

inhalt

COMPUTER-FACHWISSEN 3/2003

- 2 Magazin**
Schlaglichter, Kurzberichte, Neuigkeiten

TRENDS & HINTERGRÜNDE

- 4 I. Räder, D. K. Sinn: Digital Rights Management ...**
Das Ende der Freiheit im Internet?

MITBESTIMMUNGSPRAXIS

- 10 J. Meier: E-Thrombose – Gefahr am PC-Arbeitsplatz?**
Thrombose durch langes Sitzen vorm PC ...
- 13 K. Hirschfeld: Probleme mit der ›Kurzzeit-Mobilität‹**
Auslandsreisen, Arbeitsbedingungen, Privatleben
- 18 M. Wilke: GPS – Mitbestimmung im Weltraum?**
Navigationssysteme und Mitbestimmung

DATENSCHUTZ

- 24 K. Schuler: Datenschutz-Gütesiegel**
Die ›Blauen Engel‹ für den Datenschutz ...
- 28 H. Köppen: Datenschutztipp aus der Praxis, für die Praxis**
Krankenkassendaten an den Arbeitgeber?

HARD- & SOFTWARE

- 33 K.-H. Böker: Belegschaftsbefragung mit PDF**
Artikelreihe zum PDF-Einsatz – Folge 5
- 35 S. Fricke: Durch die Textwüsten des Intranet ...**
Artikelreihe zur Website-Gestaltung – Folge 5
- 38 W. Fricke: Workflow-Management für den Personalrat**
›DoVoMa‹ – eine Software für Personalräte

VERSCHIEDENES

- 3 Impressum**
- 22 Seminare**

4

Das Bemühen um die Respektierung des Urheberrechts eignet sich durchaus dafür, ganz andere und weit weniger edle Motive zu verschleiern: Wollen und werden Microsoft & Co. also schon bald ihre Kunden noch weit perfekter ausspionieren und ihre Marktmacht nutzen, um die letzten Konkurrenten abzudrängen?

33

Belegschaftsbefragungen können für die Interessenvertretung der Arbeitnehmer eine nützliche Angelegenheit sein. Die PDF-Technik bietet dafür spannende Möglichkeiten, etwa für eine teil-automatisierte Auswertung. Auch die letzte Folge unserer PDF-Reihe liefert also interessante Tipps für die Nutzung des ›Acrobat‹ ...

10

Schlagzeilen hat es gemacht, als festgestellt wurde, dass stundenlanges, bewegungsloses Sitzen in engen Flugzeugen das Entstehen von Thrombosen begünstigt. Schlagzeilen macht auch (vorerst im englischsprachigen Ausland) eine Studie aus Neuseeland, die Gleiches für langes Sitzen am PC-Arbeitsplatz für möglich hält ...

38

Nicht nur dort, wo viele Routine-Vorgänge zu bearbeiten sind, kann die Dokumenten- und Vorlagen-Bearbeitung des BGS-Hauptpersonalrats sinnvoll zum Einsatz kommen. Im Laufe der Jahre hat sich ›DoVoMa‹ zu einem echten und dazu noch kostenlosen Workflow-Management-System entwickelt – leider nur für Personalräte ...

Welche Software im Einsatz?

[CF] Betriebs- und Personalräte setzen heute zur Unterstützung ihrer Arbeit eine Menge Software ein. Dazu gehören natürlich Standardprogramme wie eine Textverarbeitung oder eine Tabellenkalkulation, aber auch einiges an Spezial-Software – zum Beispiel zur effektiveren Vorbereitung und Protokollierung von Sitzungen, spezielle Datenbank-Lösungen oder echte »Workflow«-Steuerungen (siehe den Beitrag ab Seite 38). Daneben können auch arbeitsrechtliche Entscheidungssammlungen zum Einsatz kommen oder diverse andere Datenbanken etwa zu Arbeitssicherheitsfragen, zu Gefahrstoffen oder Rehabilitationsmaßnahmen ...

Was auch immer, wie auch immer zum Einsatz kommt: Die CF-Redaktion würde es gerne genauer wissen! Einmal, weil es sicher interessant sein wird, zu erfahren, was in der Betriebs-/Personalratspraxis so alles zur Anwendung kommt, zum Zweiten aber auch, um gezielter und damit hilfreicher über Software-Angebote und ihre praktische Nutzung informieren zu können. Deshalb:

Schicken Sie uns auf beliebigem Weg eine Liste der in Ihrem Betriebs-/Personalratsbüro eingesetzten Software-Produkte und Datenbanken! Bei etwas aus dem Rahmen fallenden Systemen wären ein paar erklärende Worte nett, ansonsten genügt eine schlichte Liste via E-Mail, Fax oder Brief. Vielen Dank schon jetzt!

**Computer-Fachwissen
 Redaktionsbüro W. Fricke
 Feldstraße 16
 24626 Kleinkummerfeld
 fax 0 43 93-9 76 79
 compfach@t-online.de**

AiB-Kongresse

[CF] Schnell Entschlossene schaffen es noch, sich rechtzeitig für den am **2. April 2003 in Berlin** stattfindenden AiB-Kon-



gress zu den Gesetzespaketen »Hartz I« und »Hartz II« anzumelden. Am **13. Mai** dann folgt das Thema: »Arbeits- und Gesundheitsschutz / Betrieblicher Umweltschutz«. In beiden Veranstaltungen geht es um einen fundierten Gesamtüberblick zum Thema, vermittelt durch ausgewiesene Experten.

Am **3. Juni** geht's dann zur Sache mit dem Thema »**Neue Informations- und Kommunikationstechnologien in Betrieb und Dienststelle**«. Schwerpunkte sind E-Mail-/Internet-/Intranet-Nutzung, IT-Mitbestimmung, Datensicherheit/Datenschutz und E-Learning. Die Vortragenden Experten dürften allen CF-Lesern gut bekannt sein: Prof. Wolfgang Däubler, Prof. Peter Wedde, Josef Haverkamp und Ulrich R. Buchholz. Anmeldungen an:

**Arbeitsrecht im Betrieb
 Verlagsgesellschaft
 Martina Voiss
 Postfach 90 08 40
 51118 Köln
 fax 0 22 03-9 35 25-41
 martina.voiss@aib-verlag.de**

Surf-Profile

[CF] Spionage am Arbeitsplatz ist beliebt und wird immer beliebter – bei den Arbeitgebern jedenfalls (siehe: »Spione am Arbeitsplatz« in CF 1/03 ab

Seite 14). Dabei müssen diese das nicht einmal unbedingt im eigenen Hause machen lassen, sondern können die Spionagetätigkeit auch »fremdvergeben«. So wirbt die Firma Cobion damit, für jeden Angestellten ein detailliertes »Surf-Profil« zu erstellen. Dafür werden die Internet-Besuche für einen bestimmten Zeitraum im Detail erfasst und ausgewertet. Auf der Grundlage dieser Aus-

wertung ließen sich dann beispielsweise bestimmte Bereiche des World Wide Web für die Nutzung vom Arbeitsplatz aus sperren.

Betriebsrats-Service im Netz

[KHB] »Betriebsrats-Service im Netz« lautet das Schwerpunktthema der dieses Jahr schon zum dritten Mal stattfindenden »Netztage« – Veranstaltungsort ist diesmal das Congress-Centrum in Würzburg. Die **vom 18. bis zum 21. Mai 2003** stattfindende Fachkonferenz wendet sich speziell an Arbeitnehmervertreter, um sie über rechtliche, technische und praktische Aspekte der Themen E-Mail, Internet und Intranet zu informieren.

Dabei stehen die Möglichkeiten der schnellen und effektiven elektronischen Kommunikation mit Beschäftigten, anderen Interessenvertretungen und der Gewerkschaften im Mittelpunkt. Es sollen aber auch neue Ideen für netzgestützte Dienstleistungen der Arbeitnehmervertretung erarbeitet werden.

Auf den »Netztagen« kommen Praktiker zu Wort aber auch Experten, die sich mit Themen beschäftigen wie: Schutz personenbezogener Daten, Verhinderung von Leistungs- und Verhaltenskontrolle, praktische Hilfen für Regelungen in Betriebs- und Dienstvereinbarungen. Auch Erfahrungen mit Qualifizierungskonzepten und deren Umsetzung sowie mit neuen Formen der Arbeits-



organisation im Kontext der Nutzung von E-Mail, Intranet und Internet sollen diskutiert werden.

Veranstalter ist ›Liaison.Net, eine Gruppe freiberuflicher Experten und Sachverständiger aus dem gewerkschaftlichen Umfeld. Für die Fachtagung ist eine Freistellung nach § 37 Abs. 6 BetrVG, § 46 Abs. 6 BPersVG sowie den entsprechenden Bestimmungen für Landespersonal- und Mitarbeitervertretungen möglich. Informationen und Anmeldeunterlagen gibt es im Internet unter

www.liaison.de

oder bei

Liaison GmbH
Brauereistraße 13
06847 Dessau
fon 0340-5029740
fax 0340-5029704

›Netzwerke‹ statt Internet

[NTR] Millionen setzen bei ihrer Suche nach einem neuen Arbeitsplatz aufs Internet. Doch neue Untersuchungen deuten darauf hin, dass solche Stellengesuche nur den Datenmüll des Netzes erhöhen – nicht aber von ernsthaft Interessierten gelesen werden. In den USA hat die Personalberatung Drake Beam Morin (DBM) untersucht, auf welchem Weg Bewerber ihren neuen Arbeitgeber fanden. Nur sieben Prozent von 14338 neuen Anstellungsverträgen war auf das Internet zurückzuführen.

Nach Meinung der Agentur ist das Problem der Jobvermittlung über das Internet das gleiche wie bei allem, was man im Netz sucht: Das Gesuchte ist bestimmt enthalten, aber wie findet man es? »Bislang versagen alle rationalen Analysewerkzeuge, wenn es um die Beurteilung von Menschen geht«, sagt Barbara Marchilonis, Direktorin bei DBM. Wenn eine Firma eine interessante Position im Netz anbietet, erhält sie meist tausende an Bewerbungen – allein deren Sichtung würde schon Wochen dauern. »Eingestellt wird die Person, die dem Chef bei ei-

nem Geschäftsessen empfohlen wurde«, sagte Allison Hemming, Präsidentin der New-Yorker Personalagentur Hired Guns über den Unterschied von Internet und ›Networking‹.



Multi-Media-Terminals

[CF] So vielfältig wie heute war die Medienwelt noch nie und immer häufiger kommt sie auch außerhalb von Büro oder Wohnung zum Einsatz. So genannte ›Multi-Media-Terminals‹ stehen immer häufiger in Eingangshallen, Läden oder Einkaufspassagen, auf Messen, Tagungen und Veranstaltungen. Nun sollten diese ›MMTs‹ leicht zu bedienen und möglichst widerstandsfähig gegen Vandalismus sein. Das Bam-



berger Unternehmen VisuKom hat deshalb Terminals aus Edelstahl entwickelt, die sich besonders einfach transportieren und aufbauen lassen und die außerdem bei unbestritten elegantem Aussehen robust konstruiert sind.

www.visukom.net

Hilfe zur Selbsthilfe

[CF] Mit einem besonderen Seminarangebot tritt jetzt CF-Autor Hans Rupp an die Öffentlichkeit: Seminare zu verschiedensten Themen, speziell für ein Betriebs- oder Personalratsgremium. Die Bandbreite ist groß und reicht von allgemeinen EDV-Fragen über Arbeitszeitthemen bis zu Datenschutz und Ergonomie. Nähere Informationen:

QBT – Hans Rupp
Friedrich-Merz-Straße 32
64401 Groß-Bieberau
fon 06166-9210043
fax 06166-920009
qbt.rupp@t-online.de
www.qbt-beratung.de

Stroh statt Kunststoff

[CF] Allein in Deutschland werden 15,8 Millionen Tonnen Kunststoffe hergestellt – davon mehr als ein Viertel nur für Verpackungsmaterialien. Das in Glindenberg ansässige Retrupor Verpackungs- und Dämmstoffwerk hat nun ein alternatives Verpackungs-

material aus nachwachsenden Rohstoffen entwickelt. Die Ausgangsstoffe – Getreidestroh und Zellulose aus Altpapier – werden zerkleinert und zu einer formbaren Masse verarbeitet. Diese wird in einer Presse in die gewünschte Form gebracht.

Probleme mit der Entsorgung der Verpackungsformteile gibt es nicht – Retrupor verrottet innerhalb einer Vegetationsperiode.

www.Retrupor.de

IMPRESSUM

Redaktion:

Wolfgang Fricke (verantwortlich)
Feldstraße 16
24626 Kleinkummerfeld
fon 04393-97696
fax 04393-97679
compfach@t-online.de
<http://www.aib-verlag.de>

Verleger:

›Arbeitsrecht im Betrieb‹
Verlagsgesellschaft mbH
Postfach 90 08 40, 51118 Köln
fon 02203-93525-13
fax 02203-93525-41

Verlagsleiter:

Dr. Jürgen Schmidt
Geschäftsführer:
Christian Paulsen,
Norbert Schaepe

Vertrieb/Abonnements:

Bund-Verlag GmbH
Postfach 90 01 68
60441 Frankfurt/M.
fon 069-79 50 10-96
fax 069-79 50 10-12
carina.grimm@bund-verlag.de

Anzeigen:

Bund Verlag GmbH,
Theodor-Heuss-Allee 90-98,
60496 Frankfurt/M.
fon 069-79 50 10-49
fax 069-79 50 10-10
Verantwortlich für Anzeigen:
Hartmut Griesbach
Es gilt Anzeigenpreisliste Nr. 5
Computer-Fachwissen
erscheint monatlich;
Einzelheft 5,90 €
Jahresbezugspreis für 12 Hefte
63,60 €; (Ausland 70,20 €)



Abbestellung zum Jahresende mit 6-Wochen-Frist

Mit Namen des Verfassers gezeichnete Beiträge geben nicht unbedingt die Meinung der Redaktion bzw. des Verlegers wieder.

Alle in dieser Fachzeitschrift veröffentlichten Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung – auch auszugsweise – bedarf daher der vorherigen Zustimmung des Verlags.

Druck: tönnes satz + druck,
Erkrath

Digital-Rights-Management – das Ende der Freiheit im Internet?

Das an sich positive Vorhaben, die Urheberrechte wirksamer auch auf digitale Inhalte anzuwenden, hat eine dramatische Wendung erfahren. Es wurde deutlich, dass die dazu angestrebte Technik von erheblichen Risiken und Nebenwirkungen begleitet wird. Die Grundlagen erläutert Ihnen diesmal nicht Ihr Arzt oder Apotheker, sondern dieser Artikel.

DER SCHUTZ GEISTIGEN Eigentums ist seit Langem gesetzlich festgeschrieben. Ebenso lange gibt es das Phänomen, dass derart geschützte Werke *illegal* kopiert, vervielfältigt und verteilt werden. Mit der Digitalisierung von Inhalten, das heißt der Umwandlung von Texten, Bildern, Filmen und Musik in ›maschinenlesbare‹ Formate (also Dateien), verschärfte sich das Problem. Und mit dem Internet kam die einfache und sozusagen ›grenzenlose‹ Möglichkeit der Verbreitung hinzu.

Datenkomprimierungstechniken und schnelle Internet-Anschlüsse lassen es heute zu, ganze Filme aus dem Internet herunterzuladen. Und CD-(oder DVD-) Laufwerke und -Brenner sind heute fast schon PC-Standard. Qualitativ hochwertiges Kopieren und Verteilen digitaler Inhalte wird damit extrem einfach und billig.

Der daraus resultierende Trend zum Raubkopieren untergräbt so einen Teil des Geschäfts der Anbieter geschützter Werke und Inhalte. Zwar haben die meisten Medien- und Unterhaltungsfirmen es jahrelang versäumt, sich auf die neu-

en Techniken und besonders die *Online*-Medien (z. B. Internet) einzustellen, denn das hätte unter anderem eine Anpassung ihrer Geschäftsmodelle und auch einen massiven Umbau ihrer Strukturen bedeutet. Andererseits können sich ›Bezahl-Inhalte‹ auch dann erst richtig etablieren, wenn eine Technik für einen effektiveren Schutz verfügbar ist. Der Ruf nach besseren Gesetzen und Techniken zur Wahrung der Urheberrechte ist daher prinzipiell nachvollziehbar.



Das Digital-Rights-Management

ZUM DIGITAL-RIGHTS-MANAGEMENT (DRM) gehören gesetzliche und technische Maßnahmen, die zum Ziel haben, die illegale Verbreitung und Nutzung digitaler Inhalte zu verhindern. Vorreiter sind die USA, dort werden seit einigen Jahren Gesetze verabschiedet (das erste unter Bill Clinton) und diskutiert, die das Copyright (= Urheberrecht) an die neuen technischen Entwicklungen anpassen wollen. Aktuelle amerikanische Gesetzesvorlagen wollen unter anderem erreichen, dass die Gerätehersteller verpflichtet werden, in alle neuen Geräte Hardware-Zusätze einzubauen, die eine unrechtmäßige Nutzung und Verbreitung digitaler Inhalte unterbinden sollen.

Technisch müsste dazu in die Geräte nur zusätzlich ein Chip integriert werden, der in Verbindung mit Verschlüsselungstechniken und spezieller Software die diversen Schutzfunktionen erfüllt. Dieser Chip wird auch ›Fritz-Chip‹ genannt (nach dem US-Senator Fritz Hol-

lings, einem der Initiatoren dieser Vorschläge).

DRM-Aktivitäten beschränken sich allerdings nicht nur auf die USA, denn es gibt eine internationale Verpflichtung innerhalb der Welthandelsorganisation (WTO) zur Angleichung der Schutzrechts-Systeme. Auch deshalb werden zur Zeit in den EU-Ländern (und damit auch in Deutschland) ähnliche Anpassungen der Urheberrechtsgesetze betrieben. Nach derzeitigem deutschem Gesetzesentwurf kann damit ein Rechteinhaber »die Nutzung eines geschützten Werkes [...] durch eine Zugangskontrolle, einen Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Umwandlung oder einen Mechanismus zur Kontrolle der Vervielfältigung [...] unter Kontrolle halten«. Die Umgehung solcher technischen Schutzmaßnahmen soll verboten werden – dass Regelungen dieser Art erhebliche Auswirkungen auf den heute üblichen Computer-Einsatz haben könnten, wird im Laufe dieses Artikels noch deutlich werden.

TCPA – Trusted Computing Platform Alliance

UM DEN GESETZLICHEN Anforderungen gerecht zu werden und um die Interessen am Schutz der eigenen Inhalte und Programme zu verfolgen, haben sich in der internationalen T CPA-Initiative Vertreter der IT- und Medienbranche zusammengeschlossen. Es gehören mehr als 130 Firmen zu dieser Allianz, darunter Intel, AMD, Compaq, Dell, Fujitsu-Siemens, HP, IBM, Infineon, Microsoft und Motorola.

Ziel dieser Allianz ist es, Personal Computer und andere Abspiegelgeräte durch technische Vorkehrungen sicherer zu machen und dabei auch das illegale Kopieren, Verbreiten und Nutzen urheberrechtlich geschützter Inhalte einzuschränken. Dies soll durch entsprechende Hardware- und Software-Erweiterungen erreicht werden und zwar – wie schon erwähnt – durch Einbau eines separaten Chips (»Fritz-Chip«), der diver-

se Verschlüsselungs- und Authentifizierungsfunktionen bietet.

Dieser Chip erlaubt das Entschlüsseln und damit ein Verarbeiten, Abhören, Abspielen oder Benutzen digitaler Inhalte nur dann, wenn sich der Nutzer rechtmäßig einen Schlüssel dafür besorgt hat. Dieser Schlüssel ist ein Datensatz, der via Internet übertragen wird und ohne den die Datei nicht korrekt ent-

schlüsselt werden kann. Er funktioniert also ähnlich wie ein digitales Passwort. Offen ist noch, ob die Schlüssel von den Medienanbietern oder von bestimmten zentralen Organisationen verwaltet werden und wer diese Organisationen sein könnten.

Eine Spiele-Firma könnte dann beispielsweise verschlüsselte Spiele über das Internet zum Herunterladen anbieten oder als CDs oder DVDs verkaufen. Die Spiele wären aber nur auf einem Gerät mit dem T CPA-Mechanismus zu benutzen. Je nachdem, welche Rechte (= Schlüssel) der Kunde erworben hat, kann dieser das Spiel dann zum Beispiel nur einmal, mehrmals oder eine bestimmte Zeit lang nutzen – oder er muss weitere Abspielrechte erwerben. Ähnlich funktioniert das mit Programmen, Musik und Filmen.

Die Hardware soll auch die Basis für mehr Sicherheit und Authentifizierung sein. Es ist bekannt, dass fast alle heute verfügbaren Kopierschutztechniken irgendwie und von irgendwem unterlaufen wurden. Die T CPA-Initiative strebt daher ein System an, das nicht geknackt werden kann. Dazu sind allerdings einige Voraussetzungen nötig: Einerseits der Chip, der ganz eng an den Prozessor des jeweiligen Geräts angebunden ist. Beispielsweise überprüft der Chip in Verbindung mit bestimmter Software, ob

se an den Rechnereinstellungen vorgenommen wurden.

Unter anderem soll damit ein »Überbrücken« der Sicherheitseinrichtungen verhindert werden. Falls es eine Veränderung gegeben hat, muss das System erneut über das Internet als »sicher« zertifiziert werden.

Authentifizierung = das sichere Bestimmen der Identität eines Nutzers als Voraussetzung für den sicheren Zugang zu Systemen und als Basis für Bezahlungen und elektronische Rechte.

Wer künftig geschützte Programme oder Inhalte benutzen will, muss beim Systemstart einmal Kontakt zur Zertifizierungsstelle herstellen, die Geräte, Programme und Rechte überprüft.

Im Rechner werden dafür bestimmte Abläufe zwangsweise vorgegeben. Wer geschützte Programme oder Inhalte nutzen will, muss einmal im Rahmen des Systemstarts über das Internet mit der Instanz verbunden gewesen sein, die die Hard- und Software überprüft und die entsprechenden Rechte und Schlüssel verwaltet.

Palladium oder Next-Generation Secure ...

»PALLADIUM« IST DER Projektname für eine Reihe von Sicherheitsmerkmalen, die die Firma Microsoft in künftige Windows-Betriebssysteme integrieren will, um ein »vertrauenswürdiges Arbeiten mit Rechnern« (»trustworthy computing«) sicherzustellen. Microsoft baut dabei auf den T CPA-Mechanismen und den oben beschriebenen Chip auf.

Palladium oder »Next-Generation Secure Computing Base«, wie das Projekt jetzt heißt, soll höhere Datensicherheit und eine sichere Kommunikation gewährleisten. Erreicht werden soll dies durch diverse Elemente, um die das Betriebssystem erweitert wird. In einem sicheren Speicherbereich beispielsweise, auch »Tresor« genannt, werden sensible



Begriffserklärungen:

Digital-Rights-Management ...

- **Digital-Rights-Management-Systeme (DRM):** Technische Vorrichtungen, die den Schutz digitaler Inhalte gewährleisten und deren illegale Nutzung und Verbreitung unterbinden sollen. Der Ursprung ist in amerikanischen Gesetzen/Gesetzesvorlagen zu sehen, forciert durch die Medien-Industrie und die US-Regierung, die digitale Inhalte besser geschützt wissen wollen. Auch die europäische Gesetzgebung verfolgt inzwischen ähnliche Ziele.
- **Trusted Computing Platform Alliance (TCPA):** Zusammenschluss vieler führender IT- und Medien-Anbieter, um die technischen Voraussetzungen zu schaffen, digitale Inhalte gegen illegale Nutzung zu schützen. Geschützte Dateien können unter anderem nur mit Schlüsseln (einer Art digitalem Passwort) dekodiert werden, die der Nutzer ›rechtmäßig‹ über das Internet erwerben muss. Dieser Schutz soll durch Dekodier- und Authentifizierungs-Chips gesichert werden, die ganz eng in die Prozessoren der jeweiligen Geräte integriert werden.
- **Palladium / Next-Generation Secure Computing Base:** Projektname(n) für ein sicheres, erweitertes Windows-Betriebssystem, das Microsoft auf der Basis von TCPA-Hardware aufbauen will.

Zusammenfassung:

Die Risiken und ihre Kritik

- Wer soll die Schlüssel und Rechte verwalten und wer soll die entsprechenden Systeme im Internet betreiben? Dort werden viele Informationen über die Nutzer anfallen – unter anderem wird bekannt sein, welche Inhalte von wem wie oft genutzt werden, folglich muss man diese Informationen schützen.
- Wenn man solche Daten nicht einzelnen Software- und Medien-Firmen überlassen will, braucht man übergeordnete Instanzen. Sollen staatliche Stellen diese Aufgabe übernehmen und damit die Kontrolle über Informationszugang und -verteilung erhalten?
- Es wird befürchtet, dass IT- und Inhalte-Anbieter (z. B. Microsoft) diese Techniken auch zur Abschottung der Konkurrenz nutzen könnten, indem sie ›unliebsame‹ Software oder Systemzusätze ausschließen.
- Die Dienste und Systeme für die digitale Rechtewahrung können herstellerseitig nur genutzt werden, wenn die Software-Entwickler oder Inhalte-Anbieter ihre Produkte anpassen und die (wahrscheinlich aufwändigen) Zertifizierungen durchlaufen. Große Firmen können an einem solchen Verfahren teilnehmen, was aber geschieht mit kleinen Inhalte- oder Software-Anbietern?
- Unklar ist, ob das System jemals hundertprozentig sicher sein kann. Viel höher noch ist das Risiko, dass über Hacker-Angriffe das gesamte System stillgelegt wird, weil relativ viel Kommunikation zwischen den einzelnen lokalen Systemen und den zentralen Instanzen im Internet stattfindet.
- Ohne Internet-Verbindung oder ohne die TCPA-Zusätze in den Geräten könnten auch zertifizierte Inhalte nicht genutzt werden.
- Es könnte eine Abhängigkeit von Initiativen und Techniken entstehen, die überwiegend von der US-Industrie dominiert und gestaltet werden.

Daten wie Passwörter, Zertifikate oder Schlüssel für verschlüsselte Dokumente ablegt. Nur zertifizierte, das heißt, als sicher eingestufte Programme können dann auf diese Schlüssel zugreifen und Daten oder Dokumente für den Gebrauch entschlüsseln.

Da über den Hardware-Chip auch eine Identifikation und Authentifizierung des Rechners eingebunden werden kann, wäre es möglich, den Zugriff auf

Daten oder Dateien nur für bestimmte Rechner und deren Nutzer freizugeben. Eine derart geschützte Datei (Dokument) könnte dann zwar weitergegeben werden, ließe sich aber auf einem nicht-autorisierten Gerät (z. B. außerhalb der Abteilung oder außerhalb des Firmennetzes) nicht öffnen. Dieses Sicherheitsmerkmal soll besonders Firmen und Organisationen ansprechen, die damit die Weitergabe vertraulicher Informationen, zum Beispiel auch von E-Mails, verhindern könnten. Palladium soll auch

besseren Schutz vor Manipulationen, sprich Computerviren und ähnlichen Angriffen bieten. Noch allerdings ist Palladium ein Planungs- und Entwicklungsprojekt und kein verfügbares Produkt.

Erste Praxisbeispiele gibt es bereits

DAS GESCHILDERTE IST aber nicht nur Zukunftsmusik. So baut Sony bereits ›Sicherheits‹-Chips in die neuen Speicherkarten seiner Spielekonsolen ein. Mit dieser Technik macht die Nutzung illegaler Spielekopien kaum noch Spaß, denn die Spieler können ihre Daten, sprich: Spielstände, dann nicht mehr abspeichern. Auch die Xbox-Spielekonsole von Microsoft nutzt bereits Mechanismen zur Software-Zertifizierung, um sicherzustellen, dass nur von Microsoft autorisierte Spieleprogramme zum Einsatz kommen.

Einen Vorgeschmack davon, wie Hersteller diese Techniken zum Schutz ihrer eigenen Interessen und zum Nachteil ihrer Konkurrenz nutzen könnten, zeigt folgendes Beispiel. Einige Druckerhersteller stellen bereits bestimmte neue Druckermodelle (oder auch die dazu gehörenden Toner-Kartuschen) mit ›Sicherheits‹-Chips aus. Dadurch kann – ganz im Sinne des Herstellers – unter anderem geprüft und sichergestellt werden, dass nur Originalteile des Herstellers genutzt werden. Die Original-Kartusche ›authentifiziert‹ sich also beim Drucker als ›zulässiges‹ Modell, während Kartuschen anderer Hersteller möglicherweise gar nicht oder nur eingeschränkt funktionieren. Anbieter von Fremdkartuschen imitieren inzwischen schon solche Chips, was wiederum mit Hinweis auf das Urheberrecht angegriffen wird ...

In diesen Fällen wird das Urheberrecht also dazu benutzt, den Wettbewerb abzuschotten – eine Entwicklung, die sicher nicht im Sinne der Copyright-Gesetzgebung liegen kann. Dass man sich zumindest mancherorts dieses Problems bewusst ist, zeigt ein kürzlich von

Trends & Hintergründe

der EU verabschiedetes Gesetz zum ›Recycling von Elektronikschrott‹, in dem der Einbau solcher ›Sicherheits-Chips ausdrücklich verboten wurde. Dieses Beispiel zeigt, wie schnell das Urheberrecht in eine überraschende Richtung

Bedenken kommen in diesem Zusammenhang auch von Befürwortern so genannter Open-Source-Software, also von Programmen, die frei verfügbar sind. Denn Open-Source-Software und das ebenfalls frei verfügbare Betriebs-

gilt für den organisatorischen Aspekt: Wer kann Betreiber einer solchen Authentifizierungs-Stelle im Internet werden? Wird es eine staatliche Instanz geben oder sollen es die IT-Anbieter machen? Welche Voraussetzungen müssen sie erfüllen und wer überwacht diese Instanzen? Fragen, die besonders dann schwer zu klären sein werden, wenn die Rechte-Verwaltung auf internationaler Ebene stattfinden soll.

Wenn der Rechte-Überprüfungs-Server eines Software- oder Inhalte-Anbieters via Internet auf einen Rechner zugreift, prüft er dann wirklich nur die Rechte?

gewendet werden kann, dieses Feld darf der IT-Industrie also nicht alleine überlassen werden.

Befürchtungen zu Technik und Gesetz

DIE TCPA-INITIATIVE versucht, die Basis-Elemente für Schutz und Sicherheit zu schaffen. Unbekannt ist bis heute, wie das Gesamtsystem aussieht und wie die einzelnen Elemente zusammenwirken werden. Die aktuelle Diskussion ist jedenfalls geprägt durch massive Kritik und viele Befürchtungen. Dazu gehören unter anderem die folgenden Szenarien:

Wenn der Authentifizierungs-Server über die Internet-Verbindung die Sicherheit prüft, greift er auf den lokalen Rechner zu und analysiert bestimmte Komponenten.

Dazu stellen sich Fragen: Prüft der Server (z. B. der Rechte-Verwaltungs-Computer eines Herstellers) tatsächlich nur, ob die notwendigen Rechte vorliegen und ob Mechanismen oder Programme vorhanden sind, die ein Überbrücken der Sicherheitseinrichtungen und ein illegales Kopieren ermöglichen oder sucht er auch nach anderen ›unliebsamen‹ Programmen oder Inhalten? Will sich ein Anbieter vielleicht Wettbewerber vom Halse halten, indem er deren Software als ›unsicher‹ einstuft? Wer definiert überhaupt, ob die Software eines Wettbewerbers ein Sicherheitsrisiko ist?

system Linux müssten sich zertifizieren lassen, um TCPA-Funktionen nutzen zu können. Da aber Open-Source-Entwickler oft kleine Firmen oder Einzelpersonen sind, könnte für sie die Zertifizierung durch das TCPA-Konsortium zu teuer werden. Außerdem steht der prinzipielle TCPA-Ansatz einer Zertifizierung von Software dem Grundgedanken ›freier‹ Software entgegen.

Ähnlich betroffen sind viele kleine Anbieter von Software und Inhalten, ebenso wie die Urheberrechte für Inhalte, die nicht tausendfach benutzt werden. Für sie könnte die Anpassung und Verwaltung durch die Rechte-Instanz zu aufwändig werden. Und in der Tat fällt auf, dass die Gesetzgebung und die technischen Initiativen besonders durch die großen Medienkonzerne beeinflusst werden, so dass die Interessen der ›kleinen‹ Rechtesbesitzer sehr schnell auf der Strecke bleiben könnten.

Auch bei der praktischen Umsetzung des Digital-Rights-Managements gibt es noch offene Fragen. Nehmen wir das Beispiel Datenschutz:

Die Authentifizierung gegenüber einem großen Inhalte-Anbieter oder einer zentralen Instanz führt dazu, dass dort eine Vielzahl von Informationen über den einzelnen Nutzer auflaufen: zum Beispiel welcher Nutzer (Rechner) wie oft auf welche Informationen oder Programme zugreift. Damit entsteht ein beträchtliches Wissen über den einzelnen Nutzer und sein ›Profil‹. Wie damit umgegangen wird und wie diese Daten entsprechend geschützt werden können und sollen, ist noch ungeklärt. Gleiches

Microsoft im Blickfeld

DIE AKTIVITÄTEN VON Microsoft werden bei alldem besonders kritisch begleitet. Manche Stimmen vermuten, dass es Microsoft mit seiner ›Next-Generation Secure Computing Base‹ (früher: Palladium) auch um die bessere Kontrolle der eigenen Software-Lizenzen geht. Mit Palladium könnte möglicherweise bei jedem Programmstart geprüft werden, ob alle Lizenzen noch gültig sind und ob die Software auch tatsächlich auf dem dafür autorisierten Rechner läuft. Ist dies nicht der Fall, müsste die Lizenz erneuert werden – oder die weitere Nutzung des Programms wird gesperrt ...

Auch deshalb bekräftigt Microsoft öffentlich immer wieder, dass dies nicht in ihrem Interesse liege, sie wollten schließlich mit Palladium nicht ihre Kunden ›verärgern‹. Um Transparenz bemüht, will Microsoft sogar den Quellcode (die Programmierung) der Palladium-Software offenlegen und damit Einblick in die genauen Funktionen der Software geben.

Wahrscheinlich wird man einen PC auch künftig *ohne* aktivierten Sicherheitsmechanismus starten können, allerdings wird man dann wohl nach und nach auf immer mehr gesicherte und verschlüsselte Programme und Inhalte nicht mehr zugreifen können. Und weil für die Prüfung beim Start des Rechners immer eine Verbindung zum Internet nötig sein wird, könnten auch alle Personal Computer ohne Internet-Anschluss oder ohne TCPA-Einrichtung

auf zertifizierte Inhalte nicht mehr zugreifen.

Trotzdem: Weiterentwicklung statt Verweigerung

ES IST LEGITIM UND für eine Wirtschaft und Gesellschaft sogar notwendig, illegales Verhalten einzuschränken – auch beim Umgang mit Urheberrechten. Stellt sich die Frage, ob man dies allein durch die Androhung von Strafen erreichen kann und will, ob in der Folge immer häufiger Polizei-Razzien auf Schulhöfen und Hausdurchsuchungen stattfinden sollen oder ob eine technische Verhinderung illegaler Nutzung und ›Piraterie‹ nicht doch die bessere Lösung wäre?

Dabei lassen wir die Diskussion um die so genannten Privat-Kopien (also das zulässige Anfertigen von Kopien für den eigenen privaten Gebrauch) einmal ausgeklammert. Ebenso den Fakt, dass sich manche Software überhaupt nur verbreitet hat, weil sie immer wieder (illegal) kopiert wurde. Auch die Tatsache, dass sich Schüler nicht nur über gekaufte Musik-CDs mit Musik versorgen können, soll hier nicht vertieft werden – manches wird sich da über den Markt regeln müssen ...

Schaut man sich nun die aktuelle Diskussion um das Digital-Rights-Management an, fällt auf, dass Kritik und Bedenken darin einen sehr breiten Raum einnehmen, während die ja ebenfalls vorhandenen Vorteile kaum thematisiert werden: Wer daran interessiert ist, dass sich digitale Angebote verbreiten und dass dabei auch neue Geschäfts- und Beschäftigungsmöglichkeiten entstehen, muss als Voraussetzung ein funktionierendes System zum Rechteschutz anstreben. Wir halten es – gerade auch als Autoren – für einen Irrweg, dass so viele Inhalte (vor allem im Internet) kostenlos sein ›müssen‹. Wir glauben vielmehr, dass mehr und bessere Inhalte im Internet entstehen könnten, wenn sich geeignete Verfahren zum Schutz und zur Bezahlung durchsetzen würden.

Die pauschale Ablehnung jeder ›Kopierschutz‹-Initiative scheint uns daher nicht hilfreich. Vielmehr sollten die vorhandenen Ansätze und Initiativen weiterentwickelt werden. Wichtig ist dafür, dass Juristen und Politiker noch mehr Einsicht in die technischen Gegebenheiten und Marktmechanismen der ›digitalen Wirtschaft‹ bekommen.

Wie dargestellt, ist die technische Lösung notwendigerweise komplex und birgt deshalb Risiken. Auch wird ein besserer Schutz der Inhalte und mehr Sicherheit für die Nutzer nur dann möglich sein, wenn bestimmte Verfahren etabliert und standardisiert werden, selbst wenn dies eine gewisse Einschränkung im Komfort nach sich ziehen sollte.

Alles in allem muss deshalb dafür gesorgt werden, dass die zum Einsatz kommende Technik transparent ist, dass ihr Einsatz rechtssicher gestaltet ist und weitgehend von den Interessen einzelner Firmen entkoppelt wird – und dass nicht gleichzeitig staatliche Stellen dabei zum ›Big Brother‹ gemacht werden. Eine Aufgabe, die viel zu wichtig ist, um allein den IT-Herstellern und Technikern überlassen zu werden.

Isolde Räder und Dieter K. Sinn arbeiten als Berater mit den Schwerpunkten neue Technologien, IT-Märkte und IT-Strategien; Kontakt: sinn-consulting, Knorrstraße 11, 80807 München, fon 089-3590195; sinn-consulting@t-online.de <http://www.sinn-consulting.de>



E-Thrombose: Gefahr am PC-Arbeitsplatz?

Im englischsprachigen Raum wird es schon heftig diskutiert: das Risiko, durch langes Sitzen vor dem Computer eine Thrombose zu bekommen ... »E-Thrombose« – nur ein neues Schlagwort oder eine ernst zu nehmende Gesundheitsgefährdung?

DIE MEISTEN WERDEN sich noch an die Schlagzeilen erinnern, die das so genannte »Economy Class Syndrom« im Zusammenhang mit längeren Flugreisen gemacht hat:

Verursacht durch langes Sitzen in einer beengten Position und bei mangelnder Beinfreiheit können sich Blutgerinnsel (Thromben) in den Venen der unteren Körperhälfte – und hier vor allem in den Waden – bilden, was unter Umständen dann zu einer Verstopfung von Blutgefäßen etwa in der Lunge oder im Herzen führen kann. Dr. John Belstead – tätig am Ashford Hospital in Middlesex/England – behandelt eingelieferte Patienten vom nahe gelegenen Flughafen Heathrow und berichtet von etwa zehn Todesfällen pro Jahr – verursacht durch Thrombosen. Dr. Belstead schätzt, dass weltweit pro Jahr bis zu 2000 Menschen an einer »Flug-Thrombose« sterben ...

Und jetzt kommen auch die Bildschirmarbeitsplätze in Verdacht: Stundenlanges Sitzen am PC ohne ausreichende Bewegung zwischendurch kann ebenfalls die Bildung von Thromben begünstigen!

Zu dieser Erkenntnis jedenfalls kommt eine Studie des neuseeländischen Wissenschaftlers Professor Richard Beasley, die in der Februar-Ausgabe 2003 des britischen »European Respiratory Journal« unter dem Titel erschien: »Thrombosis: the 21st Century variant of thrombosis associated with immobility« (= E-Thrombose: die durch Bewegungsmangel verursachte Thrombosen-Variante des 21. Jahrhunderts).

Diese Studie vom anderen Ende der Welt macht zur Zeit im englischsprachigen Internet und anderen IT-Fachmedien Schlagzeilen, die ihresgleichen suchen. Von: »Ihr PC bringt Sie um!« bis zur wohl weniger ernst zu nehmenden Empfehlung sich wegen akuter »E-Thrombose« vorsorglich schon mal für ein paar Tage krank zu melden, ist da alles vertreten.

Bereits kurz nach dem Erscheinen der Studie von Professor Beasley wurden die ersten Meldungen ins Internet gestellt, die sich mit weiteren Todesfällen – verursacht durch die »E-Thrombose« – befassten. Das Thema wird also sicherlich noch zu mehr Schlagzeilen in den kommenden Monaten führen. Um so wichtiger ist es, bei einem so heiklen Thema so früh wie möglich zu einer sachlichen Information und Diskussion beizutragen.

Der beste Weg dazu war, direkten Kontakt zu Professor Beasley, der am »Medical Research Institute of New Zealand« arbeitet, aufzunehmen und ihn um die notwendigen »harten« Fakten zu bitten.

Danach scheint festzustehen, dass es wohl keinen Grund zur Panik an den Büroarbeitsplätzen gibt. Die unter Umständen lebensbedrohlichen Gefahren einer Thrombose hat es schon immer gegeben (und nicht erst seit die ersten Meldungen über das »Economy Class Syndrom« im Oktober 2000 erschienen sind). Und klar ist auch, dass regelmäßiges und (zu) langes Sitzen an einem Bildschirmarbeitsplatz ganz sicher zum



allgemeinen Bewegungsmangel beiträgt und damit als eine Ursache für Thrombosen in Frage kommt. Genau so selbstverständlich ist jedoch, dass jeder für sich etwas zum Ausgleich und zur Vorbeugung tun kann.

Die Studie und ihre Ergebnisse

BEI DER VON PROFESSOR BEASLEY und seinen Kollegen verfassten Studie handelt sich um die erste ihrer Art, die sich am Fall eines 32-jährigen Neuseeländers orientiert, der regelmäßig mindestens

12 Stunden – manchmal bis zu 18 Stunden! – täglich am Computer verbrachte, oft bis zu 6 Stunden ohne einmal aufzustehen oder sich Bewegung zu verschaffen.

Der Patient berichtete bei der Begutachtung durch Professor Beasley von einer zehn Tage lang stark angeschwollenen Wade – ein Symptom, das etwa sechs Wochen vor der ersten fachärztlichen Konsultation aufgetreten war (siehe info-Kasten auf Seite 12). In den letzten vier Wochen vor der Begutachtung beklagte er sich dann über zunehmende Atemlosigkeit, die selbst minimale Anstrengungen praktisch unmöglich machte. Am Tage der Begutachtung brach der Patient dann mit einer Lungenembolie – verursacht durch einen Thrombus – zusammen.

Nachdem alle anderen möglichen Risikofaktoren als Verursacher aus medizinischer Sicht ausgeschlossen werden konnten, verblieb als einzig wahrscheinliche Ursache der extreme Bewegungsmangel des Patienten (der sich nach entsprechender medikamentöser Behandlung und Änderung seines Bewegungsverhaltens übrigens nach sechs Monaten wieder voll erholte).

gehen, dass der Thrombosegefahr und den Möglichkeiten ihrer Verhütung zukünftig eine weit größere Bedeutung beizumessen sein wird, als dies bisher der Fall gewesen ist.

Der Grundgedanke ist nicht neu, wird uns aber verstärkt ins Bewusstsein geru-



fen werden: Zur Vermeidung krankmachender Belastungen am Büro- oder Bildschirmarbeitsplatz werden nicht nur ergonomisch gestaltete Sitzmöbel, Schreibtische, Bildschirme und Tastaturen benötigt, sondern es obliegt auch dem Einzelnen selber, den drohenden Bewegungsmangel auszugleichen oder bei besonderer Anfälligkeit weitere Maßnahmen zur Vorbeugung gegen Thromboserisiken zu ergreifen.

Aufgabe sowohl des Arbeitgebers wie auch des Betriebs- oder Personalrats ist es mit zur Aufklärung der Beschäftigten beizutragen. Zugleich aber sollten bestehende Betriebs-/Dienstvereinbarungen über Pausenregelungen überprüft und gegebenenfalls neu verhandelt werden. Die rechtliche Grundlage dafür bildet der § 87 Abs. 1 Nr. 2 BetrVG (Mitbestimmungsrecht bei Beginn und Ende der täglichen Arbeitszeit einschließlich der Pausen). Unterstützend kann hinzuge-

zogen werden der § 87 Abs. 1 Nr. 7 BetrVG (Regelungen über die Verhütung von Arbeitsunfällen und Berufskrankheiten sowie über den Gesundheitsschutz im Rahmen der gesetzlichen Vorschriften oder der Unfallverhütungsvorschriften).

Hinzu kommen die klaren Bestimmungen der Bildschirmarbeitsverordnung, in der es im § 5 heißt, dass der Arbeitgeber die Tätigkeit der Beschäftigten so zu organisieren hat, dass die tägliche Arbeit an Bildschirmgeräten regelmäßig durch andere Tätigkeiten oder durch Pausen unterbrochen wird, die jeweils die Belastung durch die Arbeit am Bildschirmgerät verringern (siehe dazu: ›Mach mal Pause!‹ in CF 3/01 ab Seite 14).

Vor allem diese Bestimmung bekommt durch das Thema E-Thrombose natürlich zusätzliches Gewicht. Zugleich wird aber auch hier wieder deutlich, dass eine fortschrittliche (Pausen-)Regelung allein das Problem nicht lösen wird. Viel zu oft wird die vereinbarte Pausenzeit entweder nicht in Anspruch genommen oder zweckentfremdet ›genutzt‹, im schlimmsten Fall um Computerspiele zu spielen oder privat noch etwas im Internet zu surfen – kaum die richtige Vorbeugung gegen E-Thrombose oder andere Belastungen durch Bildschirmarbeit.

Modebegriff: ›E-Thrombose‹?

DER VON PROFESSOR BEASLEY und seinen Kollegen in diesem Zusammenhang geprägte Begriff der ›E-Thrombose‹ dürfte uns wohl noch lange erhalten bleiben, zumal das ›E‹ bei allem, was mit Informationstechnologie zu tun hat, fast täglich zu neuen Wortschöpfungen führt. Trotzdem ist es mehr als eine Mode. Unter Berücksichtigung der Tatsache, dass mehr und mehr Menschen immer längere Zeiten vor dem Computer verbringen (sei es bei der Arbeit und/oder zusätzlich auch noch zu Hause) ist davon auszu-

Symptome der Thrombose und Vorbeugung

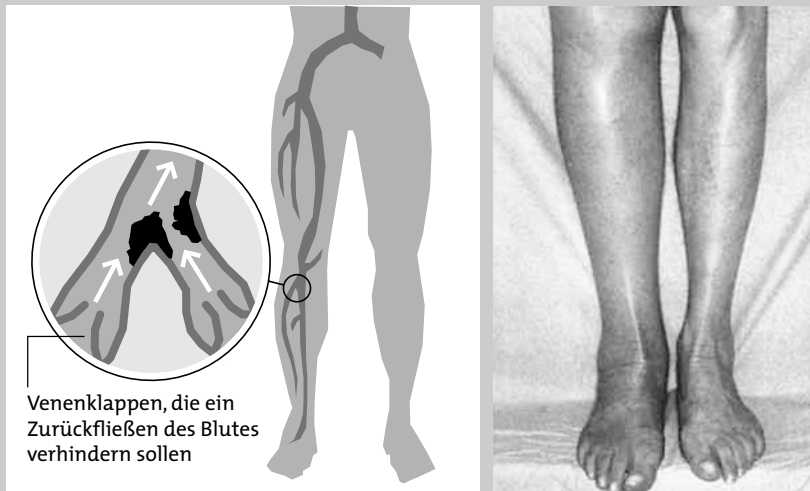
UM EINER THROMBOSE vorzubeugen ist das Aufstehen vom Arbeitsplatz und Bewegung erforderlich, weil nur das die Durchblutung der Beinvenen anregt (siehe info-Kasten auf Seite 12). Hierauf muss also im Rahmen einer innerbetrieblichen Aufklärungsaktion deutlich hingewiesen werden.

Dass es tatsächlich jeder selbst in der Hand oder vielmehr ›im Bein‹ hat, sich vor E-Thrombose zu schützen, wird



Übersicht:

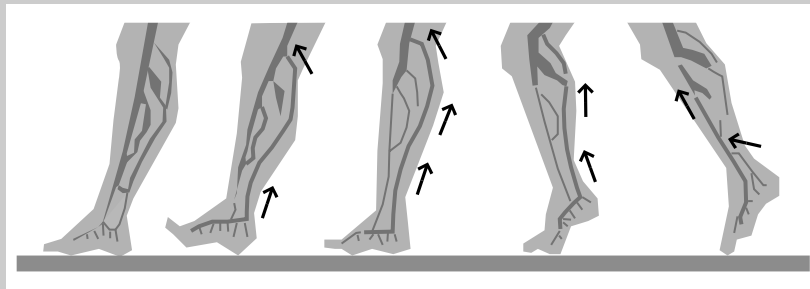
Thromboserisiko durch Bewegungsmangel



Venenklappen, die ein Zurückfließen des Blutes verhindern sollen

Wenn das Pumpen-System der Beinvenen nicht immer wieder durch Muskelbewegungen aktiviert wird, bilden sich Blutgerinnsel, die Venen blockieren, sich aber auch losreißen und an gefährlichen Stellen (Herz und Lunge) wieder absetzen können.

Bild eines durch Bewegungsmangel und schlechte Venenfunktion stark angeschwollenen Beines (= höchste Thrombosegefahr).



Dieses Bild zeigt, wie sich der Druck im Venen-System des unteren Beins beim Gehvorgang verändert. Die Anspannung der unterschiedlichen Muskeln und Muskelgruppen sorgt dabei dafür, dass während eines Schrittes die Venen im Wadenbereich fast komplett entleert werden.

schon daran deutlich, dass das ›Economy Class Syndrom‹ und die E-Thrombose zwar die gleichen physiologischen Ursachen haben, aber dennoch nicht in einen Topf geworfen werden sollten. Ursache für die Thrombenbildung ist in dem einen wie in dem anderen Fall ein überlanges Verharren in einer Sitzposition. Während dies bei Fluggästen aber durch die objektiv beengte Beinfreiheit im Flugzeugsitz erzwungen wird, kann an einem einigermaßen vorschriftsmäßig eingerichteten Bildschirmarbeitsplatz von beengter Beinfreiheit in diesem Sinne normalerweise nicht die Rede sein. Es ist also in der Tat eine Frage des

Bewusstseins, vorhandene Bewegungsmöglichkeiten auch zu nutzen.

Mit zu berücksichtigen sind dabei allerdings persönliche Risikofaktoren: Etwa zwei von 1000 Frauen erkranken jährlich neu an einer Blutgefäßverengung, Männer sind seltener betroffen. Für Patienten, die schon einmal an einer Thrombose erkrankt waren, ist das Risiko, ein zweites Mal eine Thrombose zu bekommen, um ein Vielfaches höher als bei Patienten, die noch keine derartige Vorerkrankung hatten.

Als Hinweis auf eine Thrombose gelten plötzliche oder belastungsabhängige Schmerzen, die sich durch Hochlagerung des Beines bessern. Weitere Symptome können sein: Druckschmerz

an der Innenseite des Fußes und im Verlauf der betroffenen Vene, Schmerzen in der Wade bei Beugung des Fußes, Wadenschmerzen auf Druck und zunehmende Schwellung des Beins (vor allem nach längerem Sitzen), sowie verstärktes Hervortreten oberflächlicher Venen.

Bewegung beugt vor – auch im Büro

AUCH WER, WIE DIE meisten Menschen, nicht zu Turnübungen im Büro neigt, kann doch durch gar nicht so aufwändige und unauffällige Übungen wirksame Vorbeugung betreiben. Mal abgesehen von gelegentlichem Aufstehen und kurzen Gängen hilft vor allem die folgende Übung:

Füße flach auf den Boden stellen, dann abwechselnd Ferse und Zehen heben und wieder auf den Boden drücken – dies regt die Wadenmuskulatur an, ›abgesacktes‹ Blut im Bein wieder hoch zu pumpen (siehe Abbildung links)!

Die vor allem in den 80-er Jahren hochgelobten Kniestühle taugen für eine Vorbeugung gegen E-Thrombose allerdings nicht – werden an Bildschirmarbeitsplätzen aber auch kaum eingesetzt (eher schon mal im privaten Bereich). Bedenklich in diesem Zusammenhang ist nicht nur die oft beklagte Belastung der Kniegelenke, auch die Durchblutung der Unterschenkel wird durch die spezielle Sitzhaltung nicht gerade gefördert. Sinnvoller könnte es da schon sein, Stühle einzusetzen, die deutlich höher sind als konventionelle Bürostühle und die wegen nicht so stark gebeugter Gelenke insgesamt das Blut besser fließen lassen (siehe auch: ›Vom Stehen und vom Sitzen‹ in CF 6/01 ab Seite 5). Erforscht sind diese Zusammenhänge zur Zeit aber noch nicht.

Für alle diejenigen, die wegen eines Venenleidens bereits so genannte Stützstrümpfe tragen zum Schluss noch die Empfehlung eines renommierten Blutgefäßspezialisten: Er warnt vor der Benutzung handelsüblicher Stützstrümpfe oder so genannter ›Support Stockings‹.

Im Gegensatz zu klinisch getesteten Kompressionsstrümpfen seien diese zur Vorbeugung gegen Thrombosen nicht geeignet. Diese Stützstrümpfe hätten meist einen *gleichmäßigen* Druckverlauf und seien am Oberschenkel am engsten. Medizinische Kompressionsstrümpfe dagegen seien am engsten im Fesselbereich, da dort der Druck besonders wichtig ist. Hier würden die Sprunggelenks- und Wadenmuskelpumpen unterstützt, die für den Rücktransport des Bluts zum Herzen die meiste Arbeit leisteten (weitere Informationen dazu im Internet unter www.medi.de; eine gute Einführung in die Materie – auch für medizinische Laien verständlich – findet sich auch unter www.durchblutung.com).

Joe Meier ist gebürtiger Deutscher, lebt seit über zehn Jahren in Australien/Neuseeland und arbeitet dort als freiberuflicher Unternehmensberater; Kontakt: tbsc@usa.com



Eine Kopie des veröffentlichten Inhalts der Studie (in englischer Sprache) könnte besonders für Betriebsärzte und medizinisch vorgebildetes Personal interessant sein; als PDF (von praktisch jedem PC zu lesen) kann sie beim Autor via E-Mail (siehe oben) erbeten werden.

Den bisher einzigen deutschsprachigen Hinweis auf diese Studie fanden wir auf der Website des Westdeutschen Rundfunk unter der Überschrift: ›Volkskrankheit E-Thrombose‹ (www.wdr.de/themen/computer/schiebwoche/2003/index_06.jhtml). Die Seite ist informativ, aber auch unterhaltsam aufgemacht – eine Passage möchte Ihnen Joe Meier nicht vorenthalten:

»... Wie bitte? Mein PC trachtet mir also nach dem Leben? Schwer zu glauben. Ich denke eher, diese Forscher aus Neuseeland sind schlechte Verlierer. Lässt sich allzu leicht durchschauen, diese List: Bauen keine vernünftigen Computer, die Kiwis, entwickeln weder nützliche Software, noch fesselnde Computerspiele – und wollen uns deshalb warnen. Nach dem Motto: ›Esst mehr Kiwis und Lammfleisch!‹«

Joe Meiers Kommentar: »Ich lebe im Südpazifik und entwickle nützliche Software (www.tbsc.int.tc) – wenn auch keine Computerspiele; persönlich sind weder Lammfleisch noch die Kiwi-Frucht mein Geschmack und die Computer werden hier – genauso wie in Deutschland – überwiegend aus Teilen südasiatischer/fernoöstlicher Herkunft zusammengesetzt ...«

Probleme der ›Kurzzeit-Mobilität‹

Es wird nicht so gerne darüber geredet, aber gerade in der IT-Industrie erweist es sich, dass die schönste Kommunikationstechnik die persönliche Begegnung nicht ersetzen kann. Die Folge: Immer mehr Menschen müssen für jeweils kurze Zeit ins Ausland.

DIE SOFTWARE-INDUSTRIE gilt als eine Branche mit hochflexibler, mobiler ›Wissensarbeit‹. In zahlreichen Zeitungen und Management-Journalen werden international verstreute Projekte und ›virtuelle Teams‹ präsentiert. Da tauschen Projektmitarbeiter sich effizient über Datenetze aus und treffen sich ab und zu – jeder mit einem winzigen Laptop im Gepäck – an irgendeinem Ende der Welt. Die ›Helden‹ dieser Artikel sind zumeist jung, flexibel, hoch motiviert und abenteuerlustig – oder erwecken zumindest glaubhaft diesen Eindruck. Entsprechend leichtfüßig kommt in solchen Darstellungen denn auch die internationale Mobilität daher. Selten wird hinterfragt, mit welchen konkreten Folgen ein solches hochmobiles Arbeiten verknüpft ist.

Im Folgenden werden einige Aspekte projektbezogener Mobilität beschrieben, mit denen international arbeitende Software-Experten konfrontiert sind. Ich beziehe mich dabei auf Fallstudien aus den Forschungsprojekten EMERGENCE¹ und ›Grenzenlose Arbeit‹². Darin wurden IT-Experten befragt, die in indisch/deutschen Software-Projekten arbeiten. Ebenso fanden Gespräche mit den jeweiligen Projekt-Managern, zum Teil auch mit Personalverantwortlichen und

– sofern vorhanden – mit Arbeitnehmervertretern statt.

Bei den meisten, eher generellen Aspekten geht es dabei um die Situation indischer wie deutscher IT-Experten. Vor allem beim Verhältnis von Berufs- und Privatleben der hochmobilen Wissensarbeiter beschränkt sich die Auswertung allerdings auf die Situation der deutschen Software-Entwickler. Die ›indische Situation‹ unterscheidet sich in diesem Bereich doch wesentlich von der westli-

1... EMERGENCE ist ein von der EU-Kommission finanziertes europäisches Verbundprojekt, in dem Verlagerungsprozesse elektronisch gestützter Arbeit (›eWork‹) innerhalb Europas und von und zu anderen Regionen untersucht wurden. Ergebnisse aus dem Projekt sind zu finden unter:

www.emergence.eu

2... Das von der Volkswagen-Stiftung geförderte Forschungsprojekt ›Grenzenlose Arbeit‹ untersuchte die Arbeitsbedingungen in internationalen F&E-Kooperationen. Eine ausführliche Fallstudie der Autorin über das Arbeiten in indisch-deutschen Software-Projekten ist zu finden unter:

www.fastev-berlin.de (FAST-Studie Nr.33)



cher Industrienationen und kann in diesem Rahmen nicht eingehend analysiert werden.

Untersuchung der Kurzzeit-Mobilität

UNTER ›KURZZEIT-MOBILITÄT‹ ist ein Auslandsaufenthalt von wenigen Tagen bis hin zu wenigen Monaten zu verstehen, bei einer am Heimatstandort und am Wohnsitz weitgehend unverändert bleibenden Situation.

Folgende Software-Kooperationen wurden untersucht (die wirklichen Firmennamen wurden durch ›Decknamen‹ ersetzt):

(1) Bei Globecom handelt es sich um ein multinationales Unternehmen mit etwa 90 000 Beschäftigten, das Teams von Software-Entwicklern unter anderem in Deutschland und Indien hat. Die indische Einheit bildet konzernintern mittlerweile den größten Software-Standort. Sie nimmt allerdings auf Grund der Ferne zu den Kundenmärkten eine überwiegend interne Zulieferer-Rolle ein. Untersucht wurde ein indisch/deutsches Team, in dem verschiedene Software-Lösungen gemeinsam entwickelt werden. Es handelt sich also um eine firmeninterne Kooperation. Die technische Projektleitung erfolgt überwiegend von Deutschland aus. Es finden Reisen zwischen Deutschland und Indien sowie auch zu Kunden in anderen Ländern statt.

(2) Softec ist ein Software-Unternehmen mit einem Hauptquartier in Bombay und Tochterunternehmen in verschiedenen westlichen Industrieländern, zum Beispiel auch in Deutschland. Softec hat über 1000 Beschäftigte. Die Software-Entwicklung findet überwiegend in Indien statt, aber es arbeiten häufig indische Entwickler für eine gewisse Zeit bei deutschen Kunden. Die deutsche Tochter – Softec Deutschland – ist mit etwa zehn Angestellten für Marketing und Koordination in Deutschland zuständig. Und sie betreut indische Ingenieure während ihrer Deutschlandaufenthalte.



Der generelle Bedarf an projektbezogenen Reisen

ANDERS ALS VIELFACH angenommen, ist in internationalen Projekten trotz immer leistungsfähigerer elektronischer Kommunikationsmedien das reine ›Arbeiten auf Distanz‹ sehr selten. Persönliche Mobilität ist weiterhin nötig und erreicht sogar ein erhebliches Ausmaß. So sind viele in Kundenprojekten arbeitende Software-Entwickler 50 Prozent (!) ihrer Arbeitszeit unterwegs.

Reisen sind immer dort nötig, wo es um kompliziertere Aufgaben geht, die viel Kommunikation zwischen den Entwicklern erfordern – zum Beispiel bei der Festlegung der Anforderungen an eine Software oder wenn es um das Design der Software geht. Hier muss im Zusammenspiel von Ideen, Kritik und Gegenvorschlägen ein gemeinsames Verständnis über die zu entwickelnde Software erarbeitet werden.

Aber nicht nur dabei ist die persönliche Zusammenarbeit (›Face-to-Face‹-Kommunikation) nötig, auch soziale Funktionen lassen sich nicht ohne Weiteres durch Kommunikationsmedien ersetzen – dies betrifft die Entwicklung von Vertrauen und Verbindlichkeit in einem an verschiedenen Orten arbeitenden Team ebenso wie die Überbrückung kultureller Differenzen. Und schließlich

zeigen sich auch oft noch Grenzen der eingesetzten Telekommunikationstechnik. So kommt es beim Datentransfer zwischen den Kontinenten immer noch zu sehr langen Wartezeiten und bei Videokonferenzen sorgen Bild/Ton-Verzerrungen dafür, dass sie oft keinen echten Ersatz für persönliche Zusammenkünfte bieten.

Die Erwartung westlicher Kunden, sie könnten nach einer Festlegung der Anforderungen die eigentliche Software-Entwicklung komplett zum Beispiel nach Indien delegieren, um sich dann nur noch aus der Ferne und ›nebenbei‹ darum kümmern zu müssen, wird in aller Regel also nicht erfüllt. Es entsteht vielmehr ein hoher Gesprächs-, Rücksprache- und Steuerungsbedarf, der über die Distanz hinweg nicht eingelöst werden kann. Häufig gibt es deshalb sehr kurzfristig anberaumte Treffen im Ausland, bei denen aktuell auftretende Probleme bearbeitet werden müssen.

Die Folge ist: Viele Reisen sind – und das wäre dann auch das erste Problem der Kurzzeit-Mobilität – nicht langfristig und gut genug geplant, oft verlängert sich ein Auslandsaufenthalt sogar kurzfristig.

Konsequenzen für die private Lebensführung

HÄUFIGES REISEN HAT natürlich Konsequenzen für die private Lebensführung. Die persönliche Zeitverwendung wird durch die kurzfristig anfallenden Reisen weitgehend fremdbestimmt. So meint ein deutscher Entwickler in Bezug auf seine privaten Pläne für die nächsten Wochenenden: »Für die nahe Zukunft bin ich nicht besonders gut im Planen [...] Es kann sein, dass ich von dann bis dann irgendwo in Arabien sein muss. Eigentlich will ich das nicht – aber man weiß ja nie. Und da das durchaus auch noch einige Tage vorher oder nachher brauchen kann, weiß ich alles nicht so genau.« Eigene Vorhaben wie Urlaub oder Besuche hält dieser Entwickler lange Zeit in der Schwebe, immer in der

Hoffnung, dass es ›in letzter Minute‹ doch noch klappt. Dies beeinflusst natürlich in erheblichem Maß die soziale Integration der Beschäftigten und die Gestaltung ihres Privatlebens. Betroffen sind auch nicht nur die jeweiligen Ingenieure selbst, sondern ebenso (Ehe-) Partner, Kinder und andere nahe-stehende Personen. In einer anderen Studie über berufliche Mobilität zeigt sich denn auch, dass vor allem die Partner hochmobiler Beschäftigter sich negativ betroffen fühlen³. Und die ›Mobilen‹ selbst haben häufig ein ›schlechtes Gewissen‹. Das kann so weit gehen, dass die Phase der Familienbildung zeitweilig verschoben wird oder sogar ganz ausbleibt.

Andererseits gibt es eine gewisse ›Bandbreite‹ im Umgang mit der projektbedingten Mobilität. Am einen Ende dieses Spektrums steht der ›Drifter‹ (oder der ›bindungslose Nomade‹), am anderen Ende der Familienvater, der seine sozialen Verpflichtungen gegen die Übergriffe aus dem Beruf verteidigt.

Der Drifter – ein ›bindungsloser Nomade‹

Ein Beispiel für den ›Drifter‹ ist der schon erwähnte allein stehende Software-Entwickler, dem die häufigen Reisen die Verfolgung von Freizeitaktivitäten und die Aufrechterhaltung sozialer Kontakte erschweren. So berichtet er von einem Theaterkurs, an dem er teilnehmen wollte: »Das erste Mal hätte ich gekonnt, aber schon an den nächsten Terminen nicht mehr, und das bringt's ja nicht.« Also verzichtete er auf den Kurs. Auch der schon lange geplante Umzug in eine neue Wohnung findet nicht statt – durch die häufige Abwesenheit fehlt es an der Motivation, sich eine schönere

Wohnung zu suchen. Auch frische Lebensmittel hat er selten – es sei denn, er ist einmal fünf Wochen am Stück zu Hause. Der ›Drifter‹ öffnet dem Übergreifen des Berufslebens ins Private also Tür und Tor und stellt damit seine persönliche Lebenszeit der Firma als ›Flexi-



bilitäts-Ressource‹ zur Verfügung. Soziale Bindungsarmut und Konzentration aufs Berufliche verstärken sich gegenseitig: Der Entwickler hat wenig Privatleben, weil er viel reist, und er reist viel, weil er wenig Privatleben hat ...

Der ›Familienvater‹

Der Gegenteil ist der ›Verteidiger des Privatlebens‹: Auch er ist etwa hundert Tage im Jahr abwesend und seine Ehefrau beklagt, dass seine Zeit ein ›knappes Gut‹ darstellt. Der Familienvater setzt jedoch – im Gegensatz zu seinem allein stehenden Kollegen – einige Grenzen: Zwar macht auch er zahlreiche Überstunden und arbeitet oft zu Hause,

nutzt die relative Selbstständigkeit in seiner Zeitgestaltung jedoch auch für seine Familie: »Ich versuche die Balance zwischen Arbeits- und Privatleben. Ein Beispiel: Ich hab zum Schluss meine Reisen nur noch so geplant, dass ich Montags gehe und Donnerstags aus den USA zurückfliege. Das heißt, ich bin

Freitag mittag hier. ›Freitag mittag hier‹ heißt: Ich gehe nicht mehr ins Büro. Ich verbringe die Zeit mit der Familie.«

Das führt allerdings oft zu stark komprimiertem Arbeiten im Ausland: »Ich habe in den USA 16 Stunden am Tag gearbeitet – regelmäßig. Samstag und Sonntag. Einfach: Ich hab keinen Tou-

risten-Trip gemacht oder so, sondern durchgearbeitet und gesagt, die Zeit möchte ich zu Hause wieder abfeiern.« Dieser Ingenieur erlaubt auch nicht, dass plötzlich auftretende Reise-notwendigkeiten jederzeit seine private Planung torpedieren: »Zum Beispiel an Geburtstagen von Kindern, da nehme ich Urlaub.

Punkt. Da gibt es keine Diskussion. Und das kann ich jetzt schon festlegen, dass ich in zwei Jahren, am 19. Juli, am Geburtstag meiner Tochter, auf keiner Geschäftsreise bin.« Diese Zeitsouveränität behauptet er auch bei Kundenkontakten, die ansonsten häufig als absolut zwingende Gründe gelten, eigene Planungen zu revidieren: »Dieses Jahr, da war ich in England. Da war an einem

Freitag Kinderfest, irgendwas, wo es traurig gewesen wäre, wäre ich nicht da gewesen. Da habe ich gesagt: ›Ihr habt das schon zwei Monate vorher gewusst. Ich buche meinen Flug genau so, dass ich Donnerstagabend heimkomme.‹«

Eine solche Terminplanung nehme einem auch keiner übel.

Familiäre Verpflichtungen zählen also durchaus als legitime Ursachen für Unabkömmlichkeit und werden von Kollegen und Vorgesetzten akzeptiert. Dies durchzusetzen erfordert allerdings die Bereitschaft, die Souveränität des Priva-



3... N. Schneider, K. Hartmann, R. Limmer: **Berufsmobilität und Lebensform / Sind berufliche Mobilitätsanforderungen in Zeiten der Globalisierung noch mit Familie vereinbar?** Schriftenreihe des Bundesministeriums für Familie, Senioren, Frauen und Jugend 2001

ten ständig gegen Anforderungen von Seiten der Kunden, Vorgesetzten oder Kollegen zu behaupten. Nicht zu vergessen ist hierbei auch, dass IT-Experten sich oft sehr stark mit den zu erreichenden Projektzielen identifizieren. Es entsteht also auch ein innerer Konflikt zwischen dem Erfüllen von Projektanforderungen und dem Erhalt des Privatlebens. Und: Private Freiräume, die sich die Betroffenen schaffen, müssen häufig durch höhere Arbeitsintensität oder Überstunden an anderer Stelle ausgeglichen werden. Denn meistens sind die Projektziele so eng gesteckt, dass sie in Normalarbeitstagen einfach nicht zu bewältigen sind.

Insgesamt lässt sich also sagen, dass die projektbezogenen Mobilitäts-Erfordernisse stark an den Betroffenen zerren; es bleibt Aufgabe des Einzelnen, ständig von Neuem über die Grenzen zu verhandeln und das Übergreifen der Arbeit auf das private Leben zu verhindern.

Die Situation der indischen Software-Entwickler/innen

Noch einmal anders gestaltet sich die Balance von Arbeits- und Privatleben bei den indischen IT-Experten: Von einer Abwesenheit des Ehepartners ist die zu Hause bleibende indische Familie weit stärker betroffen als in Deutschland, denn das (auch nur zeitweise) Alleinleben ist dort eine weit weniger verbreitete Lebensform. Das Verreisen eines verheirateten Ingenieurs stellt deshalb die gesamte Familie unter Anpassungsdruck. Beispielsweise zieht die Ehefrau eines indischen Entwicklers zeitweise zu ihren Eltern, oder die Geschwister ziehen zu ihr – jedenfalls wird durch das Reisen eines Entwicklers oft die gesamte Familie mobil. Die betroffenen Angehörigen sind damit nicht glücklich, akzeptieren aber die Reisen als finanziell einträgliche und karrierefördernde Notwendigkeiten.

So ist das bei indischen Männern. Indische Software-Entwicklerinnen hingegen stehen, nachdem sie geheiratet haben, für längere oder häufige Auslandsreisen oft gar nicht mehr zur Ver-

fügung. Ein deutscher Manager dazu: »Es gibt öfter mal eine Frau, die sich bestimmte Fähigkeiten erworben hat bei der Arbeit in Indien, und die man vor Ort schicken müsste. Das geht dann einfach nicht, weil sie nicht darf und nicht kann.«

Insofern ist die projektbezogene Realität insbesondere für weibliche indische IT-Experten mit besonderen Problemen verbunden. Deren Auswirkungen auf die Chancengleichheit weiblicher und männlicher IT-Fachkräfte wären gesondert zu untersuchen.

Die Arbeitssituation im Ausland

DAS BEFRISTETE ARBEITEN im Ausland ist zumeist durch exzessive Überstunden gekennzeichnet. Überstunden und unbezahlte Mehrarbeit sind zwar für die Software-Industrie generell nicht untypisch, aber im Ausland potenziert sich diese Tendenz noch. Das kommt zum einen davon, dass vor allem wenige Tage dauernde Geschäftsreisen zeitlich oft sehr knapp geplant sind, so dass jede verfügbare Stunde für Treffen und andere Tätigkeiten genutzt wird. Aber auch bei längeren Aufenthalten haben die Entwickler außer Arbeiten oft nicht viel zu tun. Die meisten Interviewpartner berichten daher, dass sie während ihrer Geschäftsreisen fast ausschließlich zwischen Hotel und Firma pendeln.

An die Arbeitstage schließen sich zumeist dann noch gemeinsame Abendessen mit den Gastgebern oder Kollegen an. So beschreibt ein deutscher Software-Entwickler seinen Besuch bei der Partnerfirma in Indien: »Der Arbeitstag war sehr lang. Da sind wir jeden Abend zum Essen eingeladen worden, und ich wollte das eigentlich gar nicht. Ich wollte auch mal direkt ins Hotel, um acht oder neun Uhr, und ein bisschen fernsehen oder an die Bar und dann schlafen. Ich war halt wegen der Zeitverschiebung fertig und k.o. – aber da hatten die schon immer einen Tisch reserviert. Also, mir gefällt das allgemein nicht so.«

Hier wird deutlich, dass es oft auch die informellen Verpflichtungen sind, die den Beteiligten in internationalen

Projekten einen hohen Grad zusätzlichen Engagements abfordern.

Dies trifft natürlich auch für die ›Gastgeber‹ zu, die ihre Besucher oft tage- oder wochenlang betreuen. Die heimischen Kollegen fühlen sich meist verpflichtet, ein soziales Begleitprogramm anzubieten, seien es die gemeinsamen Abendessen, Stadtbesichtigungen oder Wochenendausflüge. Meist versucht man, diese informellen Verpflichtungen auf mehrere Schultern zu verteilen. Ein deutscher Ingenieur jedoch, der der einzige Bezugspartner für die ausländischen IT-Experten der Partnerfirma war, ging wochenlang täglich mit den indischen Gästen aus: »Ich hab das schon als Bestandteil der Arbeit begriffen. Sehr belastend ist es natürlich nicht, aber schon verpflichtend. Halb freiwillig, halb gezwungen.« Eine Folge dieser Aktivitäten sei, dass man, wie er sagt, »auch persönlich nichts mehr erledigt bekommt«. Insofern sind Auslandsreisen auch für die ›empfangenden‹ Kollegen eine nicht unerhebliche Beanspruchung.

Zurück zu den ›Mobilen‹: Von ihnen kann man überwiegend sagen, dass es ein wirkliches Privatleben während der Dienstreisen oft nicht gibt. Soziale Kontakte sind meist auf Kollegen beschränkt – auch bei längerfristigen Auslandsaufenthalten sind es oft andere ›Verbannte‹, mit denen man seine Freizeit gestaltet. Die sozialen Kontakte gehen also weitgehend im Beruflichen und dessen Begleiterscheinungen auf. Das Fehlen des ›rechten Privaten‹ wird vor allem bei mehrwöchigen Aufenthalten als vereinsamend und entleerend empfunden. Ein Ingenieur, der für mehrere Monate in den USA arbeitete, flog daher jedes zweite Wochenende nach Deutschland zu seiner Familie.

Konkrete Probleme der Alltagsgestaltung

UM DIE UNTERBRINGUNG der mobilen Arbeitskräfte kümmern sich die Firmen. Die meisten Software-Entwickler wohnen bei kurzen Reisen im Hotel. Bei et-

was längeren Aufenthalten werden Wohnungen in Appartementshotels oder möblierte Wohnungen angemietet. Dies ist häufig der Fall bei der deutschen Softec-Tochter, deren indische IT-Experten oft mehrere Wochen oder Monate bei einem deutschen Kunden arbeiten.

Nun ist ja das Wohnen für die meisten Menschen eine sehr persönliche Angelegenheit, bei der individuelle Vorlieben und Abneigungen eine große Rolle spielen. Durch die fremdbestimmte Organisation des Wohnens treten deshalb Probleme auf – sei es, weil sich zum Beispiel die indischen IT-Experten in einer möblierten Wohnung fremd fühlen, sei es, weil die Wohnung eine für einen Fremden sehr ungünstige Lage hat. So berichtet der Geschäftsführer der deutschen Softec: »Es gab einmal einen Fall, wo ein Programmierer gesagt hat, er kommt nicht mehr zurück nach Deutschland für längere Zeit. Der war während dem Winter in St. Georgen untergebracht. Tiefschnee, die schneereichste Gegend im Schwarzwald, und der Kunde hat ihn unglücklicherweise damals in eine Neubausiedlung gesetzt, wo wenig Busse gefahren sind. Ich bin zwar zwei bis drei Mal mit ihm wandern gegangen und so, hab mich selber um ihn gekümmert, aber das können Sie nicht jeden Tag tun.«

Die Softec-Tochter fühlt sich auch nur begrenzt dazu verpflichtet oder in der Lage, den Entwicklern individuell optimale Wohnungen anzubieten. So meint eine Assistentin von Softec: »Teilweise, wenn ich Wohnungen suche und die sind nicht zufrieden damit, dann gibt's schon mal die Frage, ob ich nicht noch weitersuchen kann. Aber ich kann nicht für jeden drei Wohnungen suchen zur Auswahl.« Ein Personalverantwortlicher der indischen Softec-Mutter bringt es so auf den Punkt: »We are here to do business. We are not here to end up in a real estate agency for people.« (Wir sind dafür da, unsere Arbeit zu tun. Wir sind nicht dafür da, zu einer Immobilien-Vermittlung zu werden.)

Finanziell ist die Mobilität für die meisten Entwickler der untersuchten Firmen übrigens attraktiv: Es gibt tägli-

che Pauschalen von mindestens 50 US-Dollar und die Übernahme der Wohnungsmiete oder großzügige Zulagen. Keiner der Befragten berichtete von finanziellen Nachteilen durch die Auslandsreisen. Vor allem für die indischen IT-Experten ist der Auslandseinsatz mit einem starken finanziellen Anreiz verbunden.

Schwierigkeiten treten eher in »profanen« Bereichen auf – zum Beispiel wenn indische Software-Entwickler keine gültige internationale Fahrerlaubnis besitzen. So berichtet ein deutscher Globecom-Manager: »Wir hatten vorletztes Jahr einen Inder in den USA eingesetzt in einem meiner Projekte. Es war katastrophal. In den USA, in einer ländlichen Gegend, braucht man einfach ein Auto, was anderes geht nicht. Wir hatten dann einen, der hat den jeden Morgen abgeholt und wieder hingefahren. An solchen einfachen, praktischen Dingen scheitert es oft.« Auch der deutsche Kollege, der den Inder täglich chauffieren musste, reagierte nach einiger Zeit entnervt.

Als letzter alltäglicher aber dennoch wichtiger Punkt sei noch die Frage der Ernährung genannt, die vegetarisch lebenden Indern zum Teil erhebliche Probleme bereitet. Um das fleischreiche Essen der Süddeutschen zu umgehen, fuhr beispielsweise ein indischer Projektmanager jeden Abend in die nächste Stadt, da dort das einzige indische Lokal weit und breit war.

Es gibt aber auch einige Glanzlichter bei Geschäftsreisen. Dies vor allem, wenn bei längeren Aufenthalten genug Zeit ist für Ausflüge ins Umland. Der Kontakt mit der Fremde ist für einige der Befragten durchaus faszinierend, was für sie die Geschäftsreisen trotz aller Belastungen auch zu einer Bereicherung macht.

Selbst die potenziellen Belastungsfaktoren, mit denen der Alltag im Ausland verbunden ist, werden von einigen IT-Experten eher als motivierende Herausforderung erlebt. Die Notwendigkeit, zahlreiche Mobilitätsfolgen individuell auszuhalten oder in Eigenregie zu bewältigen, wird von den Betroffenen keineswegs immer kritisiert, sondern als selbstverständlicher Bestandteil der eigenen Berufsrolle wahrgenommen.

Diese Software-Entwickler erleben den Umgang mit Unvorhergesehenem und Ungeordnetem als Element ihrer beruflichen Identität. Mehr noch: Einige beschreiben die notwendige Bewältigung der Anforderungen des internationalen Arbeitens geradezu lustvoll. Nach wenigen Wochen der Arbeit am heimatischen Schreibtisch werden sie unruhig und hoffen auf eine baldige Reisemöglichkeit. So meint ein deutscher IT-Experte: »Ich würde keinen Job wollen, wo ich jeden Tag immer am gleichen Schreibtisch sitze. Ich genieße das schon, die Reiserei. Ab und zu mal rauszukommen, mal was anderes zu sehen. Ich finde das toll.« Insofern wäre es einseitig, die Kurzzeit-Mobilität als reine Belastung zu beschreiben. Oftmals wird sie auch als eine attraktive Abwechslung und anspornende Herausforderung erlebt.

Unterstützung durch die Firma?

WAS TUN DIE FIRMEN, um die internationale Mobilität ihrer Beschäftigten zu unterstützen und Schwierigkeiten zu vermeiden? In der Management-Literatur ist man sich ja einig über die hohe Bedeutung eines »International Human Resources Management«, das Mobilität gestaltet und mögliche Belastungen abfängt. Zu wichtigen Aspekten zählen dabei die systematische Vorbereitung von Auslandseinsätzen und das Training sowie die Unterstützung während des Auslandseinsatzes selbst.

Die Praxis sieht aber oft ganz anders aus: Gerade beim großen multinationalen Unternehmen Globecom bleibt die Gestaltung der internationalen Mobilität weitgehend der Verantwortung der Angestellten überlassen; organisierte Unterstützung wird kaum angeboten. Bis auf die »harten« administrativen Dinge wie Visum-Organisation, Reise-gestaltung, Wohnungssuche und die großzügig geregelte finanzielle Seite ist die Gestaltung der projektbezogenen Mobilität weitgehend der Selbststeuerung der IT-Experten überlassen.



Auf das Ausland bezogene Trainingsmaßnahmen hatte keiner der Befragten gemacht. Wie man im Ausland zurecht kommt, können die Ingenieure nur lernen, indem sie auslandserfahrene Kollegen befragen. Das heißt: Lernprozesse werden individuell durchlaufen und starten immer am Punkt Null. Auch die Betreuung im Ausland ist vor allem eine informelle Verpflichtung der ›Gastgeber‹-Kollegen. Personal, das für die Betreuung der ›Mobilen‹ zuständig wäre, gibt es nicht (oder ist den Betroffenen zumindest nicht bekannt).

Besser ist das bei der wesentlich kleineren indischen Softec und ihrer deutschen Tochter geregelt. Auch hier gibt es zwar keine inter-kulturellen Trainings, aber immerhin werden Deutsch-Sprachkurse angeboten für Inder, die nach Deutschland kommen. Auch gibt es eine interne Website mit Informationen über Deutschland. Diese reichen von den ›Do's and Dont's‹ (was man tut und was man besser lässt) in sozialen Kontakten bis hin zu der Frage, welche Münzen man am deutschen Flughafen parat haben sollte, um einen Fahrkartenautomaten zu bedienen.

In der deutschen Softec-Tochter arbeitet sogar ein Inder als ›Account Manager‹. Darauf wurde in der deutschen Einheit großer Wert gelegt, da ein Inder natürlich die Schwierigkeiten indischer Entwickler in Deutschland besser verstehen und lösen kann. Softec hat generell einen recht fürsorglichen Ansatz. Man versucht, engen Kontakt zu den in Deutschland arbeitenden Entwicklern zu halten und sie bis hin zur Organisation von Zahnarztterminen zu unterstützen.

Dennoch aber gibt es im Softec-Büro, in dem weniger als zehn Angestellte arbeiten, keine eigenständige Position für diese Aufgaben. Das führt zu einer hohen Beanspruchung aller Angestellten. Fast alle sind ›nebenbei‹ mit Fragen der Betreuung indischer IT-Experten befasst – von der Assistentin über die Verkäufer bis hin zum Geschäftsführer und dazu auch noch der Personal-Manager in Indien. So mischt zum Beispiel

jeder ein bisschen mit bei der Wohnungsfrage.

Anzunehmen ist, dass das Fehlen einer professionellen Personalbetreuung die betroffenen Entwickler mit zum Teil unzusammenhängenden, zerfaserten Verfahren und Regeln konfrontiert. So machte zum Beispiel jeder der Angestellten unterschiedliche Angaben über die Urlaubstage, die den Entwicklern bei längeren Aufenthalten zustehen (die Aussagen reichten von 10 bis 30 Tage im Jahr!). Ob und in welcher Weise sich das auf den von den indischen Entwicklern tatsächlich in Anspruch genommenen

Urlaub auswirkt, konnte im Rahmen der Fallstudie leider nicht mehr festgestellt werden ...

Karin Hirschfeld ist wissenschaftliche Mitarbeiterin bei der Forschungsgemeinschaft für Außenwirtschaft, Struktur- und Technologiepolitik (FAST) e.V., Berlin; Kontakt: hirschfeld-fastev@t-online.de



Der Artikel basiert auf einem Vortrag, den die Autorin im November 2002 im Rahmen des ›IT mobility forum‹ von UNI (Union Network International) in Sophia Antipolis (Frankreich) hielt. Nähere Informationen:

www.union-network.org

MATTHIAS WILKE

GPS: Mitbestimmung im Weltraum?

**Mitbestimmung kennt keine Grenzen –
das zumindest dann nicht, wenn Satelliten eingesetzt
werden, um die Leistung und das Verhalten von
Arbeitnehmer hier auf mitteleuropäischer
Erde zu überwachen.**

DER AUFGABENBEREICH für Betriebsräte hat sich ausgedehnt – bis weit hinein in die Erdumlaufbahn! Denn dort kreisen die Satelliten für das weltweite Global Positioning System (GPS). Diese Technologie ermöglicht es, jederzeit festzustellen, welche Person sich zu welcher Zeit und an welchem Ort aufgehalten hat. GPS ist damit (unter anderem) ein neues Instrument, das ›dazu bestimmt ist, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen‹ (§ 87 Abs. 1 Nr.6 BetrVG). Die ›Einführung und Anwendung‹ die-

ser, wie es im Betriebsverfassungsgesetz so schön heißt, ›technischen Einrichtungen‹ ist also mitbestimmungspflichtig ...

Und tatsächlich findet die GPS-Technologie nach und nach Einzug in den betrieblichen Alltag. In Firmenwagen und LKW wird GPS bald so selbstverständlich sein, wie es heute die klassischen Fahrtenschreiber sind – und es sind noch darüber hinausgehende Einsatzmöglichkeiten denkbar.

Speditionen wissen jetzt bereits punktgenau, wo sich ihre Lieferfahrzeu-

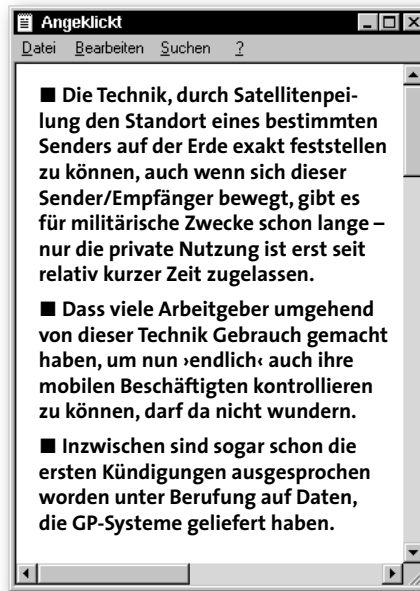
ge gerade befinden, der Einsatz von Baumaschinen wird damit koordiniert, Rettungsfahrzeuge werden per GPS an Ort und Stelle geleitet, ambulante Pflegedienste können ihr Personal und deren anstehende Aufgaben über GPS aufeinander abstimmen und selbst Mittelklassewagen sind inzwischen schon mit elektronischen ›Straßenkarten‹ ausgestattet, die den Weg zu jedem beliebigen Ziel zeigen.

Gut funktionierende GP-Systeme sind bereits ab etwa 300,- Euro auf dem Markt zu haben und kaum größer als ein ›Handy‹, so dass es im Grunde jeder in der Tasche mit sich führen kann. Kein Wunder, dass inzwischen immer mehr Unternehmen ihre Dienstfahrzeuge mit GPS ausgerüstet haben – und: Kein Wunder, dass den ersten Beschäftigten auf Grund von GPS-Protokolldaten bereits gekündigt worden ist.

Wie so viele technische Innovationen hat die GPS-Technologie einen militärischen Hintergrund. Sie entstand ursprünglich als Navigationssystem im Rahmen des so genannten ›Star-War‹-Programms der Reagan-Regierung. Neben der militärischen Nutzung wurde GPS aber schon vor Jahren auch weltweit zur zivilen Navigation freigegeben. Um aber dem ›Feind‹ im so genannten Kalten Krieg den Gebrauch des hochgenauen Systems für eigene militärische Zwecke zu erschweren, wurde die Genauigkeit des zivilen GPS-Signals künstlich vergrößert, so dass zivilen Nutzern statt der auf wenige Meter genauen militärischen Positionsbestimmungen nur eine grobe Annäherung zur Verfügung stand.

Durch Selective Availability (SA = ausgewählte Zugänglichkeit) veränderte das US-amerikanische Verteidigungsministerium je nach militärischer Lage die Genauigkeit des zivilen Signals und schaltete es zeitweise auch ganz aus. Für die praktische Nutzung in der Wirtschaft stand GPS deshalb nicht zur Verfügung, allenfalls Freizeitsegler setzten die Technik zur Unterstützung ihrer herkömmlichen Navigation ein.

Seit Mai 2000 aber hat die US-Regierung die künstliche Ungenauigkeit des



GPS-Satelliten-Systems abgeschaltet. Mit dieser Abschaltung erfüllte die Regierung Forderungen der amerikanischen Wirtschaft, die eine genaue Ortung durch GPS beispielsweise in der Autoindustrie oder im Transportwesen einsetzen wollte. Statt der früher global angewendeten ›Selective Availability‹ lässt sich nun – etwa im Fall regionaler Kriege – die GPS-Genauigkeit gezielt für einzelne Länder herabsetzen.

Seitdem ist der GPS-Empfänger auch für zivile Anwendungen interessant geworden, da jetzt die tatsächliche Position zu Lande oder zu Wasser auf ein bis zwei Meter genau angezeigt werden kann.

Wie funktioniert die GPS-Technologie?

DIE GRUNDIDEE IST einfach: Das System basiert auf der Messung der Weg- und Zeitdifferenzen, die auftreten, wenn Signale zwischen der Erde und verschiedenen GPS-Satelliten im Weltraum ausgetauscht werden. Das bedeutet, dass die Position auf der Erde durch die Messung der Entfernung zu einer Gruppe von Satelliten im All bestimmt wird – die Satelliten bilden die exakten Referenzpunkte.

Die Entfernung zu einem Satelliten wird dabei durch die Messung der Zeit bestimmt, die ein Funksignal braucht, um den Empfänger vom Satelliten aus zu erreichen. Um nun die jeweilige Position auf der Erde zu bestimmen, muss das GP-System neben der Entfernung

auch die Position der Satelliten im Weltall kennen. Und die GPS-Satelliten fliegen so hoch, dass ihre Umlaufbahnen sehr gut vorherzusagen sind. Kleine Veränderungen der Position im Orbit werden ständig vom US-Verteidigungsministerium gemessen und von den Satelliten an die GP-Systeme auf der Erde übermittelt.

Durch ständige Neuberechnung der aktuellen Position kann der GPS-Empfänger auch genau die Geschwindigkeit und Bewegungsrichtung (als ›ground speed‹ und ›ground track‹ bezeichnet) berechnen.

Vereinfacht gesagt liegt der Positionsbestimmung das gleiche Prinzip zu Grunde, das man bereits als Kind genutzt hat, um die Entfernung eines Gewitters abzuschätzen. Dabei wurde (und wird wohl immer noch) abgezählt, welche Zeitdifferenz zwischen dem Sehen des Blitzes und dem Eintreffen des Donners vergangen ist (im Vergleich zur Schall- ist die Lichtgeschwindigkeit so hoch, dass man die Laufzeit des Lichts vom Ausgangspunkt zum Beobachter nicht berücksichtigen muss). Da sich Schall in Luft mit etwa 340 m/s ausbreitet, ergibt sich so aus zum Beispiel drei Sekunden Zeitdifferenz zwischen Blitz und Donner eine Entfernung von etwa einem Kilometer.

Dabei wird allerdings noch keine Position bestimmt, sondern nur eine Entfernung ermittelt. Mit mehreren Entfernungsbestimmungen ließe sich jedoch zusätzlich eine Positionsbestimmung durchführen. Um beim Beispiel mit dem Blitz zu bleiben, würde das bedeuten, dass mehrere Leute um die Stelle des Blitzschlags verteilt stehen und die Zeit messen müssten.

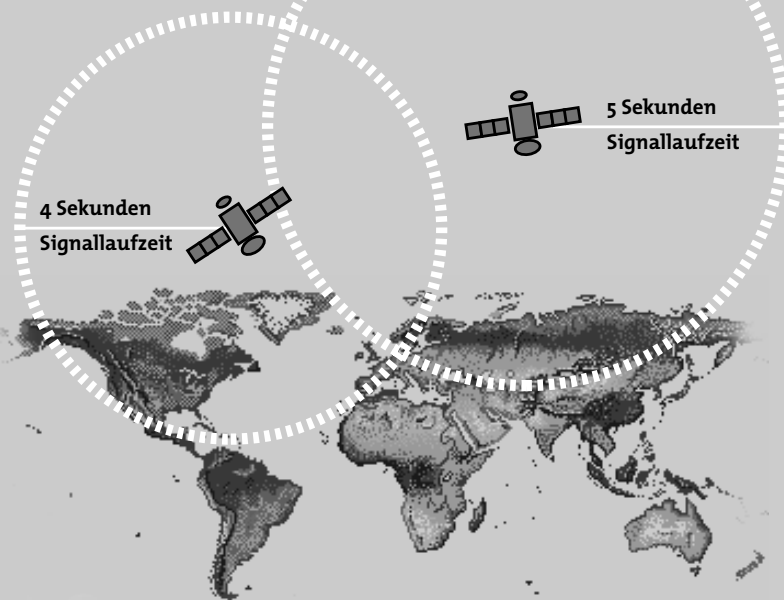
Die vereinfachte Darstellung des GPS-Prinzips auf Seite 20 geht zunächst von zwei Dimensionen aus. Das Prinzip bleibt auch bei steigender Satellitenzahl das gleiche, die Genauigkeit ist allerdings um ›Dimensionen‹ besser ...

Durch die Ermittlung der Entfernung und Position zu mindestens drei Satelliten im Weltall können zusätzlich noch angenommene Uhren-Ungenauigkeiten in den Satelliten korrigiert werden.



Schema 1:

Global-Positioning-System (GPS)



Das Signal vom ersten der beiden Satelliten braucht bis zum GPS-Standpunkt vier Sekunden (tatsächlich beträgt die Laufzeit der Signale vom Satelliten zur Erdoberfläche bei einer Lichtgeschwindigkeit von 299 792 458,0 m/s etwa 0,07 Sekunden). Mit dieser Information lässt sich sagen, dass die gesuchte Position irgendwo auf einem Kreis mit der ›Entfernung 4 Sekunden‹ um den ersten Satelliten herum sein muss. Wenn nun die Laufzeit vom zweiten Satelliten fünf Sekunden beträgt, bleiben die zwei Schnittpunkte der Kreise als einzige mögliche Positionen für Standpunkt des GPS.

So lässt sich der Aufenthaltsort auf der Erde exakt bestimmen (triangulieren). Mit wenigstens drei Satelliten kann der GPS-Empfänger also den Längen- und Breitengrad bestimmen. Dies wird ›2D position fix‹ (zweidimensionale Positionsbestimmung) genannt. Mit Hilfe von vier oder mehr Satelliten kann eine ›3D position fix‹, also zusätzlich noch die Höhe bestimmt werden.

Die ersten Auswirkungen dieser exakten Ortungsmöglichkeiten bekommen die Arbeitnehmer mittlerweile hautnah zu spüren. Unter der Überschrift ›GPS überführt trödelnde Mitarbeiter‹ berichtet die Hannoversche Allgemeine Zeitung vom 23. 11. 2002, dass mehrere Außendienstler ohne ihr Wissen mit einem Satelliten-Ortungs-System überwacht wurden.

Der Arbeitgeber ließ die Dienstfahrzeuge seiner Beschäftigten mit GPS-

Anlagen ausrüsten. Dann verglich er die Protokolle der Ortungs-Systeme mit den Tagesberichten seiner Beschäftigten – und stellte fest, so der Artikel weiter, dass die Berichte allesamt gefälscht waren. Die Mitarbeiter fuhren später los, machten länger Pause oder waren überhaupt nicht bei den Kunden, die sie angegeben hatten. So hatte einer der Außendienstler berichtet, dass er morgens um 8.00 Uhr den ersten Kunden aufgesucht habe. Nach Auswertung der GPS-Protokolle hatte sich sein Auto aber erst kurz nach zehn Uhr zum ersten Mal bewegt.

Auf Grund dieses GPS-Einsatzes und der Auswertung der Protokolle kam es daraufhin bei mehreren Mitarbeitern zu fristlosen Kündigungen. Nachdem die Betroffenen mit den – scheinbar objektiven – GPS-Protokollen ihrer Bewegungsdaten konfrontiert wurden, haben sie den Kündigungen auch nicht widersprochen oder nach Androhung von Strafver-

fahren wegen Betrugs sogar von sich aus gekündigt.

»Im Schnitt waren es pro Mitarbeiter drei Stunden am Tag, die er entgegen seinen Angaben nicht für das Unternehmen tätig war«, so ein Sprecher des Sicherheitsunternehmens Proschutz. Dort war die Software entwickelt worden, die jetzt mit den Daten der GPS-Satelliten ›kriminaltaktische Dienste‹ für Arbeitgeber anbietet.

Bei dieser Form des ›Flotten-Managements‹ besteht die Zielsetzung in erster Linie in der Kontrolle der mobilen Arbeitnehmer. Die Herstellerfirma wirbt denn auch damit, dass ›der Zeitklau‹ der Beschäftigten ›tödlich‹ für ein Unternehmen sei, und rät deshalb: »GPS zur Arbeitsqualitätssicherung, Sie können damit jederzeit den Standpunkt Ihres Mitarbeiters orten!«

Die regelmäßige Positionsbestimmung einzelner mit GPS ausgerüsteter Fahrzeuge oder Personen, ist mittlerweile Standard bei so genannten Positions-Management-Systemen. Marktübliche Systeme zur routinemäßigen Positionsbestimmung liefern in der Regel Daten zu:

- Ort (Stadt/Straße/Hausnummer)
- Zeitpunkt (Abfahrt/Ankunft/Dauer)
- Strecke (Länge und Verlauf)
- Geschwindigkeit (Durchschnitts- und Höchstgeschwindigkeit)
- Standzeit

Im Bereich des ›Flotten-Managements‹ erfolgt daraufhin die Darstellung mehrerer, an verschiedenen Orten sich befindender Fahrzeuge auf elektronischen Landkarten. Die Aktualisierung der Positionsdaten kann jederzeit nach frei wählbaren Kriterien vorgenommen werden.

GPS und Datenschutz

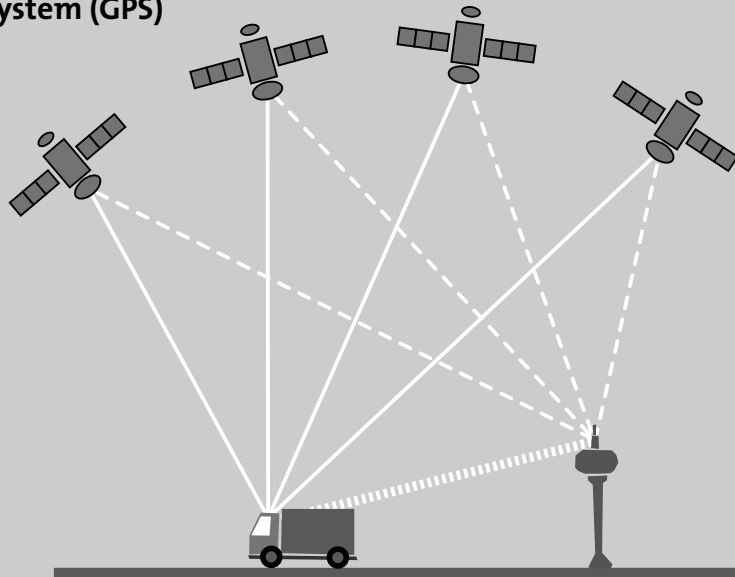
IM GRÖßEREN STIL werden GPS-Geräte bereits in den folgenden Bereichen eingesetzt:

- Speditions- und Transportunternehmen (Logistik und Sicherheit),

info

Schema 2:

Global-Positioning-System (GPS)



Bei der Fahrzeug-Navigation werden Messgenauigkeiten zwischen ein bis drei Meter angestrebt, dafür müssen eine ganze Reihe von Fehlereinflüssen (Ionosphäre, Zeit, Satellitenbahn) eliminiert werden. Dies geschieht mit Hilfe terrestrischer (erdgebundener) Referenzsender und -empfänger. Die Position dieser GPS-Sende-/Empfangsstationen wird sehr genau vermessen. Unter der Voraussetzung, dass am Ort des Nutzers eine Reihe von Abweichungen die gleiche Größenordnung hat wie am Referenzpunkt, wird dann eine Positionsverbesserung errechnet. Die Positionsdaten der Satelliten werden also mit den genau bekannten Positionsdaten der Referenzpunkte auf der Erde verglichen und zu einem Korrekturwert verarbeitet. Dieser wiederum wird über einen Funkkanal an die GPS-Fahrzeuge übertragen, die mit diesem Korrekturwert die Satelliten-Daten verbessern.

- Taxiunternehmen (Disposition von Fahraufträgen, Ortung eines Fahrzeugs nach Auslösung des Notrufs),
- Verwaltung von Fahrzeugen von Sicherheitsunternehmen (optimaler Einsatz beispielsweise bei Alarmverfolgungen),
- Überwachung von Gefahrentransporten, Sonderfahrzeugen (VIP), Geld- und Werttransporten (Sicherheit, standortabhängige Freigabe der Geld-Container ...),
- Baumaschinen-Vermietungsfirmen (Logistik und Sicherheit),
- Dienstwagen von Handelsvertretern und Service-Mitarbeitern.

Entscheidend ist in allen Fällen die Frage, in welcher Form die Positionsdaten und damit die personenbezogenen Daten der Arbeitnehmer für den Arbeitgeber aufbereitet werden – insbesondere hinsichtlich der Leistungsbeurteilung.

Für GP-Systeme, die bei einfacher Konfiguration bereits zu geringen Investitionskosten zu haben sind, sollten Betriebs-/und Personalräte also auf alle Fälle Betriebs-/Dienstvereinbarungen abschließen, damit nur zweckgebundene Auswertungen (z. B.: Sicherheit, Disposition, Alarmverfolgung ...) gemacht werden können und die Beschäftigten vor Verhaltens- oder Leistungsüberwachungen, die zu ihrem Nachteil wären, geschützt sind. Das Mindeste aber ist, dass die Betroffenen über diese neue Form der technischen Kontrolle aufgeklärt werden.

Wie bei jeder Anwendung von Informations- und Kommunikationstechnologie gilt auch für den GPS-Einsatz das Gebot der *Datensparsamkeit* und *Zweckbindung*. Danach dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder nach Abschluss einer Betriebsvereinbarung verwendet werden. Eine personenbezogene Auswertung der GPS-Protokolldateien nach Leistungs- und Verhaltenskriterien aber wäre durch den ursprünglichen Verwendungszweck (z. B. Logistik oder Sicherheit) nicht mehr gedeckt und stellt damit eine Auswertung ohne ge-

setzliche oder vereinbarte Zweckbindung dar.

Nach den Grundsätzen des Datenschutzes hat sich außerdem die Gestaltung und Auswahl der Datenverarbeitung an dem Ziel auszurichten, keine oder so wenig wie möglich personenbezogene Daten zu verarbeiten! Die Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Möglichkeiten, die GPS bietet, abschätzen und ihre Rechte wahrnehmen können.

Der GPS-Einsatz zur Kontrolle der Beschäftigten ist deshalb grundsätzlich nicht zulässig, er ist ein unzulässiger Eingriff in das Persönlichkeitsrecht! Für die Überwachung der Arbeitnehmer durch GP-Systeme gelten dieselben Grundsätze wie beispielsweise bei der Video- und Kameraüberwachung am Arbeitsplatz. Nach Auffassung des Bun-

desarbeitsgerichts verletzt die heimliche technische Überwachung die grundgesetzlich garantierten Persönlichkeitsrechte der Beschäftigten (siehe BAG-Entscheidung vom 7. 10. 1987, Aktenzeichen: 5 AZR 116/86).

Der Videoüberwachung entsprechend kann der Betriebsrat also den GPS-Einsatz am Arbeitsplatz gerichtlich untersagen lassen, wenn dabei Personaldaten verarbeitet werden (siehe: LAG Baden Württemberg vom 14. 4. 1988, Aktenzeichen: 6 Ta BV 1/88).

Demzufolge muss eine Kündigung nicht hingenommen werden, wenn sie auf der Auswertung von GPS-Protokolldateien beruht und wenn für die Datenerhebung keine rechtliche Grundlage (z. B. eine Betriebsvereinbarung) bestand



– selbst eine Eigenkündigung ist ungültig, wenn sie durch Drohung mit einer Strafanzeige und durch den Hinweis auf Aufzeichnungen heimlicher GPS-Protokollierungen zustande gekommen ist (siehe LAG Mannheim vom 6. 5. 1998).

Langfristig wird GPS in immer mehr Bereichen eingesetzt werden und zu enormen Veränderungen in der Arbeitsorganisation führen. Die Betriebsräte stehen bei der Einführung und Anwendung von GPS vor zwei zentralen Herausforderungen: den Arbeitnehmer-Datenschutz sicherzustellen und Rationalisierungsfolgen abzumildern! Denn klar ist, dass die Einführung von GPS nicht ausschließlich zu Lasten der Beschäftigten geschehen darf.

Matthias Wilke, M.A., ist Politologe und Technologieberater bei der Beratungsstelle für Technologiefolgen und Qualifizierung; Kontaktadresse: BTQ Kassel, Akazienweg 22, 34117 Kassel; E-Mail: btqks@bwbtq.de



seminare tagungen schulungen veranstaltungen



BTQ – Beratungsstelle für Technologiefolgen und Qualifizierung Hessen
Akazienweg 22
34117 Kassel

fon 05 61-77 60 04
fax 05 61-77 60 57

18.03.2003

Der gläserne Arbeitnehmer – weltweit? Datenverkehr/Datenschutz in einer globalisierten Welt

27.03.2003

Zielgerichtet handeln – professionelle Arbeitsplanung für den Betriebsrat/Personalrat

13. 05.–15.05.2003

Neue Arbeitszeitmodelle im Krankenhaus

21.05.–23.05.2003

Das Internet richtig nutzen – Praxis-Workshop

26.05.–27.05.2003

Betrieblicher Datenschutz konkret – Auswirkungen des neuen BDSG

02.06.–03.06.2003

Kollege Computer im Krankenhaus – Diagnosis Related Groups (DRG)



tbo-Beratung, Technologie, Beteiligung, Organisation
Lützowstraße 5
30159 Hannover

fon 05 11-13 13 43
fax 05 11-17 5 38

13.03.2003

Arbeiten ohne Ende? Arbeitszeit gesundheitsförderlich gestalten

01.04.–02.04. 2003

Der Wirtschaftsausschuss – Rechtsgrundlagen und wirtschaftliches Basiswissen



TBS NRW Ruhrgebiet
Lothringer Straße 62
46045 Oberhausen

fon 02 08 / 8 20 76 - 0
fax 02 08 / 8 20 76 - 41

06.05.–07.05.2003

Software-Ergonomie am Beispiel SAP

14.05.–15.05.2003

Soziale Beziehungen, soziale Belastungen

21.05.–22.05.2003

Mitarbeitergespräche, Leistungsbeurteilung und Zielvereinbarung



TBS NRW Niederrhein
Goebenstraße 4
41061 Mönchengladbach

fon 0 21 61 / 2 94 07 - 0
fax 0 21 61 / 2 94 07 - 29

08.04.–10.04.2003

Die Homepage für den Betriebs-/Personalrat



TBS NRW Südwestfalen
Körnerstraße 82
58095 Hagen

fon 0 23 31 / 39 76 70
fax 0 23 31 / 1 49 03

02.04.–03.04.2003

Integration von Arbeitsgestaltung und Gesundheitsschutz



TBS NRW Ostwestf./Lippe
Nikolaus-Dürkopp-Str. 17
33602 Bielefeld

fon 05 21 / 9 66 35 - 0
fax 05 21 / 9 66 35 - 10

07.04.–09.04.2003

SAP R/3 kennen lernen – Nutzung durch die Interessenvertretung



TBS NRW Münsterland
Geiststraße 26 a
48151 Münster

fon 02 51 / 5 39 29 - 0
fax 02 51 / 5 39 29 - 99

08.04.–09.04.2003

Digitale Telefonanlagen

07.05.–08.05.2003

Psychosoziale Belastungen bei der Arbeit abbauen – betriebliches Gesundheitsmanagement aufbauen (Teil 2)



VBG Verwaltungs-Berufsgenossenschaft
22281 Hamburg

fon 040-5146-2940
www.vbg.de/seminar/

02.06.–04.06.2003

18.06.–20.06.2003

23.06.–25.06.2003

Bildschirmarbeitsplatzgestaltung: Anforderungen an den Bildschirmarbeitsplatz

07.05.–09.05.2003

Bildschirmarbeitsplatzgestaltung: Software-Ergonomie

14.04.–16.04.2003

12.05.–14.05.2003

19.05.–21.05.2003

Bildschirmarbeitsplatzgestaltung: Workshop Büroeinrichtung

Datenschutz-Gütesiegel

Die Idee ist faszinierend: Ob Software, Hardware oder ein ganzes Unternehmen – Datenschutzsiegel drauf und schon kann man sicher sein, dass mit dem Datenschutz alles paletti ist. Aber: Ganz so einfach ist es leider nicht ...

DER ›BLAUE ENGEL‹ feiert in diesem Jahr seinen 25. Geburtstag und hat, bei aller berechtigten Kritik, im Laufe der Jahre doch einen hohen Bekanntheitsgrad erreicht. Aber ist seine Vergabe für ein Produkt immer gerecht? Hilft der Aufdruck auf dem Produkt dem Verbraucher wirklich in jedem Einzelfall umweltfreundlich einzukaufen, ja, sich umweltfreundlich zu verhalten? Insbesondere Letzteres sicher nicht: Zwar ist der (relativ) schadstoffarme, wasserlösliche Lack weniger gesundheitsschädlich als die lösungsmittelbasierten Alternativen, aber absolute Aussagen zur Umweltfreundlichkeit würden spätestens dann ad absurdum geführt, wenn der Heimwerker die Lackreste in die Kanalisation spült oder Kleinkinder den Lack als Fingerfarbe verwenden.

Obwohl in kritischen Diskussionen zu Qualitätssiegeln häufig das ›Ganz-oder-gar-nicht‹-Argument zu hören ist (wenn schon ein Siegel vergeben wird, dann muss es unter allen Umständen, umfassend und immer gelten – alles andere sei Augenwischerei), haben wir uns doch inzwischen daran gewöhnt, dass die Aussagen etwa zur Umweltfreundlichkeit des ›Blauen Engels‹ an gewisse Voraus-

setzungen und Beschränkungen geknüpft sind. ›Umweltfreundlich – weil lösemittelfrei‹, heißt eben nicht, dass dieser Lack selbst bei unsachgemäßer Anwendung keine Schäden verursacht.

Inwieweit man dem Verbraucher also trotz offiziellem Siegel verantwortungsvolles Handeln und eigenes Abwägen abverlangen kann (und muss) ist eine fast philosophische Fragestellung, deren Erörterung an dieser Stelle sicherlich zu weit führen würde ...

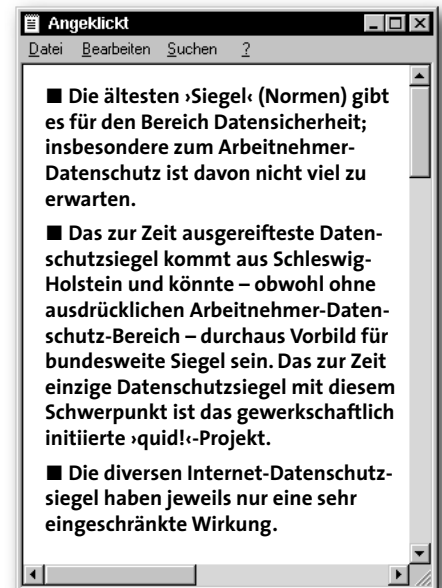
Was leisten Datenschutzsiegel?

BLEIBT DIE FRAGE, welche Leistung ein Siegel denn sinnvollerweise erbringen und welchen Nutzen ein interessierter Anwender daraus ziehen kann. Sicher ist jedenfalls, dass es kaum jemals ausreichen kann, allein mit dem Blick auf irgendwelche ›Aufkleber‹ Produkte zu kaufen ohne zu wissen, was genau der Aufkleber denn bescheinigt. Diesen Rest Eigenverantwortung kann einem kein Siegel abnehmen und ohne die Kenntnis der Rahmenbedingungen (hier wird nur die Lösemittelfreiheit geprüft, nicht aber die Frage der umweltschonenden Entsorgung) lässt sich kein wirklicher Nutzen aus dem Siegel ziehen.

In diesem Sinne können Siegel immer nur dort Unterstützung bieten, wo sie nicht etwa gedankenlos als Freibrief missinterpretiert werden.

Warum diese lange Vorrede, obwohl es doch eigentlich ums Thema Datenschutz gehen soll?

Erfahrung mit dem ›Blauen Engel‹, seinen Vorzügen und Nachteilen hat in den letzten 25 Jahren fast jeder Verbraucher im Alltag gemacht. Datenschutzsiegel hingegen sind für viele noch ein ›Buch mit sieben Siegeln‹ und können häufig nicht so recht eingeordnet werden. Vermeintlicher Nutzen und befürchteter Schaden werden teilweise sehr kontrovers diskutiert und dabei



sowohl übertriebene Hoffnungen als auch unbegründete Befürchtungen geäußert. Da hilft die Analogie zum ›Blauen Engel‹, wenn es jetzt darum gehen soll, die Chancen von Datenschutzsiegeln abzuschätzen.

Zunächst aber: Welche Arten von Datenschutzsiegeln gibt es inzwischen überhaupt ›auf dem Markt‹, wie unterscheiden sie sich und welche Aspekte beurteilen sie jeweils? Dabei soll im Folgenden der Begriff ›Siegel‹ nicht allzu eng verstanden werden. Es wird ebenfalls die Rede von allgemein gebräuchlichen Normen sein, deren Umsetzung man sich – so man denn möchte – zertifizieren (bescheinigen) lassen kann.

Siegel mit Schwerpunkt IT-Sicherheit

HISTORISCH BETRACHTET sind die ersten ›abgeschlossenen‹ Normen zum Datenschutz im Bereich der IT-Sicherheit zu finden. In einigen dieser Regelwerke werden dem Datenschutz als einer eng mit der IT-Sicherheit verflochtenen Materie eigene Kapitel gewidmet. Als Beispiel können diesbezüglich sowohl die ISO-Norm 17799¹ als auch das Grundschutzhandbuch (GSHB) des Bundesamts für die Sicherheit in der Informationstechnik (BSI)² gelten. Das BSI bemerkt zu dieser Verflechtung in seiner aktuellen GSHB-Ausgabe: »Aufgrund der engen Verflechtungen von Datenschutz und IT-Sicherheit sollte es Ziel eines IT-Grundschutzkapitels zum Thema ›Datenschutz‹ sein, einerseits die Rahmenbedingungen für den Datenschutz praxisgerecht aufzuarbeiten und andererseits die Verbindung zur IT-Sicherheit über den IT-Grundschutz aufzubauen.«

GSHB

Das Grundschutzhandbuch stellt eine inzwischen anerkannte Methode zur Erzielung eines geordneten und sicheren EDV-Betriebs dar. Es handelt sich dabei um die systematische, vollständige und zyklisch wiederkehrende Untersuchung von Sicherheitsgefährdungen mit Hilfe einer umfassenden, strukturierten Auflistung, aus der sich, je nach untersuchtem System, nahezu ›automatisch‹ die zu ergreifenden Schutzmaßnahmen ergeben. Unternehmen und Behörden, die ihre EDV unter Einsatz des Grundschutzhandbuchs absichern, können sich den Erfolg ihrer Bemühungen inzwischen durch vom BSI lizenzierte Gutachter (IT-Grundschutz-Auditoren) zertifizieren lassen. Dabei wird nach einer Überprüfung ein Revisionsbericht erstellt, der dem BSI als Grundlage für die Vergabe des IT-Grundschutz-Zertifi-

1... www.iso-17799.com

2... www.bsi.de

3... <http://www.bsi.de/gshb/deutsch/b/35.htm>

kats dient. Das Zertifikat selber ist zunächst für die Dauer von zwei Jahren gültig.

Das geplante Kapitel ›Datenschutz‹ im GSHB wurde vom Bundesbeauftragten für den Datenschutz vorgeschlagen und – laut Veröffentlichung auf der Website des BSI³ – noch nicht in das GSHB übernommen. Eine Einbindung ist jedoch wahrscheinlich. Die Verweise auf



den Vorschlag erscheinen bereits in der Online-Version des GSHB.

Dabei wird darauf hingewiesen, dass insgesamt die der IT-Sicherheit dienenden Maßnahmen des GSHB gleichermaßen dem Datenschutz zugute kommen. Zusätzlich werden einige über Sicherheitsgefährdungen hinaus gehende Datenschutz-Gefährdungen (jeweils mit vorgeschlagenen Maßnahmen) aufgeführt. Dabei handelt es sich um ...

- fehlende oder nicht ausreichende Rechtsgrundlage,
- Nichteinhaltung der Zweckbindung,
- Überschreitung des Erforderlichkeitsgrundsatzes,
- Verletzung des Datengeheimnisses,
- Gefährdung der Rechte Betroffener,
- fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen,
- Gefährdung der vorgegebenen Kontrollziele,

- fehlende oder unzureichende Datenschutzkontrolle.

Die je nach Einzelfall zutreffenden Gefährdungen sollen dann zu so unterschiedlichen Maßnahmen wie der Regelung der Verantwortlichkeiten, der Verpflichtung und Unterrichtung der Beschäftigten, der datenschutzgerechten Protokollierung oder der Regelung der Auftragsdatenverarbeitung führen – um nur einige zu nennen.

Leider ist der Textentwurf zum Datenschutz noch recht dünn in Bezug auf die Ausgestaltung der Maßnahmen-Vorschläge. Insbesondere findet der Betriebsrat keine Erwähnung, obwohl dies zum Beispiel bei Zulässigkeits- und Mitbestimmungs-Fragen durchaus sinnvoll wäre. Da der Vorschlag auch insgesamt noch den Eindruck einer ›Vorversion‹ macht, bleibt zu hoffen, dass die Formulierungen noch konkretisiert und dann auch die Arbeitnehmervertretungen als Akteure wahrgenommen werden.

ISO 17799/BS7799

Etwas anders – jedoch nicht vollständig unterschiedlich – wird die ISO-Norm 17799 eingesetzt, bei der es sich um einen international anerkannten Standard zur Errichtung eines Sicherheits-Managements im Unternehmen handelt. Sie ist aus der britischen Norm BS7799 entstanden, weshalb beide Normen häufig gleichbedeutend nebeneinander stehen. Ziel der Umsetzung ist in erster Linie die Etablierung eines möglichst umfassenden Risiko- und Qualitäts-Managements. So soll durch ein System von Analysen, Verfahren und ständiger Verbesserung ein hoher Schutz erreicht werden.

ISO 17799 gibt jedoch, im Gegensatz zum GSHB, keine konkreten Hilfen zur Durchführung von Gefährdungsanalysen oder zur Umsetzung von Maßnahmen. Sie formuliert im Wesentlichen übergeordnete Ziele und überlässt die Detaillierung dem jeweiligen Anwender. Aber auch die Einhaltung dieser Norm



können sich interessierte Unternehmen formal bescheinigen lassen. Die Zertifizierung nach dem Standard BS7799 erfolgt für einen beschränkten Zeitraum von in der Regel drei Jahren.

Innerhalb der in zehn Steuerungs-bereiche gegliederten Norm finden sich kaum Teile, die nicht auch mitbestimmungspflichtige Aspekte berühren würden. Jedoch beschäftigt sich keines ausdrücklich mit Anforderungen in Bezug auf Sicherheit oder Datenschutz von Beschäftigendaten. Einen Brückenschlag zum Thema Datenschutz, vergleichbar dem im GSHB begonnenen, findet man in der ISO-Norm nicht. Dennoch werden wegen der Verschränkungen zwischen Datenschutz und IT-Sicherheit viele Fragen thematisiert, die auch die Überschrift ›Datenschutz‹ tragen könnten. Besonders die Steuerungs-bereiche ›personnel security‹ (Personal/Belegschafts-Sicherheit), ›security organisation‹ (Sicherheitsorganisation) und ›security policy‹ (Sicherheits-Richtlinien) beinhalten Anforderungen nach etablierten Verfahrensregelungen, zum Beispiel zur geregelten Schulung von Beschäftigten, zu Sicherheitsanforderungen, zur Entwicklung einer unternehmensweiten Sicherheits-Richtlinie oder zur Einschaltung externen Sachverständigen.

Insgesamt bietet die ISO-Norm jedoch lediglich eine Hilfe bei der grundlegenden Organisation des Themas Sicherheit im Unternehmen. Sie bietet keinerlei Spezifikationen oder Vorschläge für Maßnahmen an, so dass sie ein aus Betriebsrats-sicht recht mühsam einzusetzendes Werkzeug darstellt.

Siegel mit Schwerpunkt Datenschutz

SEIT EINIGEN JAHREN gibt es unterschiedliche Bestrebungen, den Datenschutz zum Hauptthema von Normen zu machen (und nicht nur als Nebenbedingung der IT-Sicherheit ›abzuhandeln‹) und für deren Einhaltung ebenfalls Zertifikate oder Siegel zu vergeben.

Im deutschen Einflussbereich gehören zu dieser Gruppe im wesentlichen die vom Unabhängigen Landeszentrum für den Datenschutz in Schleswig-Holstein (ULD) vergebenen Zertifikate und das Datenschutzsiegel ›quid!‹:

- Das ULD ist die Behörde des schleswig-holsteinischen Landesbeauftragten für den Datenschutz⁴ und vergibt das Datenschutz-Gütesiegel für IT-Produkte (Hardware, Software und Datenverarbeitungsverfahren) und ein Siegel für Behörden-Audits (Überprüfung von Behörden).
- ›quid!‹ (›Qualität im Datenschutz‹) ist entstanden aus einem von der Fachhochschule Frankfurt am Main und der Deutschen Postgewerkschaft (heute: ver.di) durchgeführten Projekt zur Entwicklung eines Datenschutz-Gütesiegels in privaten Unternehmen. Inzwischen wird dieses von der gleichnamig gegründeten GmbH vermarktet.

ULD: Datenschutz-Gütesiegel Hardware/Software

Beim Datenschutz-Gütesiegel des ULD handelt es sich um eine durch das schleswig-holsteinische Landesdatenschutzgesetz in Verbindung mit der Datenschutzauditverordnung (DSAVO) definierte Qualitätsaussage.

Obwohl in erster Linie für öffentliche Einrichtungen konzipiert, lässt sich beobachten, dass das Gütesiegel zunehmend auch im privatwirtschaftlichen Bereich auf Interesse stößt. Der ursprüngliche Zweck der Vergabe liegt in der Qualitätssicherung für Ämter und Behörden: Im Landesdatenschutzgesetz wird diesen Stellen auferlegt, vorrangig Produkte einzusetzen, die das Gütesiegel vorweisen können.

Die Vergabe des Siegels erfolgt durch das ULD auf Grund eines Prüfberichts, der durch akkreditierte Sachverständige auf Antrag des Herstellers angefertigt wird. Zusätzliche Prüfungen durch das ULD selber vor Erteilung des Siegels sind möglich. Die Gültigkeitsdauer ist in der Regel auf zwei Jahre befristet.

Das ULD weist darauf hin, dass die zu prüfenden Kriterien und die damit ver-

bundenen Vorgaben im Laufe der Praxiserprobung noch verändert werden können, so dass zur Zeit voraussichtlich einmal im Jahr mit Anpassungen zu rechnen ist, was auch in der Benennung des Siegels (Gütesiegel 2002, Gütesiegel 2003 usw.) deutlich wird – Zitat:

»Da das Gütesiegel auf eine Verbesserung des Datenschutzes und der Datensicherheit abzielt, aber nicht mit unrealistisch hohen Vorgaben beginnen will, werden sich die Anforderungen über die Zeit entwickeln und in Abhängigkeit des Stands der Technik fortgeschrieben werden.«⁵

Das ULD bietet von allen Zertifizierungsstellen einen der umfangreichsten, wenn nicht gar den umfangreichsten Internet-Auftritt zu seinen Zertifikaten an – und schafft damit eine große Transparenz für diejenigen, die das Vorliegen des Datenschutz-Siegels schließlich honorieren sollen. Und es ist nun einmal – genau wie beim eingangs erwähnten ›Blauen Engel‹ – recht wichtig für den einzelnen Verbraucher, Kunden oder auch Arbeitnehmer, abschätzen zu können, was denn nun tatsächlich geprüft wurde und zur Erteilung des Siegels geführt hat.

In der Produktprüfung wird grundsätzlich zwischen der Betrachtung aus rechtlicher und aus technischer Sicht unterschieden. Dies äußert sich beispielsweise auch in der Anerkennung von Gutachtern, die nicht automatisch für beide Bereiche zugelassen werden, sondern ihre Zuverlässigkeit, Unabhängigkeit und Fachkunde für jeden der beiden Bereiche separat nachweisen müssen. Es gibt daher durchaus Gutachter nur für den rechtlichen oder nur für den technischen Bereich, so dass Gutachten in der Konsequenz oft von mehreren Gutachtern gemeinsam erstellt werden.

Als Hauptprüfungskriterien dienen bei der Untersuchung des jeweiligen Produkts die Datenvermeidung, die

4... www.datenschutz-zentrum.de

5... ULD – das schleswig-holsteinische Datenschutz-Gütesiegel, Hintergrundinformationen, Version 1.0

Datensparsamkeit, die Datensicherheit und die Revisionsfähigkeit (also die Nachvollziehbarkeit aller sicherheitsbedeutsamen Aktionen z. B. anhand von Protokoll-Dateien) der Datenverarbeitung sowie die Gewährleistung der Rechte der Betroffenen. Orientiert an diesen grundlegenden Zielen stellt das ULD detaillierte Anforderungs- und Maßnahmenkataloge zur Verfügung, die den Gutachtern einen Rahmen für ihre Untersuchung bieten.

Obwohl der Anforderungskatalog nicht ausdrücklich den Datenschutz von Arbeitnehmern erwähnt, werden im Ergebnis auch die Rechte der Arbeitnehmer im Hinblick auf den Datenschutz untersucht und bewertet:

- Könnte das gleiche Verarbeitungsergebnis mit geringerer Erhebung und Verarbeitung personenbezogener Daten erzielt werden?
- Sind die zur Verfügung stehenden Auswertungen und Verarbeitungskombinationen wirklich alle notwendig?
- Wird die Möglichkeit frühzeitiger Pseudonymisierung (Nutzung von Tarnnamen) genutzt?
- Ist die Transparenz der Datenverarbeitung für die Betroffenen gewährleistet?

All dies sind Fragen, die einem Betriebsrat zum Beispiel bei Einführung einer Projekt-Management-Software oder Skill-Datenbank (um nur wahllos zwei Beispiele heraus zu greifen) auf der Seele liegen, wenn er an den Datenschutz für die Beschäftigten denkt.

Und obwohl der Arbeitnehmer-Datenschutz beim Datenschutz-Gütesiegel nicht als »eigenes« Thema behandelt wird, ist der allgemein zugängliche Kriterien- und Anforderungskatalog (auch zum Arbeitnehmer-Datenschutz) detaillierter und klarer aufgebaut als der des gleich noch zu beschreibenden Datenschutz-Siegels »quid!«.

ULD: Behörden-Audit

Beim Behörden-Audit des ULD handelt es sich um die Zertifizierung der datenschutzgerechten Gestaltung von

Datenverarbeitungsverfahren oder -prozessen öffentlicher Stellen in Schleswig-Holstein. Das Audit stützt sich ebenfalls auf die schleswig-holsteinische Gesetzgebung, stößt aber auch außerhalb des Bundeslands auf großes Interesse.

Dies liegt nicht zuletzt daran, dass Schleswig-Holstein als erstes Bundesland eine Durchführungsverordnung zum Datenschutz-Audit umgesetzt hat und damit als Vorreiter und Modell für das im Bundesdatenschutzgesetz (BDSG) ja ebenfalls vorgesehene Audit privater Unternehmen fungiert. Je länger der Bundesgesetzgeber keine Ausführungsbestimmung zu diesem im BDSG vorgesehenen Instrument vorlegt, desto wahrscheinlicher wird es, dass sich eine solche Bestimmung an einem funktionierenden und erprobten Modell orientiert – in diesem Fall dem schleswig-holsteinischen.

Es läge deshalb nicht ganz fern, sich dieses Modell auch dann anzuschauen, wenn man nicht gerade Personalrat einer schleswig-holsteinischen Behörde ist ...

Vor der Erteilung dieses Zertifikats wird hauptsächlich das Datenschutzkonzept der beantragenden Behörde insgesamt oder bezüglich einzelner Verfahren durch das ULD selbst geprüft. Auditiert wird dann jeweils natürlich nur der untersuchte Gegenstand.

Beispielsweise hat der Kreis Ostholstein die Anbindung seines internen Netzes an das Internet auditieren lassen und die Gemeinde Büchen die gesamte Verarbeitung personenbezogener Daten in der Gemeindeverwaltung sowie im Rahmen des Projekts »Virtuelles Rathaus«.

Eine Reihe weiterer Auditierungen sind abgeschlossen, in Arbeit oder in der Anbahnungsphase. Das Interesse an diesem Verfahren weckt nach Aussagen des ULD reges Interesse...⁶.

Datenschutz-Siegel »quid!«

»quid!« vergibt ein Datenschutz-Siegel, mit dessen Hilfe die Beurteilung verschiedener Bereiche des betrieblichen Datenschutzes ermöglicht werden soll. Der für die Prüfung vorgesehene Ablauf ordnet diese zu betrachtenden Bereiche in einer Hierarchie an, innerhalb derer die Anforderungen an jeden

Bereich in so genannten Qualitätsmodellen beschrieben werden. Von der »quid! GmbH«⁷ zertifizierte Prüfer untersuchen anhand dieser Modelle die im Einzelfall ausgewählten Bereiche und erstellen einen Prüfbericht. Zugelassene Zertifizierungsstellen (wozu z.B. die TÜV Informationstechnik GmbH...⁸ gehört) entscheiden dann auf dieser Grundlage über die Vergabe des zunächst auf zwei Jahre befristeten Siegels.

Die verschiedenen Bereiche (also Schwerpunkte, unter denen die Datenschutzerfordernisse geprüft werden können) sind:

- **Produkte ...** Ist ein bestimmtes Produkt datenschutzgerecht einsetzbar?
- **Arbeitsplätze ...** Ist die Gestaltung aller Arbeitsplätze datenschutzgerecht?

6... **Erfahrungsbericht über die praktische Anwendung der Instrumente Datenschutz-Audit und IT-Gütesiegel in Schleswig-Holstein, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Dezember 2002**

7... www.quid.de

8... www.tuevit.de



- **Betrieb ...** Werden alle Anforderungen an den betrieblichen Datenschutz eingehalten?
- **Funktionsbedingungen Datenschutz/Datenschutzbeauftragte ...** Sind die Anforderungen der §§ 4 f und 4 g Bundesdatenschutzgesetz angemessen umgesetzt?
- **Prozesse ...** Ist ein bestimmter Prozess datenschutzgerecht gestaltet?

Das Qualitätsmodell eines jeden Bereichs besteht wiederum aus ›Gütemerkmalen‹, denen ihrerseits so genannte ›Faktoren‹ zugeordnet sind. Dadurch entsteht eine vordergründig klar erscheinende Hierarchisierung. Allerdings gibt es auf der Faktorenebene vielfältige Überschneidungen und Abhängigkeiten.

Die gleichzeitige Beurteilung verschiedener Bereiche erfordert daher ein Aussortieren redundanter (wiederholt auftauchender) Faktoren. Obwohl man bei genauer Analyse der Qualitätsmodelle außerdem feststellt, dass die Ebenen der Gütemerkmale und der Faktoren manchmal durcheinander geraten und nicht immer einheitlich gestaltet sind, enthalten die verwendeten Modelle im Grundsatz doch die für den jeweiligen Bereich wichtigen Anforderungen.

Bei der Handhabung der Zertifizierung muss vermutlich noch einige Erfahrung gesammelt werden – das zeigt etwa die Vergabe des erste Zertifikats an ›Coca Cola und ihre 100-prozentigen Schwesterunternehmen‹ im Bereich ›Funktionsbedingungen Datenschutz‹: Dort ist im Gütemerkmal ›Mitarbeiter- und Kundenorientierung‹ auch der Faktor ›Erreichbarkeit der Ansprechpartner zu Datenschutzfragen‹ zertifiziert worden. Zumindest die Website von Coca Cola ist jedoch unter Datenschutzgesichtspunkten nicht gerade das, was man als Internet-Benutzer vorbildlich nennen würde:

Weder gibt es einen jederzeit abrufbaren Link zu einer Datenschutz-Richtlinie noch ist der Datenschutzbeauftragte dort überhaupt erwähnt – auch eine Ansprechadresse steht nicht zur Verfügung⁹. Will man den Namen des

Datenschutzbeauftragten erfahren, so schafft man das eher in einer mit Hilfe der Suchmaschine ›Google‹ gefundenen Pressemeldung des Konzerns¹⁰ als an der Stelle, wo er auf jeden Fall hingehören würde.

Dennoch: ›quid!‹ ist das einzige Siegel, das sich ausdrücklich und schwerpunktmäßig die Entwicklung des Arbeitnehmer-Datenschutzes in den Betrieben zum Ziel gesetzt hat.

Siegel mit Schwerpunkt Web-Angebote (Online-Siegel)

UND DANN GIBT ES noch eine ganze Menge auch internationaler Datenschutzsiegel, die sich in erster Linie an die Benutzer von Internet-Seiten richten. Hier besteht ganz offensichtlich aus Anbietersicht der größte Bedarf, potenziellen Kunden durch den Erwerb eines Datenschutz-Siegels zu demonstrieren, wie verantwortungsbewusst man mit ihren Daten umgeht – um sich so positiv von den Mitbewerbern abzuheben und den Umsatz anzukurbeln.

Genau dort scheint auch die Parole ›Privacy sells‹¹¹⁺¹² vorrangig zu wirken. Diese Kurzform für die Erkenntnis, dass sich Datenschutz als Wettbewerbsfaktor gewinnbringend einsetzen lässt, hat fast unmittelbar zum Wunsch geführt, die Einhaltung datenschutzrechtlicher Normen ›vorzeigbar‹, ja, ›beweisbar‹ zu machen.

Dennoch sollte man sich wohl keinen Illusionen hingeben: Datenschutz wird im Bereich des E-Commerce (Geschäftsabwicklung übers Internet – siehe dazu cf 7-8/02) von den Unternehmen durchaus nicht immer aus Überzeugung in der Sache befördert. Zwar haben die Verbraucher durch die ›Abstimmung über den Geldbeutel‹ eine nicht zu unterschätzende Marktmacht, vorerst aber führt dies zu dem Ergebnis, dass diese Art von Siegeln nur die Bereiche abdecken, in denen ein unmittelbarer finanzieller Nutzen (im Wesentlichen: steigender Umsatz) durch die Erteilung des Siegels wahrscheinlich ist. Die sehr große Zahl derartiger Siegel lässt erahnen, dass die Hoffnung auf geldwerte Vorteile entsprechend groß ist.

Dass die inzwischen entstandene Siegel-Vielfalt für den Online-Verbraucher wirklich noch sinnvoll nutzbar ist, darf deshalb bezweifelt werden. Dies wird besonders deutlich, wenn sich Online-Shops aus durchaus nachvollziehbaren Gründen möglichst viele der auf dem Markt vorhandenen Siegel ›sichern‹ wollen. Ohne ein inhaltliches Urteil abgeben zu wollen, drängt sich beim Betrachten mancher mit Siegeln geradeteu tapezierten Internet-Seite der Eindruck auf, dass hier nach dem Motto ›Viel hilft viel!‹ vorgegangen wurde. Ein Beispiel dafür ist die Website des Online-Shops ›www.computeruniverse.net‹, der stolz seine sechs (!) unterschiedlichen Siegel präsentiert, diese jedoch offensichtlich erhalten hat, ohne einige eigentlich selbstverständliche Datenschutz-Anforderungen zu erfüllen.

So wird zum Beispiel in der Datenschutzerklärung dem Kunden nicht konkret angegeben, welche Daten denn nun genau über ihn gespeichert werden (Verbindungsdaten und die für die Benutzung der Seiten zwingend erforderlichen ›Cookies‹ werden überhaupt nicht erwähnt). Außerdem hat der Kunde keine Möglichkeit, direkt bei der Bestellung der Nutzung seiner Daten für Werbezwecke zu widersprechen und der Datenschutzbeauftragte wird weder mit eigener E-Mail noch mit einer Postadresse genannt.

Beispiele für Online-Siegel

ZUNÄCHST: KEINES DER im Bereich E-Commerce vergebenen Siegel ist als reines

9... So z. B. www.cceag.de, www.coca-cola.de, www.coca-cola-gmbh.de

10... www.cceag.de/presse/pressemeldungen/pressemeldung.jsp?content_id=386

11... hierzu auch Weichert: www.datenschutzzentrum.de/material/themen/divers/verbrsch.htm

12 hierzu auch Bäumler, Mutius: Datenschutz als Wettbewerbsvorteil – Privacy sells: Mit modernen Datenschutzkomponenten Erfolg beim Kunden; Vieweg, 2002

Datenschutz-Siegel zu betrachten. Allgemein übliche Einschränkungen werden bei einer kurzen, beispielhaften Betrachtung der folgenden Siegel deutlich:

Das Privacy Seal des amerikanischen Vereins TRUSTe...¹³

Dabei handelt es sich um eine nicht-kommerzielle Initiative, die auf Anregung unter anderem der Electronic Frontier Foundation (EFF)...¹⁴ entstanden ist. Die EFF ist eine gemeinnützige Bürgerrechts-Organisation, die sich den Schutz der Privatsphäre im Internet auf ihre Fahnen geschrieben hat. Das Siegel soll Verbrauchern anzeigen, dass der Anbieter in seinem WWW-Angebot dem Nutzer im Rahmen einer Datenschutz-Richtlinie (Privacy Policy) Informationen über Speicherung, Verwendung und Schutz personenbezogener Daten gibt und dabei auch eventuell zur Verfügung stehende Alternativen (in Bezug auf Formen der Datenerhebung) herausstellt. Online-Verbraucher sollen so größtmögliche Kontrolle über die Verwendung ihrer personenbezogenen Daten erhalten. Zertifiziert wird allerdings im Wesentlichen nur die Übereinstimmung der Datenverarbeitung mit der vom Unternehmen selbst gestalteten Datenschutz-Richtlinie.

Das WebTrust Seal...¹⁵

Dies ist ein von kanadischen und amerikanischen Wirtschaftsprüfern ins Leben gerufenes Zertifikat zur Beurteilung von Online-Shops. Die Prüfungsstandards orientieren sich an den traditionell hohen Standards von Wirtschaftsprüfern und befassen sich in erster Linie mit Kriterien der Sicherheit und Ordnungsgemäßheit. Das Prüfmodul ›Da-

tenschutz‹ hat die Rechte der Online-Verbraucher im Blick. In Deutschland will die IDW Net GmbH...¹⁶ für die Verbreitung und Vermarktung sorgen. Zertifiziert wird in Deutschland durch von IDW Net GmbH akkreditierte Wirtschaftsprüfungsgesellschaften.

Das IPS (Internet Privacy Standards)

Dieses Datenschutz-Zertifikat für Online-Dienste kommt von der datenschutz-nord GmbH...¹⁷, und wurde erst im Dezember 2002 etabliert. Die datenschutz-nord GmbH selber ist akkreditierter Gutachter für das Datenschutz-Gütesiegel des ULD. Mit ihrem eigenen Siegel will sich das Unternehmen jedoch insbesondere auf die Beurteilung von WWW-Angeboten spezialisieren.

Trusted Shops GmbH...¹⁸

Dieses Unternehmen beurteilt insbesondere Online-Shops unter den Aspekten Datenschutz, Preistransparenz und verbrauchergerechte Gestaltung des Angebots. Das Ziel des Siegels ist nach eigenen Aussagen die Erreichung eines möglichst weltweiten Standards. Verstößt ein zertifizierter Online-Shop gegen die Vertragsregeln, so fallen Konventionalstrafen an. Allerdings sind die zum Bereich Datenschutz abverlangten Standards wenig mehr als das gesetzlich ohnehin Vorgeschriebene.

Für Interessierte bietet www.online-profiling.de einen recht guten Überblick über die im Bereich E-Commerce zu vergebenden Siegel.

Nur Transparenz führt zu Akzeptanz

DIE HIER IM ÜBERBLICK vorgestellten Siegel, Zertifikate und Normen stellen nur einen kleinen Ausschnitt aus der ungeheuren Menge auf dem Markt befindlicher Angebote dar. Die Auswahl für diesen Artikel erfolgte unter den Aspekten:

- **Relevanz ...** Ist das Siegel/die Norm sinnvoll nutzbar um den Datenschutzstandard im Unternehmen anzuheben?
- **Verbreitungsgrad ...** Hat das Siegel/die Norm in Deutschland einen gewissen

Verbreitungsgrad oder lässt sich eine zunehmende Verbreitung erwarten?

- **Nutzen ...** Lässt sich das Siegel/die Norm in der Betriebsratsarbeit sinnvoll einsetzen oder ergänzt es Bemühungen um Verbesserung des Arbeitnehmer-Datenschutzes?
- **Vollständigkeit ...** Trifft das Siegel/die Norm Aussagen, die den Datenschutz eines gewissen Gebietes (Verfahren, Prozess o.ä.) möglichst vollständig bewerten?

Schaut man sich weiter auf dem Markt um und betrachtet europäische oder gar internationale Angebote ebenfalls, so wird deutlich, dass bei der riesigen Menge an Zertifikaten und Siegeln auf Dauer eine Konzentration nötig sein wird. Um potenziellen Nutznießern von Siegeln die Chance auf Überblick und Vergleichbarkeit zu lassen, darf die Vielfalt nicht zur Unübersichtlichkeit verkommen. Wenn das Verstehen von Siegeln und deren Unterschieden nur nach tagelangem Studium möglich ist, werden Siegel entweder nicht beachtet oder aber – was viel schlimmer ist – doch nur auf den ›Aufkleber‹ reduziert.

Um eine gewisse Überschaubarkeit zu erzielen, hat die Wirtschaftsinitiative D21, ein Zusammenschluss von Wirtschaftsunternehmen, der auf seiner eigenen Website übrigens keinerlei Datenschutz-Erklärung anbietet, einen Anforderungskatalog für Gütesiegel-Anbieter formuliert...¹⁹ um so einen gewissen Mindeststandard zu schaffen.

Ob mit diesem ›Siegel für Siegel‹ nun wirklich der richtige Weg beschritten wird oder ob sich hier eine Überreglementierung andeutet, die Verbraucher und sonstige von Datenverarbeitung Betroffene noch mehr abschreckt, kann unterschiedlich gesehen werden.

Sicher ist jedoch, dass gerade bei der jetzigen Vielfalt, ohne umfassende und vollständige Informationen zu den verschiedenen Angeboten die Akzeptanz von Siegeln ganz allgemein nicht das gewünschte Maß erreichen wird. Gerade für den Bereich des Arbeitnehmer-Datenschutzes wäre es verdienstvoll, die Unterschiede, Wirkungsweisen, Stärken,

13... www.truste.org

14... www.eff.org

15... www.cpawebtrust.org

16... www.idwnet.de

17... www.datenschutz-nord.de/

18... www.trustedshops.de/de/home

19... www.initiated21.de/home.php3?nav=projekte/guetesiegel&teaser=projekte&text=projekte/guetesiegel/guetesiegel.html



Schwächen und Aussagekraft der verschiedenen Angebote vergleichend nebeneinander zu stellen, so dass auch Betriebsräte sich an einer zentralen Stelle einen Überblick verschaffen können.

Wer kann eine solche Arbeit leisten? Möglicherweise könnte der Grundstock im Rahmen einer Diplomarbeit oder Semesterarbeit gelegt werden, die Fortschreibung dann durch Betreiber von Portalen zum Datenschutz fortgeführt werden. Denkbare Partner wären hier das durch das ULD betreute ›Virtuelle Datenschutzbüro‹ (www.datenschutz.de) oder gewerkschaftliche Internet-Angebote wie zum Beispiel www.online-rechte-fuer-beschaefigte.de (auch hier übrigens bisher weder eine Datenschutz-Erklärung noch ein Impressum! Kollegen!!) oder eine neu zu schaffende gewerkschaftliche ›Schwerpunktseite mit ausreichender Kapazität für eine permanente Pflege.

Fazit

ES GIBT EINEN STEIGENDEN Druck auf Unternehmen, einerseits die eigene EDV vor Gefährdungen zu schützen und sich andererseits durch kundenfreundliches Verhalten positiv von Mitbewerbern abzuheben. Die Erkenntnis der Arbeitgeberseite, dass Datenschutz als Wettbewerbsfaktor zu begreifen ist und die betriebsrätlichen Bemühungen um eine Verbesserung des Arbeitnehmer-Datenschutzes sollten zu einer gemeinschaftlich geplanten Vorgehensweise führen, die die Anhebung des Datenschutz-Niveaus insgesamt zum Ziel hat.

Dazu kann ein systematischer Prozess angestoßen werden, an dessen Ende die Erteilung eines Siegels stehen kann, zumindest aber das wohlgeordnete Vorgehen und die geregelte Einbeziehung betrieblicher Akteure erreicht wird. In diesem Zusammenhang kann die Einbeziehung des Betriebsrats genauso festgelegt werden wie die Beteiligung des betrieblichen Datenschutzbeauftragten, der Arbeitssicherheits-Fachkraft und anderer.

Als Arbeitsmittel für den Betriebsrat sind dabei die vielen Gütesiegel aus dem Bereich des E-Commerce nur sehr bedingt hilfreich, da sie in der Regel keinerlei Aspekte des innerbetrieblichen Datenschutzes betrachten. Andere Normen, wie zum Beispiel ›quid!‹ oder das schleswig-holsteinische Gütesiegel versprechen mehr Gewinn für den innerbetrieblichen Datenschutz.

Aber für welche Norm, welches Zertifikat oder welches Verfahren man sich letztlich auch entscheidet: Bei der Durchführung derartiger Projekte im eigenen Haus sind Unternehmen und Arbeitnehmervertretung aufeinander angewiesen. Erfolg verspricht ein solches Verfahren nur, wenn beide an einem Strang ziehen und gemeinsam ein für das Unternehmen nützlich Vorgehen entwickeln. In Unternehmen, in denen die Stimmung von gegenseitigem Misstrauen und Abgrenzungsschmerz geprägt ist, kann keines der hier vorgestellten Verfahren zu einem sinnvollen Ergebnis führen.

Der Hauptnutzen für die Arbeitnehmervertretung und die Beschäftigten liegt in der Regel nicht in der Erteilung eines Siegels oder Zertifikats, sondern in der durch den Vorgang angestoßenen Ordnung von Datenschutz- und Datensicherheits-Verfahren und -Abläufen – aber eben auch zur Mitbestimmung, die mit den Datenschutzbelangen der Beschäftigten untrennbar verbunden ist.

Der Betriebsrat kann direkten Nutzen für die Beschäftigten daher nur durch solche Zertifizierungen erwarten, die Fragen der Sicherheit und des Datenschutzes von Beschäftigtendaten zumindest strukturell vorsehen. Derartige Siegel und Normen gibt es, wie dargestellt, nicht viele: die zunächst recht groß scheinende Auswahl beschränkt sich auf das GSHB und ISO17799 (aus dem Sicherheitsbereich kommend) und das Datenschutz-Gütesiegel des ULD und die ›quid!‹-Zertifizierung.

Gleichzeitig muss der Betriebsrat sich bei der Umsetzung und Anwendung der ausgewählten Norm frühzeitig und projektbegleitend einmischen um den Arbeitnehmerdatenschutz zu einem deutlichen Faktor im Umsetzungsprozess zu machen.

Hierfür ist in der Regel die Inanspruchnahme von Sachverständigen durchaus angemessen, wenn man bedenkt, dass auch der Arbeitgeber die Durchführung der anfallenden Analysen, die Etablierung von Verfahren und die Zertifizierung in der Regel nicht allein mit eigenen personellen Ressourcen bewältigen kann.

Denkbar ist natürlich auch die umgekehrte Situation: Der Betriebsrat soll dem Einsatz eines Produkts oder eines Verfahrens zustimmen, das ein Datenschutz-Siegel vorweisen kann. In einem solchen Fall kann die vorliegende Zertifizierung möglicherweise eine Hilfestellung sein.

Hat ein Produkt beispielsweise ein Zertifikat von ›quid!‹ oder das Datenschutz-Gütesiegel des ULD bekommen, so sollte gemäß den offiziellen Prüfkriterien das Produkt auf eine datenschutzgerechte Weise einsetzbar sein. Kein Siegel kann jedoch garantieren, dass dies im Einzelfall (also im eigenen Unternehmen) auch tatsächlich geschieht. Man sollte deshalb auf keinen Fall in den Fehler verfallen, Systeme oder Verfahren einfach ›abzunicken‹, nur weil sie ein Datenschutz-Siegel haben.

Was man mit dieser Reduzierung der Mitbestimmung auf das Abprüfen eines Aufklebers erreicht hätte, entspricht genau der eingangs erwähnten Entsorgung des lösungsmittelfreien Lacks in die Kanalisation: Verantwortung an den Aufkleber abgegeben und dann Murks gebaut. Eine inhaltliche Auseinandersetzung mit den Rahmenbedingungen und Grenzen eventuell vorgelegter Zertifikate (und damit ihrer Aussagekraft) kann kein Siegel dem Betriebsrat abnehmen.

Karin Schuler ist freiberufliche Beraterin für Datenschutz und IT-Sicherheit und Vorstandsmitglied der Deutschen Vereinigung für Datenschutz e.V. Sie berät Betriebs- und Personalräte, betriebliche Datenschutzbeauftragte und IT-Sicherheitsbeauftragte bei der Einführung und Gestaltung von Systemen und der Gestaltung betrieblicher Abläufe; Kontakt: karin@ksc.bn.shuttle.de oder fon 02 28 - 242 0733



aus der praxis datenschutztipps für die praxis

In dieser Serie werden regelmäßig Informationen und Praxisfälle zum Datenschutz veröffentlicht, wie sie in den Berichten der Datenschutzbeauftragten und Aufsichtsbehörden der Länder und des Bundes zu finden sind ...

HAJO KÖPPEN

Krankenkassendaten an den Arbeitgeber!?

KRANKENKASSEN VERARBEITEN besonders sensible Informationen über ihre Mitglieder. Daher sollte man davon ausgehen können, dass sie es mit dem Datenschutz auch besonders genau nehmen. Wer das bisher angenommen haben sollte, wird bei der Lektüre des neuen Berichts des Landesbeauftragten für den Datenschutz in Baden-Württemberg allerdings ins Zweifeln kommen. Die folgend geschilderten Fälle dürften in den Top-100 der Datenschutzverstöße jedenfalls problemlos die ersten Plätze belegen. Und der besondere Pfiff an der Sache: Eine Datenschutzschlamperei wurde erst durch eine weitere Schlamperei aufgedeckt.

Die unglaubliche Geschichte (im Bericht auf Seite 38) geht so:

1

EINE FRAU BEWARB SICH auf eine Stellenausschreibung der Krankenkasse, bei der sie auch versichert ist. Nachdem die Auswahl offenbar jemand anderen gefallen war, erhielt die Betroffene eine schriftliche Absage – und staunte nicht schlecht über die Beilage zu dem Ablehnungsschreiben. Mit dem Vermerk ›Ausdruck für Bewerber‹ versehen lag dem Schreiben ein Ausdruck aus ihrer Leistungsdatei bei. Haarklein waren auf die-

sem Ausdruck alle der Kasse gemeldeten Krankheiten aus den letzten Jahren aufgeführt. Die Bewerberin musste davon ausgehen, dass diese Liste die Auswahlentscheidung beeinflusst hatte ...

Über den Vorfall informiert klärte der Landesdatenschutzbeauftragte die Krankenkasse über die Rechtslage auf: »Rechtlich sieht es so aus, dass die Krankenkasse bei der Verarbeitung der Sozialdaten ihrer Mitglieder nicht frei ist. Vielmehr setzt ihr das ›Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung‹ enge Grenzen. Erlaubt sind nur solche Verarbeitungen, die einem der im Gesetz genau definierten Zwecke dienen (§ 284 SGB V). Die Nutzung von Sozialdaten für Zwecke einer Stellenbewerbung ist dort nicht vorgesehen. Es ist sogar so, dass nach § 35 Abs. 1 SGB I Sozialdaten ausdrücklich vor dem Zugriff durch Personen, die Personalentscheidungen treffen, geheim gehalten werden müssen. Zwar ist dort ausdrücklich nur von Sozialdaten der Beschäftigten des Sozialleistungsträgers die Rede. Nach Sinn und Zweck muss dies aber auch für Personen gelten, die sich um eine Beschäftigung erst bewerben.«

So entsetzt der Datenschutzbeauftragte über den Vorfall war, mit der Reaktion der Krankenkasse zeigt er sich weitgehend zufrieden: »Wie es letztlich dazu kommen konnte, dass der für die Personalangelegenheit zuständige Sachbearbeiter an die

Ausdrucke kam, ließ sich nachträglich (angeblich) nicht mehr aufklären. Jedenfalls reagierte man schnell und ergriff Maßnahmen, um solche Vorkommnisse zukünftig auszuschließen. So wurden die Mitarbeiter auf die Rechtslage aufmerksam gemacht und auf arbeitsrechtliche Konsequenzen bei Missachtung hingewiesen. Zum anderen wurde angeordnet, dass unmittelbar nach Eingang einer Bewerbung zunächst festzustellen ist, ob eine Mitgliedschaft besteht. Ist dies der Fall, muss ein so genanntes ›Mitarbeiterkennzeichen‹ gesetzt werden. Das bedeutet, dass die im System gespeicherten Daten mit einem Merkmal versehen werden, welches es nur noch einzelnen ausgewählten Mitarbeitern erlaubt, auf die Daten zuzugreifen. Es sind dies Mitarbeiter, die ansonsten die Leistungsangelegenheiten der bei der Krankenkasse versicherten eigenen Mitarbeiter bearbeiten. Diese Sperre wird erst dann wieder aufgehoben, wenn das Bewerbungsverfahren abgeschlossen ist.«

2

WELCHE AUSWIRKUNGEN es haben kann, wenn aus Unachtsamkeit Daten ›in die falsche Schublade‹ gelangen, beschreibt der Datenschutzbeauftragte in einem weiteren Fall (Seite 39): »Eine junge Frau wollte zum 1. August eine Lehre beginnen. Sie war bisher über ihre Mutter bei einer Krankenkasse familienversichert und wollte mit Beginn ihrer Ausbildung bei derselben Kasse ein eigenständiges Versicherungsverhältnis begründen. Dies hatte sie bereits vor Beginn der Ausbildung der Krankenkasse gegenüber erklärt. Im Juli wandte sie sich an uns und schilderte, sie sei kurz zuvor in einem Krankenhaus stationär behandelt worden.



© Roger Job

ÄRZTE OHNE GRENZEN
hilft Menschen in Not.
Helfen Sie mit –
durch Ihre Spende
oder als Mitarbeiter/in
in unseren Projekten.



Bitte schicken Sie mir unverbindlich

- allgemeine Informationen über **ÄRZTE OHNE GRENZEN**
- Informationen für einen Projekteinsatz
- Informationen zur Fördermitgliedschaft
- die Broschüre „Ein Vermächtnis für das Leben“

11103603

Name _____

Geb.-Datum _____

Straße _____

PLZ/Ort _____

ÄRZTE OHNE GRENZEN e.V.
Am Köllnischen Park 1 • 10179 Berlin
www.aerzte-ohne-grenzen.de

Spendenkonto 97 0 97
Sparkasse Bonn • BLZ 380 500 00

Unmittelbar nach ihrer Entlassung habe sie einen Telefonanruf ihres späteren Arbeitgebers erhalten. Dieser sei von der Krankenkasse über den Krankenhausaufenthalt informiert worden und habe nun wissen wollen, woran sie erkrankt gewesen sei. Nachdem wir die Krankenkasse gefragt hatten, wie sie dazu komme, künftigen Arbeitgebern ihrer Versicherten Sozialdaten zu übermitteln, klärte sie uns über die Hintergründe auf. Danach sei es üblich, künftige Mitglieder mit einer sog. Interimsanmeldung in das EDV-System aufzunehmen. Dies ermögliche beispielsweise eine frühzeitige Ausstellung der Krankenversichertenkarte. Im konkreten Fall sei es nun so gewesen, dass sowohl die für die Krankenhausaufnahmeanzeige als auch die im Kundencenter zuständigen Mitarbeiter die Vorläufigkeit der Anmeldung übersehen und die Angelegenheit so behandelt hätten, als ob ein versicherungspflichtiges Beschäftigungsverhältnis bereits bestehe. Deshalb sei die Krankenhausaufnahme in eine falsche Datei eingegeben worden, was wiederum dazu geführt habe, dass dem vermeintlichen Arbeitgeber die Aufnahme ins Krankenhaus mitgeteilt worden sei.«

Die Stellungnahme des Datenschutzbeauftragten fiel eindeutig aus: »Es ist schon mehr als ärgerlich, dass der Umstand des Krankenhausaufenthalts hier in die falsche Datei ›gerutscht‹ war und dies niemand bemerkt hatte. Inakzeptabel ist aber, dass die Krankenkasse offensichtlich Krankenhausaufenthalte generell an den Arbeitgeber meldet. Hierfür bedürfte es einer eindeutigen Rechtsgrundlage. Eine solche gibt es indes nicht. Der Hinweis seitens der Krankenkasse auf § 69 Abs. 4 SGB V geht fehl. Die dort geregelte Übermittlungsbefugnis gilt angesichts des Gesetzeswortlauts jedenfalls nicht für erstmalige Erkrankungen. Sinn der Vorschrift ist es vielmehr, dem Arbeitgeber die Möglichkeit zu geben

Arbeitnehmers auf Entgeltfortzahlung im Krankheitsfall ausnahmsweise entfällt. Dabei kommt es vor allem auf die Arbeitsunfähigkeitszeiten im Verhältnis zu früheren, für die Entgeltfortzahlung noch relevanten Arbeitsunfähigkeitszeiten an, die auf einer Fortsetzungserkrankung beruhen. Diese Informationen besitzen aufgrund der Diagnoseangaben in den Arbeitsunfähigkeitsbescheinigungen nur die Krankenkassen. Geht es dagegen nicht um eine Fortsetzungs-, sondern um eine Ersterkrankung, scheidet § 69 Abs. 4 SGB V als Übermittlungstatbestand aus. Vielmehr ist nach dem Entgeltfortzahlungsgesetz allein der Arbeitnehmer verpflichtet, dem Arbeitgeber die Arbeitsunfähigkeit und deren voraussichtliche Dauer unverzüglich mitzuteilen. Die Krankenkassen müssen deshalb solche Meldungen künftig unterlassen.«

Aus jedem Schlechten kann man auch eine positive Lehre ziehen. In den vorliegenden Fällen lautet sie: Es lohnt sich bei Datenschutzverstößen den Datenschutzbeauftragten zu informieren (siehe dazu CF 1/2003, Seite 25). Und: Arbeitgeber bekommen gesagt, wie sie Datenschutzregeln richtig anwenden müssen – und das sogar kostenfrei! Wo gibt es das heutzutage noch?

Landesbeauftragter für den Datenschutz Baden-Württemberg
Marienstraße 12
70176 Stuttgart
fon 0711-615541-0
fax: 0711-212672-50
www.baden-wuerttemberg.datenschutz.de
poststelle@lfd.bwl.de

Hajo Köppen, Assessor jur., Dozent für Datenschutzrecht und Vizepräsident an der Fachhochschule Gießen-Friedberg; Vorstandsmitglied der Deutschen Vereinigung für Datenschutz e. V. (DVD); Kontakt: dana@aktiv.org

Belegschaftsbefragung mit PDF

Umfragen machen Spaß und könnten wertvolle Informationen und Unterstützung für die Arbeit der Interessenvertretung bringen – wenn nur nicht die lästige Auswertung der ausgefüllten Fragebögen wäre!

WENN EINE BEFRAGUNG gut inszeniert ist, kann man als Betriebsrat eines mittelständischen Betriebs schon mal einige hundert Antwortzettel bekommen. Strichlisten zur Auswertung sind ›out‹ – natürlich wird man eine Datenbank verwenden wollen. Aber die will erst einmal mit den Kreuzchen und Texten, die die Beschäftigten geschrieben haben, gefüttert sein. Nun, wie in den bisherigen Folgen unserer Serie über PDF-Dateien heißt es auch in dieser Folge: Mit dem ›Acrobat‹ geht's leichter!

Die Grundlage, um mit dem ›Adobe Acrobat‹ einen Fragebogen zu erstellen, sind Formularfelder, die in PDF-Dateien einzufügen sind und wie das im Prinzip funktioniert, lässt sich ausführlich in Folge 4 (cf 2/03 ab Seite 36) nachlesen. Aber beginnen wir von vorn: Zunächst sollte eine ›Word‹-Datei erstellt werden, die die Fragen enthält. Diese wandelt man dann um in eine PDF-Datei (siehe Folge 1 in cf 10/02 ab Seite 35).

Für jede vorgesehene Antwortmöglichkeit legen Sie ein entsprechendes Formularfeld an. Die erste Frage in dem Beispiel-Fragebogen kann alternativ mit ›Ja‹ oder ›Nein‹ beantwortet werden. Für diesen Fall kann man in PDF-Formularen das ›Optionsfeld‹ benutzen. Erstellen Sie

zuerst das Feld für die ›Ja‹-Antwort und legen Sie fest, dass der ›Exportwert‹ – Sie ahnen was das ist – ›Ja‹ lauten soll.

Kopieren Sie dann dieses Feld (mit [Strg][C]) und platzieren Sie die Kopie (mit [Strg][V]) neben der ›Nein‹-Ant-

wort. Ändern Sie hier den Exportwert in ›Nein‹, belassen Sie aber den Namen des Feldes (z. B. ›Ja-Nein‹ oder ›Frage1‹), denn wenn mehrere Felder denselben Namen tragen, aber unterschiedliche ›Exportwerte‹ besitzen, dann ist nur eine der Alternativen als Antwort möglich.

Entsprechend verfahren Sie mit den Antworten bei der zweiten Frage. Hier sind allerdings vier Alternativen auszuwählen. Definieren Sie dazu ebenfalls ein Formularfeld als ›Optionsfeld‹ und kopieren Sie es dreimal, wobei Sie jeweils einen anderen Exportwert eintragen – beispielsweise die Zahlen von 0 bis 3. In unserem Beispiel ist das Formularfeld transparent gestaltet, so dass es den jeweiligen Antworttext, über den es gelegt ist, sichtbar lässt. Man kann es aber auch anders machen. Jedenfalls: Wenn eine Alternative ausgewählt ist, wird unterhalb des Antworttextes ein kleiner Stern angezeigt.

Für die Textantwort bei ›Sonstiges‹ definieren Sie ein ›Formularfeld‹ als Textfeld und lassen beliebige Eingaben zu. Im Beispiel ist eine kleine Schrift gewählt und eine mehrzeilige Antwort zugelassen, so dass die Beschäftigten



ihm auch technisch unterstützt werden. Hilfestellung dazu bekommt man im Internet unter den unten angegebenen Adressen.

Um die via E-Mail eingegangenen Antwort-Daten nun auszuwerten, gibt es viele unterschiedliche Möglichkeiten, die hier nicht alle ausführlich dargestellt werden können. Die einfachste Variante ist, die FDF-Datei im Adobe Acrobat zu öffnen. Wenn man die Fragebogen-PDF-Datei auf dem eigenen PC gespeichert hat, wird diese dann geöffnet und die Antwortdaten aus der FDF-Datei werden automatisch eingelesen. Damit hat man allerdings nur einen ausgefüllten Fragebogen auf dem Bildschirm, keine übergreifende Auswertung. Sinnvoller ist es deshalb, alle FDF-Dateien in eine Datenbank zu importieren, um sie dort systematisch auswerten zu können. Dazu ist allerdings die Unterstützung durch einen erfahrenen ›Acrobaten‹ hilfreich, denn mit ein paar Programmierkenntnissen lassen sich diese Vorgänge weitgehend automatisieren. Und das Gute daran ist: Wenn das einmal gemacht wurde, lassen sich schnell auch neue Befragungen durchführen.

Karl-Hermann Böker ist freier Journalist und Technologieberater und u. a. spezialisiert auf den PC-Einsatz in Betriebs- und Personalratsbüros; Kontakt: Böker-Beratung, Technologiezentrum, Meisenstr. 96, 33607 Bielefeld, fon 0521-2 99 72 29, fax 0521-2 99 72 28; khb@boeker-beratung.de
www.boeker-beratung.de



Mit dieser Folge wird die Serie über Anwendungsmöglichkeiten der Software ›Adobe Acrobat‹ abgeschlossen. Die vielfältigen Möglichkeiten, die diese Software bietet, sind damit allerdings noch lange nicht vollständig dargestellt. Lediglich die für Arbeitnehmervertretungen interessantesten Anwendungen wurden ausführlich beschrieben. Wer mehr darüber wissen will, wozu das PDF-Format außerdem noch geeignet ist, kann sich im Internet diverse Seiten ansehen oder entsprechende Newsletter abonnieren – hier eine kleine Auswahl der Websites:

www.adobe.de
www.prepress.ch
www.PDFzone.de
www.PDFnews.de

Durch die Textwüsten des Intranet ...

Nein, genau das sollte natürlich vermieden werden!

Es ist inzwischen ja eine Binsenweisheit:

Texte am Bildschirm lesen sich schlechter als auf Papier, sollten deshalb besonders kurz und prägnant sein – eine wichtige Gestaltungsaufgabe.

IN DER LETZTEN CF-Ausgabe haben wir uns mit Bildern und Grafiken als unterstützendem Element zum eigentlichen Informationsträger (in der Regel Text) beschäftigt – und auf die zunehmende Verbreitung von Bildinformationen in den vergangenen Jahren hingewiesen. Allerdings hat auch die Menge verfügbarer Textinformationen in den Jahren des Computer- und Internet-Booms enorm zugenommen. Nie war es einfacher, einen Text zu verfassen und ihn weltweit zu verteilen oder zugänglich zu machen – sei es als E-Mail, als ›Word-Dokument oder gar als ›Book on Demand‹ (= auf Abruf einzeln gedruckte Buchexemplare).

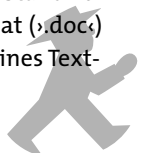
Dabei hat vor allem das Internet dazu beigetragen, dass die Anzahl der öffentlich zur Verfügung stehenden Informationen deutlich in die Höhe geschossen ist – die Summe der im World Wide Web vorhandenen Seiten übersteigt inzwischen unsere Vorstellungskraft – es dürften mehrere Milliarden sein.

Auch in diesem Artikel soll es nun um Text als Träger der verschiedensten Informationsinhalte gehen – allerdings nicht um dessen Gehalt und Qualität, sondern darum, wie Sie als (künftiger) Betreiber einer Intranet/Internet-Website die Fülle textlicher Informationen am besten in Ihre Intranet-Präsentation

integrieren und für den Benutzer aufbereiten.

In einer der ersten Folgen dieser Reihe wurde es bereits erwähnt: Es ist nicht unbedingt vonnöten, dass Sie sämtliche Texte schon fertig haben, ehe Sie Ihre Website veröffentlichen. Eine Intranet- oder Internet-Präsentation lebt durchaus von stetigen Aktualisierungen. Um aber diesen Prozess dauernder Erneuerung so flott und reibungslos wie möglich ablaufen zu lassen, ist es sinnvoll von Beginn an möglichst alle Inhalte gleich in elektronischer Form zu erzeugen und das Abtippen (oder Scannen) von Papiervorlagen tunlichst zu vermeiden. Das gilt übrigens auch für Bilder: Wenn Sie zu den Glücklichen gehören, die Zugriff auf eine Digitalkamera haben, können Sie sich bei der Pflege einer Website viel Arbeit ersparen.

Also: Erfassen Sie die (Text-)Inhalte am besten so, wie Sie es gewohnt sind – vorausgesetzt, es findet am Computer statt. Nutzen Sie dabei das Textverarbeitungsprogramm, mit dem Sie auch sonst am PC arbeiten – selbst in Sachen Dateiformate ist es zunächst nicht notwendig, von Altbewährtem Abstand zu nehmen. Das Word-Dateiformat (›.doc‹) ist ebenso geeignet wie ein reines Text-



format (».txt«) oder das immer beliebter werdende Rich-Text-Format (».rtf«). Auch an die »Gestaltung« des Textes mit verschiedenen Schriftarten und -größen (z. B. für Überschriften) sollten Sie noch keine Energien verschwenden – die eigentliche »Formatierung« erfolgt erst später.

Die von Ihnen erfassten Texte können Sie dann entweder direkt ins WWW-spezifische HTML-Format konvertieren, in entsprechende andere Programme exportieren oder schlicht durch »Kopieren« und »Einfügen« übernehmen.

Im Rahmen dieser Artikelreihe werden wir uns aber natürlich auch noch mit der entsprechenden Software und der Übernahme der Bild- und Textdaten näher auseinandersetzen.

Bessere Lesbarkeit durch klare Struktur

BESONDERS WENN ES um fachliche Inhalte geht, sind ausführlichere Texte oft nicht zu vermeiden. Wichtig ist dabei nur, dass Sie Ihren Text so gegliedert und übersichtlich wie möglich darstellen. Hier können Sie schon weit vor dem endgültigen Aufbau Ihrer Website Gutes tun, besonders bei langen Texten. Versuchen Sie möglichst schon bei der ersten Erstellung der Inhalte den Text durch möglichst viele Absätze und Zwischenüberschriften zu gliedern (siehe die Bildschirmabbildung oben).

Prüfen Sie auch zu diesem Zeitpunkt schon, ob es möglich und sinnvoll sein kann, einen längeren Text über mehrere Einzelseiten zu verteilen, also in verschiedene Abschnitte aufzuteilen. Mit

der passenden Zwischenüberschrift versehen, können Sie später dem Benutzer zu Beginn des Textes dann eine

Und wenn einmal ein längerer zusammenhängender Text angeboten werden muss, gibt es auch Alternativen:

So könnten Sie von einer Kurzfassung auf Ihrer Website aus auf ein Dokument verweisen, das auf Anforderung den vollständigen Text liefert – ein »Word«-Dokument oder ein »PDF« (siehe den vorangegangenen Artikel ab Seite 33), das Ihre Besucher mit dem »Acrobat Reader« öffnen und ausdrucken können. Eine solche Möglichkeit, Texte oder auch größere Bilder »herunterzuladen«, ist übrigens ohne große Probleme einzurichten. Grundsätzlich handelt

The screenshot shows the website 'ergo-online' with a navigation menu on the left containing links like 'inhalt', 'einstieg', 'suchen', 'a-z', 'aktuelles', 'kontakt', 'lernen', and 'hilfe'. The main content area features several sections: 'Ein noch so komfortabler Stuhl ersetzt nicht Bewegung', 'Dynamische Rückenlehne', 'Synchronmechanik', 'Integrierte höhenverstellbare Lendenwirbelabstützung', and 'Vielfältige Modelle'. Two side-by-side photographs show a woman sitting in an office chair, demonstrating different backrest positions. A quote box on the right side of the screenshot reads: 'Die Website von »ergo-online« ist nicht nur aus inhaltlichen Gründen immer einen Besuch wert. Auch die Aufbereitung der Texte mit starker Untergliederung, vielen »Rand-Überschriften« und eingestreuten Bildern ist vorbildlich!'.

Gliederungsansicht präsentieren und die einzelnen Punkte mit den entsprechenden Textteilen verknüpfen, so dass der Nutzer nach einem Klick auf eine Themenüberschrift sofort zum entsprechenden Abschnitt springt. Auch das eine oder andere Bild (Foto, Grafik, Illustration) wirkt strukturierend.

In Zeiten immer größer werdender Monitore ist es darüber hinaus auch sinnvoll, die Breite des laufenden Textes zu begrenzen. Sonst passiert es schnell, dass ein Benutzer das Fenster mit der Website auf die volle Monitorbreite zieht und der Text sich dieser Breite dann anpasst – 20 oder gar 30 Zentimeter lange Zeilen aber, womöglich noch in relativ kleiner Schrift, lassen sich nun wirklich nur sehr mühsam lesen. Verhindern lässt sich ein solcher Effekt in der HTML-Programmierung durch den Einsatz von »Frames« (siehe: »Mit oder ohne Frames« in CF 11/02 ab Seite 34) oder durch die Verwendung »unsichtbarer Tabellen« mit einer festen Breite (zu diesen technischen Feinheiten aber in den kommenden Folgen noch mehr).

es sich dabei um einen ganz normalen »Link« – nur dass eben nicht auf eine »normale« Intranet-Seite verbunden wird, sondern auf eine Datei. Aber auch dazu in einer der kommenden Folgen mehr.

Das Internet ist etwas Besonderes

WAS NUN DIE OPTISCHE Gestaltung von Texten im Internet/Intranet betrifft, muss man leider etwas umdenken. »Back to the roots!« könnte man das Motto nennen. Denn viele Dinge, die in Textverarbeitungs- oder Layout-Programmen heute schon wie selbstverständlich genutzt werden, lassen sich nicht oder zumindest nicht so einfach auf eine Website übertragen.

Viele Einschränkungen liegen in der ›Programmierung‹ der Intranet-Seiten begründet – der ›Seitenbeschreibungssprache‹ HTML (Hypertext Markup Language). Wenn man sich nämlich etwas intensiver mit der Materie beschäftigt, merkt man schnell, dass diese ›Auszeichnungssprache‹ erfunden worden ist, um Texte möglichst schnell zu übertragen, sie auf möglichst jedem Computer-Bildschirm komplikationslos anzeigen zu können und um schnelles ›Springen‹ von einer Textstelle zu einer anderen zu ermöglichen. Nicht erfunden wurde sie, um eine bis ins einzelne Zeichen ausgefeilte Text- und Seitengestaltung im Internet zu ermöglichen. Deshalb entsprechen die Möglichkeiten der Textgestaltung durch HTML auch nur denen der einfachsten Textprogramme – damit muss man sich abfinden und das Beste daraus machen.

Und noch eine Besonderheit ist bei der Website-Gestaltung zu berücksichtigen: Um die Menge der zu übertragenden Daten so gering wie möglich zu halten, wird für die Darstellung der Inhalte auf dem Bildschirm auf Ressourcen zurückgegriffen, die auf dem Rechner *des Empfängers* installiert sind. In erster Linie ist das natürlich der ›Browser‹, also das Programm, mit dem die Inhalte betrachtet werden. So können unter Umständen schon verschiedene Versionen ein und desselben Browsers eine Internet-Seite unterschiedlich darstellen.

Das stellt die Internet-Gestalter und -Programmierer häufig vor große Probleme – denn die Darstellung einer Website soll natürlich in allen Umgebungen und auf jedem Bildschirm möglichst gleich aussehen. Im Intranet eines Unternehmens ist diese Problematik etwas weniger schwerwiegend, denn oft ist die Ausstattung aller dort eingesetzten Arbeitsplatzrechner sehr ähnlich – so werden zum Beispiel das gleiche Betriebssystem und der gleiche Browser auf allen Rechnern benutzt.

Eine weitere Ressource, die auf dem Rechner des Intranet-Besuchers genutzt wird, ist die dort vorhandene Auswahl

an Schriften. Hierzu muss man wissen, dass in der Programmierung einer Website nur der *Inhalt* zu finden ist, für die *Zusammensetzung* der Inhalte auf dem Bildschirm und die verwendete *Schrift* ist der jeweilige ›Browser‹ zuständig.

Dieses Verfahren kann zu Problemen führen. Ein einfaches Beispiel: Sie gestalten eine Einladung zur nächsten Betriebsversammlung und nutzen dafür – wie vielleicht bei der Gestaltung der Aushänge für das schwarze Brett gewohnt – diverse schöne Schriften, die nicht zum Standard-Repertoire eines jeden Personal Computers gehören. Sie stellen die Einladung ins Netz und schauen sie sich in Ihrem Browser noch einmal an – alles bestens.

Am nächsten Tag ruft Sie ein Kollege an und fragt, warum die Mitteilung im Intranet denn so ›merkwürdig‹ aussehe. Nun, dieser Anrufer hat dann entweder einen schlechten Geschmack oder er hat die von Ihnen verwendeten Schriften auf seinem Rechner nicht installiert. Ist Letzteres der Fall, wird sein Browser die von Ihnen ausgewählte Schrift durch eine ›Standard-Schrift‹ (z. B. die ›Schreibmaschinenschrift‹ Courier) ersetzt haben – und das kann in einigen Fällen recht merkwürdig aussehen.

Zur Zeit gibt es noch keine ausgereifte Möglichkeit, ganz bestimmte Schriften mit zum Benutzer zu übertragen und auf dessen Bildschirm anzeigen zu lassen. Verantwortlich dafür sind vor allem rechtliche Gründe, denn die meisten Schriften sind urheberrechtlich geschützt und dürfen (wie Software auch) nicht ohne Lizenz weitergegeben werden. Aber auch die Datenmenge, die zur Darstellung übertragen werden müsste, spielt natürlich eine Rolle.

Deshalb: Verwenden Sie nur Schriften, die als Standard auf allen oder zumindest auf den meisten Rechnern installiert sind. Ohne Frage wird sich dadurch die Anzahl der nutzbaren Schriften auf eine Handvoll reduzieren. Aber wenn Sie sich im Internet umschauen, werden Sie feststellen, dass die meisten Websites mit diesen wenigen Schriften auskommen – und das nicht einmal schlecht. Unter anderem gehören dazu: die Times, die Arial, die Courier und die Verdana.

Diese geringe Auswahl an Schriften hat durchaus auch positive Seiten. Kann man über sehr viele Schriften verfügen, so neigt man dazu, sie einzusetzen – und das nicht immer zu Gunsten von Klarheit, Übersichtlichkeit und Lesbarkeit. Außerdem zeichnet sich eine Schrift wie zum Beispiel die Verdana dadurch aus, dass sie am Monitor auch in kleineren Schriftgrößen sehr gut lesbar ist. Eine Eigenschaft, die sie sich leider mit nur ganz wenigen anderen Schriften teilen muss ...

Doch etwas mehr Vielfalt gefällig?

WENN SIE ERST EINMAL auf den Geschmack gekommen sind, die Seiten Ihres Intranet-Auftritts zu gestalten, werden Sie die eben genannten Beschränkungen allerdings oft als Fessel empfinden. Aber – in der letzten Folge haben wir es bereits angesprochen – es gibt eine Möglichkeit, diese Beschränkung aufzuheben: Einzelne Textelemente können auch als Grafik erstellt und in eine Seite integriert werden. Übertreiben sollte man es damit aber nicht. Zwar könnte man rein theoretisch mit allen Textinhalten seiner Website so verfahren, aber sowohl die Übertragungsgeschwindigkeit wie auch die Pflegebarkeit würden darunter leiden.

Aus gestalterischer Sicht kann es jedoch schon eine Menge bringen, wenn Sie zum Beispiel in der Navigation oder in den wichtigeren Überschriften einer Seite eine besondere Schrift einsetzen – etwa die Schrift, die auch in Ihren gedruckten Publikationen genutzt wird oder vielleicht die Hausschrift des Unternehmens.

Sebastian Fricke, Geschäftsführer der IN.MEDIUM GmbH, Neumünster, ist Berater für Konzeption und technische Implementierung von Online-Anwendungen und außerdem Dozent und Lehrer für Medientechnik; Kontakt: IN.MEDIUM GmbH, Gartenstraße 10, 24534 Neumünster; s.fricke@inmedium.net; www.inmedium.net



Workflow- Management für den Personalrat

Es ist möglich: das papierlose Büro für den Personalrat!

Alle Eingänge kommen übers Netz oder

werden elektronisch erfasst, Fallbearbeitung am Bildschirm,

›automatisierte‹ Zusammenstellung der Tagesordnung

und so weiter und so fort ...

DIE ABKÜRZUNG ›DoVoMa‹ bedeutet ›Dokumenten- und Vorgangs-Management‹. Entwickelt wurde die Software vor rund vier Jahren speziell für die Aufgaben eines Hauptpersonalrats, und zwar den beim Bundesgrenzschutz (siehe auch: ›DoVoMa – Software für die Personalvertretung‹ in cf 7/99 ab Seite 27). Um einige DoVoMa-Besonderheiten zu verstehen, sollte man allerdings wissen, dass die Arbeit des BGSHPR (Bundesgrenzschutz-Hauptpersonalrat) in mehrfacher Hinsicht eine recht spezielle ist:

(1) Der BGS-Hauptpersonalrat hat in besonders großem Umfang an personellen Einzelmaßnahmen mitzuwirken. Das sind vor allem Versetzungen von dieser in jene Einheit oder Dienststelle, oft auch nur befristet. Obwohl der Hauptpersonalrat erst von einer etwas höheren Hierarchiestufe an zu beteiligen ist, ist es dennoch eine enorme Zahl einzelner Vorgänge, die bei ihm landet (z. B. für vorübergehende Auslandseinsätze). Erschwerend kommt noch hinzu, dass natürlich immer auch die Personalräte

der ›abgebenden‹ und der ›empfangenden‹ Dienststelle zu informieren sind und die Möglichkeit haben zuzustimmen oder abzulehnen, ehe der Hauptpersonalrat dann endgültig entscheidet und dies wiederum an alle anderen ›Prozessbeteiligten‹ zurückmeldet ... Dass bei alledem auch noch Fristen zu beachten und einzuhalten sind, versteht sich von selbst.

(2) Jede dieser personellen Einzelmaßnahmen muss also nach Information durch den Dienstherrn (Bundesministerium des Inneren) und nach Verständigung mit den beiden beteiligten örtlichen Personalräten auf der Tagesordnung der Hauptpersonalratsitzung landen – neben allen anderen (Mitbestimmungs-)Themen natürlich, mit denen sich so ein (Haupt-)Personalrat nun einmal zu beschäftigen hat. Dabei kommt dann eine viele Seiten lange Tagesordnung heraus, die einmal im Monat auf einer mehrtägigen (!) Sitzung abgearbeitet wird. Um dies auf effektive Weise möglich zu machen, muss natürlich jedes HPR-Mitglied schon vor der Sitzung möglichst klare Informationen zu jedem Tagesordnungspunkt bekommen.

(3) Erschwert wird dieses Verfahren dadurch, dass die Mitglieder des Hauptpersonalrats nicht etwa alle an einem Ort (Berlin) zusammenarbeiten, sondern zumindest zu einem großen Teil aus der ganzen Bundesrepublik anreisen (daher auch die konzentrierten mehrtägigen Monatsitzungen).

Schon diese knappe Beschreibung macht deutlich, dass es sich hier um ›Geschäftsprozesse‹ handelt, die mit herkömmlichen Mitteln außerordentlich schwierig zu organisieren sind oder vielmehr waren. Schon vor längerer Zeit nämlich begann Joachim Cortmann, HPR-Mitglied seit vielen Jahren, auf eigene Faust kleine Programme zu ›stricken‹, die bei der Bewältigung dieser Aufgabe helfen sollten. Nach einem Wechsel der EDV-Technik auf ein Windows-PC-Netz wurden diese bescheidenen Anfänge dann verknüpft und (von einem professionellen Software-Haus) weiterentwickelt zum DoVoMa-System, das seit Ende der 90-er Jahre im Einsatz ist.

DoVoMa, ein echtes Workflow-Programm

BEREITS DAS DAMALIGE DoVoMa, das jetzt gerade in einer überarbeiteten und erweiterten Fassung herausgekommen ist, war allerdings weit mehr als eine Software für die schnelle und übersichtliche Bearbeitung personeller Einzelmaßnahmen. Der Begriff war damals noch nicht so in aller Munde, aber DoVoMa war und ist eine komplette ›Workflow‹-Software für die Arbeit eines Personalrats, einsetzbar nicht nur für die speziellen Aufgaben eines BGS-Hauptpersonalrats, sondern – davon ist der DoVoMa-›Vater‹ Joachim Cortmann überzeugt – die Organisation und Verwaltung eines jeden Personalrats unterstützen kann. Möglicherweise werden dabei nicht alle DoVoMa-Funktionen genutzt werden können, aber es bleiben in jedem Fall doch genügend viele Funktionen ›übrig‹, so dass sich der Einsatz ›lohnt‹ – zumal die Nutzung von DoVoMa für jeden Per-

sonalrat im Bereich der öffentlichen Verwaltung (so gut wie) kostenlos ist. Da die Software letztlich im Auftrag des Innenministeriums entwickelt und von ihm finanziert wurde, sollte sie – das war Bestandteil des Konzepts von Beginn an – für den unbeschränkten Einsatz im Rahmen der öffentlichen Verwaltung zur Verfügung stehen.

Aber obwohl man einem geschenkten Gaul bekanntlich nicht irgendwohin schaut, muss die Frage, was DoVoMa denn konkret zu bieten hat, erlaubt sein. Denn auch wenn man für die Nutzung nichts bezahlen muss, so muss man doch Zeit und Kraft investieren, um den Umgang mit dem relativ komplexen Programm zu erlernen und es auf die eigenen Bedürfnisse und Gegebenheiten einzurichten.

Dass sich dies lohnt, verdeutlicht Cortmann gerne an einer geradezu klassischen Situation: Ein neu gewähltes Personalratsmitglied hat sich eben an seinem neuen Schreibtisch niedergelassen, als bereits ein erstes Mal das Telefon klingelt – eine Nachfrage zu einer schon etwas zurück liegenden Beschwerde.

Im Normalfall müsste sich unser neu gewähltes Personalratsmitglied nun wohl etwas winden, um Verständnis bitten und zunächst einmal versuchen, den entsprechenden Vorgang in irgendeinem Aktenordner ausfindig zu machen. Aber mit DoVoMa und geringen Grundkenntnisse kann er mit Hilfe des Namens und der Filterfunktion ❶ sofort den richtigen Vorgang suchen und finden ❷.

Der nach ein, zwei Mausklicks angezeigte Vorgang ❸ kann nun aus einem oder zwei Briefen bestehen, kann aber auch einen umfangreichen ›Workflow‹ (Bearbeitungsprozess, Arbeitsfluss) widerspiegeln: Ein erstes Eingangsschreiben (oder die Notiz zu einem Telefongespräch), die Eingangsbestätigung, eine Anfrage an den Dienstherrn, dessen

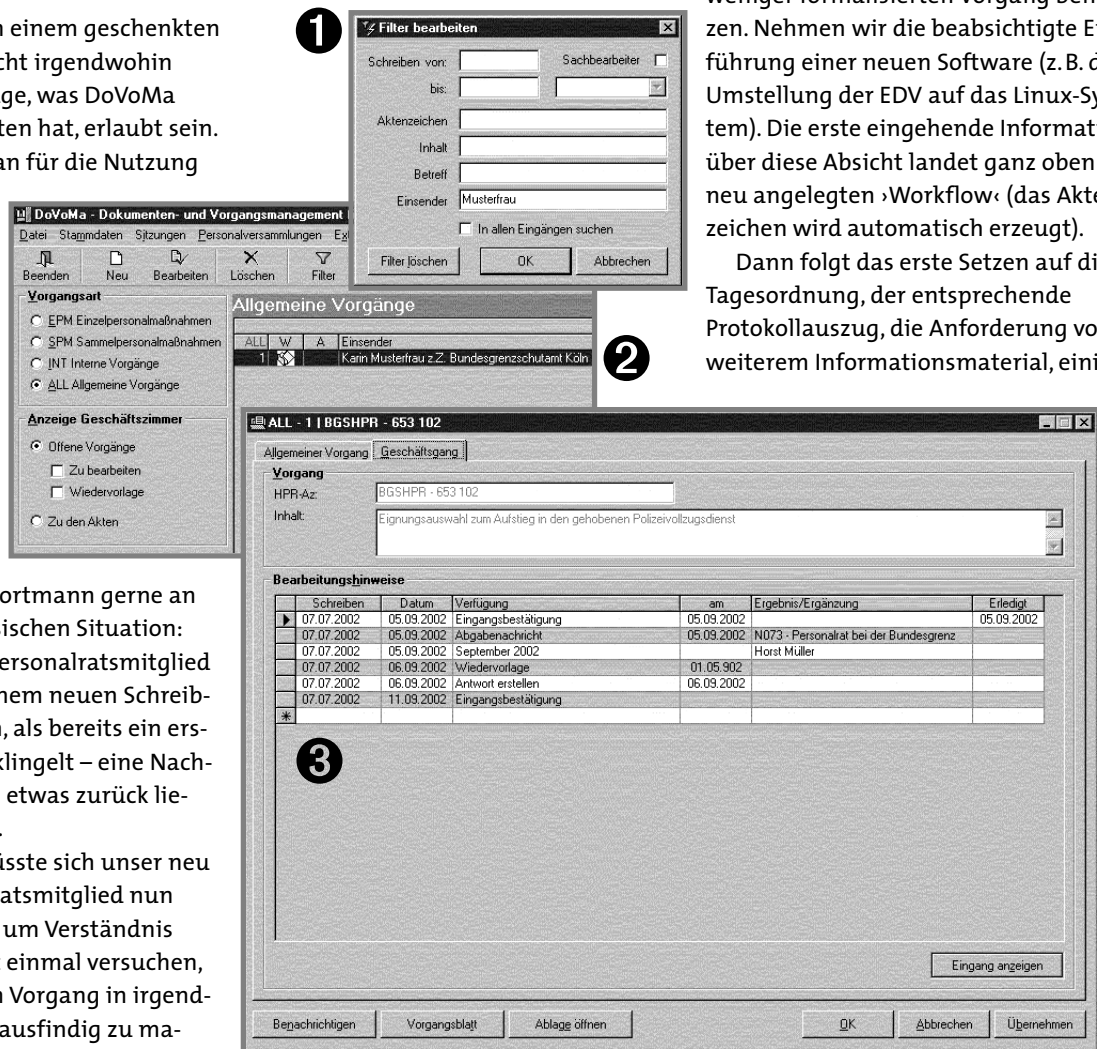
Antwort, den Entwurf einer Stellungnahme, Auszug aus Tagesordnung und Protokoll der Personalratssitzung, auf der der Fall behandelt wurde und so weiter und so fort.

Schon jetzt wird klar, dass DoVoMa um so besser funktioniert, je weitergehend alle im Verlauf eines ›Workflows‹

für eine Zuordnung wichtigen Daten (Absender, Datum, Betreff usw.) über Tastatur erfasst.

Was für Routinevorgänge wie die Mitteilung einer beabsichtigten persönlichen Einzelmaßnahme im Idealfall schon fast automatisch funktioniert, lässt sich aber auch für jeden anderen, weniger formalisierten Vorgang benutzen. Nehmen wir die beabsichtigte Einführung einer neuen Software (z. B. die Umstellung der EDV auf das Linux-System). Die erste eingehende Information über diese Absicht landet ganz oben im neu angelegten ›Workflow‹ (das Aktenzeichen wird automatisch erzeugt).

Dann folgt das erste Setzen auf die Tagesordnung, der entsprechende Protokollauszug, die Anforderung von weiterem Informationsmaterial, einige



entstehenden Dokumente von vornherein und vollständig elektronisch eingehen oder erzeugt werden. Im Fall des BGS-Hauptpersonalrats ist dies natürlich schon relativ weit fortgeschritten. So gehen Anfragen, Anträge und Stellungnahmen von Seiten des Dienstherrn (Bundesinnenministerium) von vornherein als elektronische Dokumente via E-Mail ein und werden (mit Übernahme von Aktenzeichen, Betreff usw.) automatisch für die weitere Bearbeitung aufbereitet. Ist dies (z. B. bei Anfragen von außen) nicht der Fall, werden die eingegangenen Dokumente gescannt und die

Stellungnahmen, erneutes Setzen auf die Tagesordnung, der Beschluss des Personalrats, einen Sachverständigen einzuschalten, dessen Stellungnahme, einschließlich einer Linux-Broschüre im PDF-Format und immer so weiter.

Also: Auch wenn DoVoMa speziell für die Bedürfnisse des BGS-Hauptpersonalrats entwickelt wurde, ist es doch für die Erfassung und Bearbeitung jedes Themas geeignet. Ist ein Dokument (z. B. die erwähnte Broschüre) einmal nicht in elektronischer Form greifbar



und zum Einscannen zu umfangreich, kann sie auch herkömmlich abgelegt werden – in DoVoMa wird dann nur die entsprechende Fundstelle (Hängeregister, Ordner) festgehalten.

Vorausgesetzt, der Personalrat hat seine ›Workflows‹ entsprechend organisiert und festgelegt, kommt mit DoVoMa also das ›papierlose Personalratsbüro‹ durchaus in den Bereich des Möglichen. Zu einem echten ›Workflow‹-System

Die Tagesordnung der jeweils nächsten Personalratssitzung ④+⑤ wird ebenfalls (halb-)automatisch zusammengestellt und auf Knopfdruck an alle Teilnehmenden verschickt. Die formularmäßige Erfassung der wichtigsten Da-

Ist ein Fall schließlich abgeschlossen, wird er archiviert – und zwar so, dass von nun an alle gespeicherten Dokumente schreibgeschützt sind, also nicht etwa noch nachträglich verändert werden können.

Mancher (vor allem größere) Betriebsrat könnte jetzt vielleicht neidisch werden, weil es für die Betriebsratsarbeit ein vergleichbares ›Workflow‹-Programm noch nicht gibt. Und er wird wohl auch neidisch bleiben müssen, denn bisher gibt es noch niemanden, der sich der Aufgabe, DoVoMa auf die Anforderungen der Betriebsratsarbeit umzustricken, mit Erfolg gestellt hätte ... Schade, eigentlich.



W: DoVoMa - 10_Sitzung_24.doc [Kopie]

Dokumente abrufen...

Suchen in: Sitzungen

- TO_Sitzung_10.doc
- TO_Sitzung_23.doc
- TO_Sitzung_24.doc
- TO_Sitzung_28.doc

4 Suchen nach bestimmten Tagesordnungen

Dateiname:

Dateityp: Tagesordnungen

Mit Schreibschutz öffnen

Öffnen Abbrechen

W: DoVoMa - 10_Sitzung_24.doc [Kopie]

Dokumente abrufen...

Suchen in: Sitzungen

5 Eingesetzter Tagesordnungspunkt

Lfd. Nr.	Reg. - Nr.	Aktenzeichen
-	Sachbearbeiter	Text
Nr.	Berichterstatter	
11	INT2	BGSHPR - 630 300 - VII/4 Organisation BGSi Süd Betreff: ASas
12	ALL1	BGSHPR - 653 102 Eignungsauswahl zum Aufstieg in den gehobenen Polizeivollzugsdienst Betreff: Aufstieg in den gehobenen Dienst im BGS hier: Zulassungsbedingungen

Dokumente abrufen...

Suchen in: Sitzungen

- TO_Sitzung_10.doc
- TO_Sitzung_23.doc
- TO_Sitzung_24.doc
- TO_Sitzung_28.doc

4 Suchen nach bestimmten Tagesordnungen

Dateiname:

Dateityp: Tagesordnungen

Mit Schreibschutz öffnen

Öffnen Abbrechen

DoVoMa kann übrigens von allen Personalräten der öffentlichen Verwaltung kostenlos genutzt werden!

wird es durch solche Funktionen wie eingebaute Terminwarnungen und Wiedervorlagen oder die automatisierte Information/Weiterleitung an andere Gremien in Form definierbarer ›Geschäftsgänge‹. Hinzu kommt, dass DoVoMa, wo immer das möglich ist, formular-ähnliche ›Eingabemasken‹ anbietet, so dass nichts formal Wichtiges vergessen werden kann.

Die festgelegten Geschäftsgänge beziehen dabei auch das Büropersonal ein. Wenn also ein Personalratsmitglied einen Fall am Bildschirm bearbeitet, so hat es im ›Geschäftsgang‹ ⑥ die Möglichkeit, durch Knopfdruck festzulegen, welche Aktion (z.B. das Zusenden einer Bescheinigung) durchgeführt werden muss. Die zuständige Bürokräft bekommt diesen Auftrag dann automatisch auf ihren Bildschirm, führt ihn aus und fügt einen entsprechenden Vermerk in den Geschäftsgang ein.

W: DoVoMa - 10_Sitzung_24.doc

Dokumente abrufen...

Suchen in: Sitzungen

5 Eingesetzter Tagesordnungspunkt

Lfd. Nr.	Reg. - Nr.	Aktenzeichen
-	Sachbearbeiter	Text
Nr.	Berichterstatter	
11	INT2	BGSHPR - 630 300 - VII/4 Organisation BGSi Süd Betreff: ASas
12	ALL1	BGSHPR - 653 102 Eignungsauswahl zum Aufstieg in den gehobenen Polizeivollzugsdienst Betreff: Aufstieg in den gehobenen Dienst im BGS hier: Zulassungsbedingungen

6 Einfügen des Protokolltextes (= Beschluss) in die Tagesordnungsvorlage

ten (z.B. einer personellen Einzelmaßnahme) erlaubt es auch, die Tagesordnung gleich mit den nötigsten Fakten für die Beurteilung des Falles auszustatten – was eine optimale Vorbereitung zumindest ermöglicht. Das Protokoll ⑥ wird dann (unterstützt durch automatisch eingefügte Formulareile etwa zum Abstimmungsergebnis) direkt in das Tagesordnungsformular hinein getippt.

Nähere Informationen zu DoVoMa gibt:

**Bundesgrenzschutzhauptpersonalrat
beim Bundesministerium des Innern
Alt Moabit 101 D
13519 Berlin
fon 01888-681-3448 (-2719)
fax 01888-681-53448
joachim.cortmann@bmi.bund.de**