschüren



AsylCard: Die Freiheit nehm ich Dir
FIfF-Dokumentation und Materialsammlung

hrsg. von der FIfF-Regionalgruppe Bremen
2., ergänzte Auflage, 64 Seiten, Bremen 2000, Euro 1,50



Mensch –
Informatisierung – Gesellschaft

hrsg. von Peter Bittner & Jens Woinowski
188 Seiten, Münster: Lit-Verlag 1999, Euro 20,90

Schöne Neue Arbeit

hrsg. von Jochen Krämer, Jürgen Richter, Jürgen Wendel & Gaby Zinßmeister

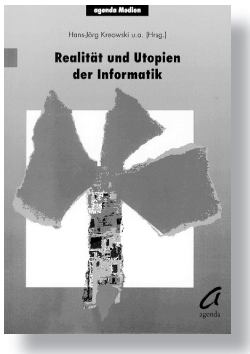
298 Seiten, Mössingen-Thalheim: Talheimer Verlag 1997,

Euro 22,50

1984 plus 10 – Realität und Utopien der Informatik

hrsg. von Hans-Jörg Kreowski, Thomas Risse, Andreas Spillner, Ralf E. Streibl & Karin Vosseberg

221 Seiten, Münster: agenda Verlag 1995, Euro 5,00



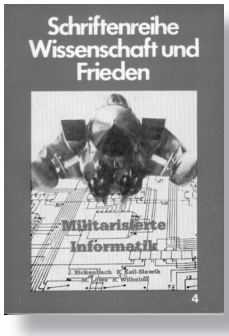
Ein sauberer Tod – Informatik und Krieg

hrsg. von Ute Bernhardt & Ingo Ruhmann
320 Seiten, Marburg 1991, Euro 5,00

Militarisierte Informatik

hrsg. von Joachim Bickenbach & Michael Löwe

209 Seiten, Marburg 1985, Euro 2,00 (nur noch kleine Restauflage)



Informatik und Militär

hrsg. von Joachim Bickenbach, Helga Genrich, Reinhard Keil, Werner Langenheder & Michaela Reisin
102 Seiten, Berlin 1984, vergriffen

ACHTUNG – Nachdruck: Diese Textsammlung aus den FIfF-Gründungstagen ist als Fotokopie erhältlich zum Preis von 3,00 Euro

Weitere Veröffentlichungen des FIfF finden Sie unter
http://www.fiff.de/veroeffentlichungen/buecher

FIfF-Kommunikation

Eine Übersicht über die Themenschwerpunkte früherer Hefte finden Sie unter:

www.fiif.de/veroeffentlichungen/fiffko-themen.html

Ein Großteil dieser Hefte ist noch lieferbar (bei Abnahme größerer Stückzahlen eines Heftes oder mehrerer unterschiedlicher Hefte gibt es natürlich Sonderkonditionen!).
Preise pro Heft: Jahrgänge 1995–97: je 2,00 Euro
Jahrgänge 1998–99: je 3,00 Euro
ab Jahrgang 2000: je 5,00 Euro

Bestellen

Bestellungen aller genannten Publikationen bei der FIfF-Geschäftsstelle (Adresse siehe Seite 60).

Die Lieferung erfolgt auf Rechnung (Preise zzgl. Versandkosten). Bei Bestellungen über 25,00 Euro liefern wir versandkostenfrei.

FIfF e.V.

Im FIfF haben sich rund 800 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FIfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

Das FIfF-Büro

Geschäftsstelle FIfF e.V.
Goetheplatz 4
D-28203 Bremen
Tel.: (0421) 33 65 92 55
Fax: (0421) 33 65 92 56
E-Mail:fiff@fiff.de

Bürozeiten:
Mittwochs und Donnerstags 13 bis 16 Uhr

Sparda Bank Hannover eG
Kontoverbindung: 927929
BLZ 250 905 00

FIfF im Netz

Das ganze FIfF: *www.fiff.de*

FIfF-Mailingliste
An- und Abmeldungen an: *fiff-l-request@fiff.de*
Beiträge an: *fiff-l@fiff.de*

Mailingliste Videoüberwachung:
An- und Abmeldung an: *cctv-l-request@fiff.de*
Beiträge an: *cctv-l@fiff.de*

FIfF-Vorstand

- **Prof. Dr. Reinhard Keil-Slawik (Vorsitzender)** Paderborn
- **Peter Bittner (stellv. Vorsitzender)** Berlin
- **Dagmar Boedicker** München
- **Prof. Dr. Leonie Dreschler-Fischer** Hamburg
- **Eva Hornecker** Wien
- **Werner Hülsmann** Mörgen-Eppishausen
- **Prof. Dr. Klaus Köhler** München
- **Prof. Dr. Dietrich Meyer-Ebrecht** Aachen
- **Michael Müller** Schwaigern
- **Prof. Dr. Gabriele Schade** Leipzig
- **Prof. Dr. Britta Schinzel** Freiburg i.Br.
- **Julia Stoll** Darmstadt
- **Ralf E. Streibl** Bremen
- **Prof. Dr. Joseph Weizenbaum** Berlin

Beirat

Michael Ahlmann (Bremen); **Prof. Dr. Wolfgang Coy** (Berlin); **Prof. Dr. Wolfgang Däubler** (Bremen); **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); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Hans-Jörg Kreowski** (Bremen); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Hans-Peter Löhr** (Berlin); **Dipl.-Ing. Werner Mühlmann** (Oppburg); **Prof. Dr. Frieder Nake** (Bremen); **Prof. Dr. Rolf Oberliesen** (Bremen); **Dr. Hermann Rampacher** (Bonn); **Prof. Dr. Arno Rolf** (Hamburg); **Prof. Dr. Alexander Rossnagel** (Kassel); **Prof. Dr. Gerhard Sagerer** (Bielefeld); **Prof. Dr. Dirk Siefkes** (Berlin); **Prof. Dr. Marie-Theres Tinnefeld** (München); **Dr. Gerhard Wohland** (Wankheim)

Überregionale Arbeitskreise des FIfF

AK »Videoüberwachung und Bürgerrechte«
Peter Bittner, Humboldt-Universität – Institut für Informatik
Unter den Linden 6 , 10099 Berlin
bittner@informatik.hu-berlin.de
www.ak-videoueberwachung.de

AK »RUIN« (Rüstung und Informatik)
Kontakt über das FIfF-Büro Bremen

Regionalgruppen und regionale Ansprechpartner

Aachen
Prof. Dr. Ing. Dietrich Meyer-Ebrecht
Lehrstuhl für Messtechnik und Bildverarbeitung
RWTH Aachen
52056 Aachen
Tel. (0241) 80 278 60
Fax: (0241) 88 222 00
me@lfm.rwth-aachen.de

Berlin
Peter Bittner
Humboldt-Universität
Institut für Informatik
Unter den Linden 6
10099 Berlin
bittner@informatik.hu-berlin.de

Berlin
Irina Piens
Schlesische Str.29
10997 Berlin
piens@prz.tu-berlin.de

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

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

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

Darmstadt
Julia Stoll
Heinheimer Str. 29-31
64289 Darmstadt
Tel.: (06151) 71 21 81
julias@acm.org

Erlangen/Fürth/Nürnberg
Klaus Thielking-Riechert
Am Dummetsweiher 9
91056 Erlangen
k.thielking@link-n.cl.sub.de

Freiburg
Prof. Dr. Britta Schinzel
Universität Freiburg
Institut für Informatik und Gesellschaft
Friedrichstr. 50
79098 Freiburg im Breisgau
Tel.: 0761-203-4953
Fax: 0761-203-4960
schinzel@modell.iig.uni-freiburg.de

Frankfurt
Ingo Fischer
Dahlmannstraße 31
60385 Frankfurt am Main

Hamburg
Ralf Klischewski
Universität Hamburg
FB Informatik SWT
Vogt-Kölln-Strasse 30
22527 Hamburg
klischew@informatik.uni-hamburg.de

Hannover
Bernhard Pfitzner
Rosenbergstraße 14a
30163 Hannover

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

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

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

Karlsruhe
Prof. Dr. Thomas Freytag
Weltzienstr. 35
76135 Karlsruhe
Tel.: (0721) 815416 (p)
fiff@thomas-freytag.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

Konstanz
Ulrich Moser
Roseneggweg 2
78244 Gottmadingen
Tel: (07731) 74261 (p)
+41-79-3112051 (d)
info@fiff-kn.kujm.de
http://fiff-kn.kujm.de/

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

Münster
Werner Ahrens
Franz-Daspestr. 36
48231 Warendorf

Oldenburg
Universität Oldenburg
Fachschaft Informatik
Ammerländer Heerstraße
26129 Oldenburg
Fachschaft.Informatik@informatik.unioldenburg.de

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

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

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

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

Kopieren, ausfüllen und einsenden an:
FIFF e.V.
Goetheplatz 4
D-28203 Bremen
Fax: (0421) 33 65 92 56

FIfF

Vielzweckschnipsel

Das möchte ich:

- ❑ aktives Mitglied des FIfF werden.
  Normale Mitgliedschaft mit Stimmrecht und Bezug der FIfF-Kommunikation. Der Mindestbeitrag ist für Verdienende **60 Euro** und für Studierende und Menschen in vergleichbarer Situation **15 Euro**.
- ❑ förderndes Mitglied des FIfF werden.
  Mitgliedschaft ohne Stimmrecht, z.B. für Institutionen. Der Mindestjahresbeitrag beträgt **60 Euro**.
- ❑ die FIfF-Kommunikation zum Preis von **20 Euro** jährlich frei Haus abonnieren.
- ❑ dem FIfF etwas spenden.

- ❑ Ich überweise den Betrag auf das **Konto 927929** bei der Sparda Bank Hannover eG, BLZ **250 905 00**.
- ❑ Der Mitglieds- bzw. Abobeitrag soll per Lastschriftverfahren von meinem Konto abgebucht werden.

Einzugsermächtigung

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

Name: _____

Jahresbeitrag: _____ EUR, erstmals: _____

Konto-Nr.: _____ BLZ: _____

Geldinstitut: _____

_____ _____
Datum Unterschrift

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

Die/der bin ich:

Name: _____

Straße: _____

Wohnort: _____

ggf. Mitgliedsnummer: _____

Telefon (privat): _____ (Arbeit): _____

Email: _____

Was sonst noch so geht:

- ❑ Ich möchte mehr über das FIfF wissen, bitte schickt mir:

  _____

- ❑ Ich möchte gegen Rechnung und zuzüglich Portokosten bestellen:

  _____

  _____

- ❑ Ich möchte das FIfF über einen Artikel oder ein Buch informieren:

  _____

  _____

- ❑ Ich möchte zur FIfF-Kommunikation beitragen mit
  - ❑ einem Manuskript zur Veröffentlichung
  - ❑ einer Anregung (siehe unten)

  _____

  _____

  _____

- ❑ Der Vielzweckschnipsel ist nichts für mich. Ich möchte einen richtigen Brief schreiben.

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 Quellenangaben) 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.

Geplante Themenschwerpunkte der nächsten Hefte:

Heft 4/2003
„Software-Patente“
zuständig: Sabrina Geißler (Paderborn)
Redaktionsschluß: 1.10.2003

Heft 1/2004
„Schöpfungen“
zuständig: Andreas Genz, Matthias Krauß,
Ralf E. Streibl (Bremen)
Redaktionsschluß: 15.01.2004

Daneben sind immer auch Artikel zu aktuellen Themen wilkommen. Bitte setzen Sie sich mit der Redaktion in Verbindung: *redaktion@fiff.de* oder über die Geschäftsstelle des FIfF e.V.

Wichtiger 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 bekannt zu geben!

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
Verlagsadresse	FIfF Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1.400 Stück
Heftpreis	5 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 20 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Carsten Büttemeier, Sabrina Geißler, Ralf E. Streibl
V.i.S.d.P.	Harald Selke
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@msf.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an Claus Stark: *claus@fiff.de*
Layout	Carsten Büttemeier
Titelbild	„Puzzle“ Matthias Krauss
Druck	Meiners Druck, Bremen

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.“ (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige AutorInnen-Meinung wieder.

Schluss-PFIfF

Dagmar Boedicker

Beiträge im nächsten Heft

... zum guten Schluss: Dieses Heft ist so inhaltsreich wie wir es uns nur wünschen können – was aber den Nachteil hat, dass einige Artikel voraussichtlich erst in der Ausgabe 4/2003 erscheinen können. Wir bitten die Autorinnen und Autoren um Verständnis und kündigen die Beiträge an dieser Stelle wenigstens an:

Peter Bittner: *Grundrechte-Report 2003*
„... ein Projekt der Humanistischen Union, der Gustav-Heinemann-Initiative, des Komitees für Grundrechte und Demokratie, des Bundesarbeitskreises kritischer Juragruppen, von Pro Asyl, des Republikanischen AnwältInnenvereins und der Vereinigung Demokratischer Juristinnen und Juristen. Er beleuchtet die blinden Flecke der Verfassungsschutzämter, ...“

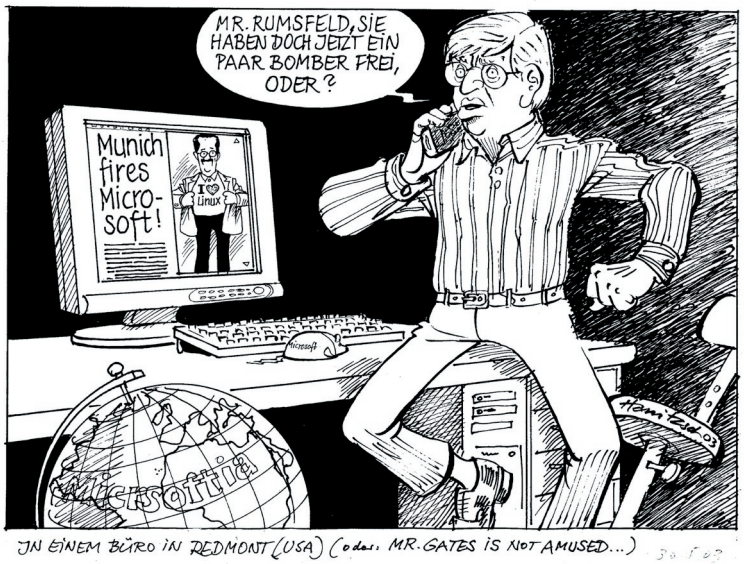
Klaus Brunnstein, Horst Oberquelle: *Fachbereich Informatik der Universität Hamburg ehrt Joseph Weizenbaum*
„Der Fachbereich Informatik der Universität Hamburg hat den weltbekannten kritischen Informatiker Prof. em. Dr. h.c. mult. Joseph Weizenbaum am 15. Januar 2003 mit einem Festkolloquium im besonderen Ambiente des Warburghauses Hamburg geehrt. ...“

Ingo Ruhmann: *Der Gegner im Inneren*
„Die Entwicklung nach dem 11. September 2001, die Ausweitung von Überwachungsbefugnissen und der inzwischen globale Kampf gegen den Terrorismus mit den Mitteln des Information Warfare geben ... Anlass, das Werk Orwells neu zu sehen.“

Gabriele Schade: *Informatik im Osten*
„... Nicht nur die, die Erinnerungen und Erfahrungen damit verbinden, sind interessiert, auch viele Studierende begreifen anhand solcher geschichtlicher Themen die Spezifik ihrer Disziplin, der Informatik.“

Hellmut Weber: *Wenn die Inbox dreimal klingelt*
„..Innerhalb weniger Jahre hat sich E-Mail zu einem nicht mehr wegzudenkenden Kommunikationsmittel entwickelt. ... es gibt noch keine wohl etablierte Kultur im Umgang mit diesem Medium.“

Jens Woinowski: *Linux für München - Eine Kampagne*
„... Bleibt am Schluss nur die Frage, ob sich das alles gelohnt hat. ...“



IN EINEM BÜRO IN REDMONT (USA) (oder: MR. GATES IS NOT AMUSED...)

Wir danken Herrn Dieter Hanitzsch für die freundliche Nachdruckgenehmigung.

Quelle: Süddeutsche Zeitung vom 30. Mai 2003, S. 41

Geeignete Texte für den Schluss-PFIfF bitte mit Quellenangabe an Claus Stark (Adresse siehe Impressum) senden.