Betriebs- und
Mitbestimmungspolitik | **Vorstand**

25

Arbeitnehmerdatenschutz

Impressum

Produkt-Nr. 15966-23149

Herausgeber:
IG Metall
Betriebs- und Mitbestimmungspolitik

Autoren: Dirk Hammann, Karl Schmitz, Wolfgang Apitzsch
Redaktion: Jochen Homburg, FB Betriebs- und Mitbestimmungspolitik

Ausgabe: März 2009

Druckvorstufe: Mediakonzept Widdig GmbH, Köln
Druck: MediaPrint, Paderborn

Vorwort

Zu einer erfolgreichen Interessenvertretung gehören gewerkschaftlich organisierte und selbstbewusst handelnde Belegschaften und qualifizierte, gut informierte Funktionäre der IG Metall.

Arbeitsplätze sichern, soziale Arbeitsbedingungen schaffen und eigene betriebspolitische Gestaltungsziele erarbeiten und durchsetzen – das sind Aufgaben, die Betriebsräte und Vertrauensleute der IG Metall in ihrer täglichen Arbeit leisten müssen. Dabei ist es von großer Bedeutung die Belegschaften, insbesondere die IG Metall-Mitglieder, durch eine beteiligungsorientierte Betriebsrats- und Gewerkschaftsarbeit in die Arbeit mit einzubeziehen.

Die Anforderungen an die Betriebsratsarbeit in Betrieben und Verwaltungen sind erheblich gestiegen. Die Rahmenbedingungen und Entwicklungen in Betrieben, Unternehmen und Konzernen werden zunehmend komplexer, schnelllebiger und finanzmarktorientierter. Betriebsräte und Vertrauensleute brauchen für ihre tägliche Arbeit ein solides Grundwissen über gesetzliche Bestimmungen und entsprechende Handlungsmöglichkeiten. Dafür steht ein breitgefächertes Seminarangebot zur Verfügung. Informationen dazu gibt es in den Verwaltungsstellen und in den Medien der IG Metall (www.igmetall.de).

Mit unserer Broschürenreihe wollen wir InteressenvertreterInnen Grundlagen vermitteln und Unterstützung und Handlungsorientierung für die betriebliche Arbeit geben (siehe Liste und Bestellmöglichkeit am Ende der Broschüre).

Sie ersetzen jedoch keinesfalls die für die Arbeit der Betriebsräte unverzichtbaren Kommentare zum Betriebsverfassungsgesetz und zu den anderen Gesetzen. Wir empfehlen folgende Kommentare zum BetrVG:

Kommentar für die Praxis – Däubler/Kittner/Klebe
Handkommentar – Fitting/Schmidt/Trebinger/Linsenmaier
Basiskommentar – Klebe/Ratayczak/Heilmann/Spoo

Kolleginnen und Kollegen, die sich tiefer in die Materie einarbeiten wollen, finden deshalb auch Hinweise auf weiterführende Literatur.

Bitte beachtet auch die vom Funktionsbereich Betriebs- und Mitbestimmungspolitik herausgegebenen Rechtsprechungshinweise zum BetrVG, die für Funktionäre der IG Metall über das Extranet -> Themen -> Recht -> Gerichtsentscheidungen abgerufen werden können.

Frankfurt am Main, März 2009

IG Metall

– Vorstand –

Detlef Wetzel

Inhalt

Abkürzungsverzeichnis 6

I. Arbeitnehmerdatenschutz – das vergessene Gesetz 7
1. Datenschutz in der Arbeitswelt 7
2. Grundrecht Informationelle Selbstbestimmung 8
3. Das so genannte Computergrundrecht 9
4. Konsequenzen für die Arbeitswelt 12
5. Der Verhältnismäßigkeitsgrundsatz 15
6. Datenschutz und Mitbestimmung 16

II. Personaldaten 19
1. Grundlagen 19
2. Überalterte Regelungen 21
3. Neuere Regelungskonzepte 22
4. Neue Themenfelder 25
5. Workflows und Self Services 27
6. Data-Warehouse-Anwendungen 32

III. E-Mail und Internet 36
1. Grundlagen 36
2. Internet 37
3. E-Mail 42
4. Webfilter-Software 46
5. Antiviren-Programme 47
6. Spamfilter-Software 48

IV. Intranet und Web 2.0 51
1. Grundlagen 51
2. Elektronische Kalender 52
3. Weblogs und Wikis 53
4. Webkonferenzen 55

V. Netzwerksicherheit und Rechner-Administration 57
1. Grundlagen 57
2. Intrusion Detection Systeme (IDS) 58
3. Organisatorische Regelungen 61
4. Remote Control – Software zur Fernsteuerung 62
5. Inventarisierung, Lizenzkontrolle und Softwareverteilung 64
6. Betriebssysteme Windows, Apple 67

VI. Telefonanlagen 69
1. Grundlagen 69
2. Telekommunikationsanlage 69
3. Automatische Anrufverteilung (ACD) 72
4. Computer-Telephony-Integration (CTI) 75
5. Dialer 76
6. Voice over IP („VoIP“) 77
7. Mobiltelefone 78
8. Local Based Services / GPS 81

VII. Videoüberwachung 83
1. Grundlagen 83
2. Leistungsmerkmale der Videosysteme 83
3. Einwände 84
4. Regelungsaspekte 85

VIII. Chipkarten und Biometrische Systeme 87
1. Grundlagen 87
2. Mitarbeiterausweise mit RFID-Chips 88
3. Zeiterfassung 89
4. Zutrittskontrolle 92
5. Login-Kontrolle 94
6. Abrechnungssysteme für die Kantine, Parkplatz-Ticketing und andere Systeme . . . 96
7. Biometrische Erkennungssysteme 97

IX. Betriebsdaten 99
1. Grundlagen 99
2. Produktionssteuerungssysteme 99
3. Andere betriebsdatenverarbeitende Systeme 102

X. Globalisierungsfolgen 103
1. Weltweite Zentralisierungstendenzen 103
2. Die datenschutzrechtliche Kehrseite 104

XI. Und was ist zu tun? 107
1. Sachverständige 107
2. Einigungsstelle 108
3. Ausblick 109

Stichwortverzeichnis 111

Abkürzungsverzeichnis

Abs.	Absatz
ACD-Anlage	Automatic Call Distribution-Anlage
Art.	Artikel
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BR	Betriebsrat
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
CIA	Central Intelligence Agency
CTI	Computer Telephony Integration
d. h.	das heißt
EG	Europäische Gemeinschaft
EU	Europäische Union
f., ff.	folgende, fortfolgende
FAQ	Frequently asked question
GG	Grundgesetz
ggf.	gegebenenfalls
HCM	Human Capital Management
HR	Human Resources
IDS	Intrusion Detection Syteme
IP	Internetprotokoll
MMS	Multimedia Messaging Service
Nr.	Nummer
o. Ä.	oder Ähnliche(s)
§, §§	Paragraf, Paragrafen
PPS	Produktionsplanungs- und -steuerungssysteme
REFA	Verband für Arbeitsgestaltung, Betriebsorganisation und Unternehmensentwicklung
RFID	Radio Frequency Identification
S.	Seite
s.	siehe
SAP	Systems Applications and Products
SMS	Short Message Service
sog.	so genannt
TBS	Technologieberatungsstelle beim DGB
TKG	Telekommunikationsgesetz
usw.	und so weiter
vgl.	vergleiche
VoIP	Voice over IP
v.	vom
z. B.	zum Beispiel

I. Arbeitnehmerdatenschutz – das vergessene Gesetz

Ein Arbeitnehmer-Datenschutzgesetz, das – über das allgemeine Datenschutzgesetz hinaus – in umfassender Form den Persönlichkeitsschutz der Menschen als Arbeitnehmer in ihrem Verhältnis zum Arbeitgeber sicherstellen soll, gibt es bis heute in Deutschland nicht.

Obwohl der Deutsche Bundestag die Forderung nach einem solchen Gesetz wiederholt mit großen, fraktionsübergreifenden Mehrheiten unterstützt hat, haben die verschiedenen Bundesregierungen – von Schwarz-Gelb über Rot-Grün bis zu Schwarz-Rot – bislang keine erkennbaren Aktivitäten auf diesem Gebiet entwickelt. Mit entschuldigendem Blick auf die Europäische Union nach Brüssel wartet man lieber auf die „Schaffung des harmonisierten Gemeinschaftsrahmens zum Arbeitnehmerdatenschutz", die von dort kommen soll.

Aber auf der europäischen Ebene kommt die Initiative für die europaweite Arbeitnehmerdatenschutzrichtlinie nicht voran. Die Aussichten für einen verbesserten Arbeitnehmerdatenschutz, gestützt auf gesetzliche Regelungen, sehen in naher Zukunft schlecht aus, kommentiert der Bundesdatenschutzbeauftragte den politischen Stillstand.[1]

Arbeitnehmer und Arbeitgeber sind daher im Wesentlichen darauf angewiesen, sich an der allgemeinen Rechtslage und an der lückenhaften, im Einzelfall für die Betroffenen nur schwer zu erschließenden einschlägigen Rechtsprechung zu orientieren. Dabei will diese Broschüre eine Hilfestellung geben.

1. Datenschutz in der Arbeitswelt

Rechtliche Grundlage

Normalerweise besteht die datenschutzrechtliche Grundlage der in den Unternehmen verarbeiteten personenbezogenen Daten in der Verwaltung des Arbeitsverhältnisses. Dabei sind allerdings gewichtige Rahmenbedingungen zu beachten. § 75 BetrVG verpflichtet Arbeitgeber und Betriebsrat gleichermaßen zur Respektierung der Würde des Menschen im Arbeitsleben und verweist damit auf das Grundrecht der informationellen Selbstbestimmung. Einschnitte in dieses Grundrecht, wie es die Verwaltung des Arbeitsverhältnisses erfordert, haben nach einer alten Entscheidung des Bundesverfassungsgerichts[2] die Grundsätze der strikten Zweckbindung, der Verhältnismäßigkeit und der Normenklarheit zu beachten.

[1] „Arbeitnehmer und Datenschutz", Rede im Namen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Arbeitnehmerdatenschutz, gehalten im Rahmen der SAP-Fachtagung 2008 des TBS-Netzes am 15.2.2008 in Berlin.

[2] Volkszählungsurteil des BVerfG v. 6.12.1983 (DB 1984, 36)

In drei Entscheidungen des Jahres 2008 hat das Bundesverfassungsgericht nachdrücklich betont, dass die Bedeutung des Computereinsatzes für den Bereich der Persönlichkeitsentwicklung beachtlich gestiegen ist und daher dem Grundrecht der informationellen Selbstbestimmung eine wesentlich höhere Bedeutung zukommt, als dies gemeinhin bisher gesehen wurde. Insbesondere hat das Gericht klargestellt, dass bei Einschnitten in dieses Grundrecht die Messlatte der Verhältnismäßigkeit hoch anzulegen ist;[3] d. h. die Eingriffe sind so sparsam wie möglich zu gestalten, und es bedarf schwerwiegender Gründe für einen solchen Eingriff.

Zwar hat das Bundesverfassungsgericht in den erwähnten Urteilen nur das Verhältnis Bürger – Staat im Visier gehabt, und sicher ist nicht alles dort Gesagte auf die Beziehung Arbeitgeber – Arbeitnehmer übertragbar, doch sind der bisher verbreitet beobachtbaren Leichtfertigkeit im Umgang mit personenbezogenen Daten in der Arbeitswelt deutlich engere Grenzen gesetzt.

Die äußerst umfangreiche Datenbasis, die für viele betriebliche Anwendungen benötigt wird, lässt sich vor dem geschilderten Hintergrund oft nicht mehr allein mit der Verwaltung des Arbeitsverhältnisses begründen. Meist umfassen die in den Unternehmen eingesetzten Systeme differenzierte Informationen, die weit über das zur Verwaltung des Arbeitsverhältnisses hinausgehen und ein detailliertes Persönlichkeitsbild abgeben. Sie sind daher in besonderem Maße schutzbedürftig.

2. Grundrecht Informationelle Selbstbestimmung

Als wegen zwei Dutzend bescheidener persönlicher Daten, die in der in den frühen 80er Jahren des letzten Jahrhunderts geplanten Volkszählung erhoben werden sollten, ein Sturm der Entrüstung durch die Republik fegte, hat nach Auffassung der Arbeitgeberverbände das Bundesverfassungsgericht in der bereits erwähnten Entscheidung ein neues Grundrecht erfunden, das Grundrecht der informationellen Selbstbestimmung. Natürlich war das keine Neuerfindung, sondern eine logische Konsequenz aus dem Grundgesetz. Die Feststellung des Gerichts besagte nicht mehr und nicht weniger, als dass jeder Einzelne selbst darüber bestimmen kann, welche persönlichen Informationen er preisgibt und für welche Zwecke diese verwendet werden dürfen.

Persönlichkeitsrecht nach Art. 2 Abs. 1 GG

Dieses Grundrecht als allgemeines Persönlichkeitsrecht leitet sich aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes ab. Dort heißt es:

[3] Vgl. Urteil v. 27.2.2007, 1 BvR 370/07 zum Computergrundrecht, v. 11.3.2008, 1 BVR 2074/05 und 1 BvR 1254/07, Urteil zum Scannen von Nummernschildern und v. 11.3.2008, 1 BvR 256/08, Urteil zur Vorratsdatenspeicherung. Kurzfassungen zum Computergrundrecht, zum Nummernscanning und zur Vorratsdatenspeicherung befinden sich auf der Website der *tse*.

- Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt (Art. 2 Abs. 1 GG).

- Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt (Art. 1 Abs. 1 GG).

Was im Grundgesetz über Aufgabe und Verpflichtung des Staates gegenüber seinen Bürgern geschrieben steht, findet sich in ähnlicher Weise in § 75 Abs. 2 BetrVG:

Freie Entfaltung des Arbeitnehmers nach § 75 BetrVG

- Arbeitgeber und Betriebsrat haben die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Sie haben die Selbstständigkeit und Eigeninitiative der Arbeitnehmer und Arbeitsgruppen zu fördern (§ 75 Abs. 2 BetrVG).

Daher sind an das Verhältnis Arbeitgeber – Arbeitnehmer ähnliche Maßstäbe zu legen, wie an das Verhältnis vom Staat zu seinen Bürgern; wir kommen darauf an späterer Stelle zurück.

3. Das so genannte Computergrundrecht

Im Frühjahr 2008 haben die Karlsruher Richter ihre Auffassung von 1983 in erstaunlicher Deutlichkeit präzisiert. In ihrem Urteil zur geplanten Online-Durchsuchung privater Computer passten sie das informationelle Selbstbestimmungsrecht den geänderten Fakten der Internet- und Computerwelt an und verliehen dem Schutz der persönlichen Computernutzung sozusagen grundrechtliche Weihen. Das Recht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ heißt es im Wortlaut der Urteilsbegründung, Kurzfassung: Das *Computergrundrecht*. Einer der Kläger gegen die geplante Lizenz zum Computerdurchsuchen, der ehemalige Bundesinnenminister Gerhard Baum, stellte dann auch mit Zufriedenheit fest: „Das Verfassungsgericht ist im Informationszeitalter angekommen“.

Die Nutzung der Informationstechnik, so argumentieren die Richter, habe für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Diese eröffne jedem Einzelnen einerseits neue Möglichkeiten, begründe aber auch andererseits neuartige Gefährdungen der Persönlichkeit, denen Rechnung getragen werden müsse.

Die jüngere Entwicklung der Informationstechnik habe dazu geführt, so die Richter, dass informationstechnische Systeme allgegenwärtig seien und ihre Nutzung für die Lebensführung der Menschen von immer größerer Bedeutung würde. Dabei ist auch zu berücksichtigen, dass sich die Leistungsfähigkeit der Computer in atemberaubendem

Neue Möglichkeiten des Computereinsatzes

Tempo erhöht hat und diese Entwicklung anhält. Die Folge ist, dass sich immer mehr Anwendungsbereiche für die Unterstützung durch Computer auftun.

Da Personalcomputer und mobile Geräte sich für eine Vielzahl unterschiedlicher Zwecke nutzen lassen, etwa zur umfassenden Verwaltung und Archivierung der eigenen persönlichen und geschäftlichen Angelegenheiten, als digitale Bibliothek oder in vielfältiger Form als Unterhaltungsgerät, ist ihre Bedeutung für die Persönlichkeitsentfaltung erheblich gestiegen. In diesem Zusammenhang verweist das Verfassungsgericht sogar darauf, dass zahlreiche Gegenstände, mit denen große Teile der Bevölkerung alltäglich umgehen, informationstechnische Komponenten enthalten (Handys, Fotoapparate und in zunehmendem Maße auch Haushaltsgeräte).

Ganz entscheidend sei auch, dass der Leistungsumfang informationstechnischer Systeme und ihre Bedeutung für die Persönlichkeitsentfaltung noch weiter zunehmen, wenn solche Systeme miteinander vernetzt werden, wie es insbesondere aufgrund der gestiegenen Nutzung des Internets durch große Kreise der Bevölkerung mehr und mehr zum Normalfall geworden sei.

Insbesondere das Internet als komplexer Verbund von Rechnernetzen öffne dem Nutzer nicht nur den Zugriff auf eine praktisch unübersehbare Fülle von Informationen, die von anderen Computern im Netz zum Abruf bereitgehalten werden. Es bietet daneben zahlreiche neuartige Kommunikationsdienste, mit deren Hilfe er aktiv soziale Verbindungen aufbauen und pflegen kann. Weiter ist zu beobachten, dass herkömmliche Formen der Fernkommunikation in weitem Umfang auf das Internet verlagert werden.

Neben diesen vielfältigen neuen Möglichkeiten der Persönlichkeitsentfaltung führt nach Auffassung der Richter die zunehmende Verbreitung vernetzter informationstechnischer Systeme zu neuen Persönlichkeitsgefährdungen.

Neue Gefahren des Computereinsatzes

Bei dem heute gegebenen breiten Spektrum von Nutzungsmöglichkeiten handelt es sich nicht nur um Daten, die der Nutzer des Rechners bewusst anlegt oder speichert. „Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weit reichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen“ (BVerfG v. 27.2.2008 – 1 BvR 370/07, Absatz-Nr. 178, vgl. NJW 2008, 822).

Bei einem vernetzten, insbesondere einem an das Internet angeschlossenen System, werden diese Gefährdungen in verschiedener Hinsicht vertieft. Zum einen führt die mit der Vernetzung verbundene Erweiterung der Nutzungsmöglichkeiten dazu, dass gegenüber einem allein stehenden System eine noch größere Vielzahl und Vielfalt von Daten erzeugt, verarbeitet und gespeichert werden. Dabei handelt es sich um Kommunikationsinhalte sowie um Daten mit Bezug zu der Netzkommunikation. Durch die Speicherung und Auswertung solcher Daten über das Verhalten der Nutzer im Netz können weitgehende Kenntnisse über die Persönlichkeit des Nutzers gewonnen werden.

Hinzu kommt noch, dass in einem Verbund vernetzter Systeme der Einzelne Zugriffe ganz anderer Personen zum Teil gar nicht wahrnehmen, und vor allem nur begrenzt abwehren kann. Dazu stellt das Gericht fest, dass informationstechnische Systeme mittlerweile einen derart hohen Komplexitätsgrad erreicht haben, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Weiter kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen.

Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgert das Verfassungsgericht ein grundrechtlich erhebliches Schutzbedürfnis. Das Gericht hatte sich nur mit den Überwachungsinitiativen des Staates gegen seine Bürger auseinanderzusetzen und stellte in diesem Zusammenhang fest, dass der Einzelne darauf angewiesen sei, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet. Dies wird man – in möglicherweise noch zu präzisierender Form – auch gegenüber den Arbeitgebern bezüglich ihres Verhältnisses zu ihren Arbeitnehmern erwarten dürfen.

Das Bundesverfassungsgericht stellt ausdrücklich fest, dass sich das Schutzbedürfnis des Nutzers eines informationstechnischen Systems nicht allein auf Daten beschränkt, die seiner Privatsphäre zuzuordnen sind. Die Möglichkeit einer Einordnung der Nutzung als privat hängt außerdem häufig von dem Kontext ab, in dem die Daten entstanden sind und in den sie durch Verknüpfung mit anderen Daten gebracht werden. Die Richter stellen fest, dass dem einzelnen Datum oft nicht anzusehen ist, welche Bedeutung es für den Betroffenen hat und welche es durch Einbeziehung in andere Zusammenhänge gewinnen kann. Dies habe zur Folge, dass mit jedem Eingriff in die Systeme nicht nur zwangsläufig private Daten erfasst werden, sondern der Zugriff auf alle Daten ermöglicht wird, so dass sich ein umfassendes Bild vom Nutzer des Systems ergeben könne. Und darin ist ein Gefährdungs-

potenzial zu sehen, das sich in der Vergangenheit in diesem Ausmaß noch nicht gestellt hat.

Grundrechtschutz der Betroffenen

Das Recht auf informationelle Selbstbestimmung, so das Gericht, geht über den Schutz der Privatsphäre hinaus. „Es gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen ... Es flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem es ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen lässt. Eine derartige Gefährdungslage kann bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, insbesondere wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden können, die der Betroffene weder überschauen noch verhindern kann. Der Schutzumfang des Rechts auf informationelle Selbstbestimmung beschränkt sich dabei nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden. Auch der Umgang mit personenbezogenen Daten, die für sich genommen nur geringen Informationsgehalt haben, kann, je nach dem Ziel des Zugriffs und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben.“[4]

Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.

Fassen wir zusammen: Mit seiner Postulierung eines Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme hat das Bundesverfassungsgericht das 1983 ausgesprochene Recht auf informationelle Selbstbestimmung erheblich ausgeweitet. Dies hat Konsequenzen auch für die Arbeitswelt.

4. Konsequenzen für die Arbeitswelt

Persönliche Daten im betrieblichen Umfeld

Wie wenig sich noch Dienstliches und Privates trennen lässt, macht ein Blick auf die heute übliche betriebliche Verarbeitung personenbezogener Daten deutlich. Dies beginnt schon bei der – zunehmend elektronisch abgewickelten – Bewerbung, bei der viele handelsübliche Systeme den Vorgang des Löschens schlicht nicht mehr kennen und für unbestimmte Zeiten die Daten gespeichert halten. In vielen Fällen wandert eine Auswahl der Bewerbungsdaten in einen so genannten Talent Pool, um sie für spätere Verwendungen verfügbar zu halten. Die

[4] BVerfG v. 27.2.2008 – 1 BvR 370/07, Absatz-Nr. 198, vgl. NJW 2008, 822

Personalsysteme, zumindest der größeren Unternehmen, speichern in ihren Stammdaten Angaben über Schulbildung, berufliche Ausbildung und bisherige Tätigkeiten, oft einschließlich der Angaben über Vorarbeitgeber. In den Bewegungsdaten der Systeme findet man bei entsprechender Systemausstattung des Arbeitgebers die komplette Historie der angefallenen Fort- und Weiterbildungsmaßnahmen. Verfügt das Unternehmen über ein elektronisch unterstütztes Arbeitszeitmanagement, so kommen die Arbeitszeitdaten hinzu: Tägliches Kommen und Gehen, die Pausen, die Urlaube, die Krankheitszeiten und sonstige „Fehlzeiten". Unternehmensparkplätze mit elektronisch gesteuerten Schranken halten auch noch das Ankommen und Verlassen der Parkplätze fest, denn die Schranke öffnet und schließt sich nur nach Lesen eines gültigen Betriebsausweises, was dank Transpondersteuerung berührungslos geht.

Das führende SAP-Personalsystem Human Capital Management (HCM) zum Beispiel bietet darüber hinaus Platz für die jährlichen Mitarbeiterbeurteilungen, für mit den Mitarbeiterinnen und Mitarbeitern vereinbarte Ziele und deren Zielerreichung. Module zum Kompetenzmanagement ergänzen diese Datensammlungen um Informationen über die Fähigkeiten und Fertigkeiten der Beschäftigten, ihre so genannten Skills, oft in einer Granularität, die Hunderte von Ausprägungen umfasst. Alles das lässt sich als Selbsteinschätzung und Fremdeinschätzung (Beurteilung durch die Führungskraft) gegenüberstellen, kann ein Berufsleben lang gespeichert und nach unterschiedlich feinen *Skill Level* bewertet werden. In den Systemen festgehaltene Qualifikationen beschränken sich keinesfalls auf fachliches und methodisches Wissen. Im Zentrum heute üblicher Systemeinführungen stehen vielmehr die *Social Skills,* wobei Vorgesetzte dann die Teamfähigkeit, die Kommunikations- und Konfliktfähigkeit, die Ziel- und Ergebnisorientierung, Lernbereitschaft oder auch die „kreative Problemlösungskompetenz" ihrer Untergebenen zu beurteilen haben, alles „weiche Faktoren", für die es kaum objektive Messkriterien geben dürfte. Ein Ausdruck der in den Systemen hinterlegten Kataloge umfasst oft viele DIN-A4-Seiten.

Digitale Telefonanlagen registrieren die Verbindungsdaten der Telefonate, Mobilfunkprovider schicken der Firma auf Wunsch Einzelverbindungsnachweise und darüber hinaus zahlreiche Statistiken über die Nutzung der Telefonie. Betreibt das Unternehmen ein Service Center, so sorgt die ACD-Anlage (Automatic Call Distribution) für weitere Details. Statistisch aufbereitet erhält man Informationen über die Zahl der Gespräche pro Kopf und Tag, die durchschnittliche Gesprächsdauer, die Ausreißerdaten für das kürzeste und längste Gespräch, ja sogar Angaben über die *ringing time,* die Zeit, die der *Service Center Agent* vom ersten Klingelzeichen bis zur Annahme des Gesprächs gebraucht hat.

Computerbetriebssysteme halten jedes Login mit Zeit- und Namensstempel fest. Anwendungssysteme führen ein Transaktionslog, aus dem hervorgeht, wer wann welche Programmfunktion aufgerufen hat. Bei der Nutzung des Internets fallen Daten über E-Mails und das Surfverhalten an. Jede Seite, die ein Benutzer aufgerufen hat, hinterlässt ihre Spur. Das Protokoll über die Surfaktivitäten der Benutzer hält nicht nur die aufgerufenen Seiten fest, sondern auch weitere Parameter, die man eingegeben hat, z. B. die Suchwörter, nach denen man „gegoogelt" hat. Schnell verirrt man sich da bei einer Recherche auf Umwege und Irrwege, und schon hat man den Tugendpfad der dienstlichen Nutzung verlassen.

Immer mehr Arbeitsplätze werden durch Videokameras überwacht, die sich rundum drehen lassen und das Objekt ihrer Überwachung heranzoomen können; die modernsten davon verfügen bereits über eine Gesichtserkennung mit automatischer Alarmauslösung, wenn eine als missliebig gespeicherte Person den Erfassungsradius der Kamera betritt. Bewegungen in Lagern können durch RFID-gesteuerte Einrichtungen festgehalten werden.

Unter der Überschrift Enterprise 2.0 oder Web 2.0 werden die neuesten Errungenschaften der Internettechnologien diskutiert, die Unternehmen insbesondere unter dem Stichwort *Social Networking* interessieren. Hier sollen sich die Beschäftigten selbst darstellen, mit ihren Kommunikationsdaten, mit Bild, ihren Hobbies und vor allem ihren besonderen Kenntnissen und Interessen, damit die Kontaktaufnahme untereinander gefördert wird.

Wenn man diese – in den kommenden Jahren sicher noch steigende – Datenflut betrachtet, so sieht man, dass eine Trennung der Daten in „dienstlich" und „persönlich" immer schwieriger wird und eine Verwischung der Grenzen von den Unternehmen nicht nur billigend in Kauf genommen, sondern bewusst gewollt wird. Alle diese Daten stehen in einem für sich betrachtet engen Verwendungszusammenhang, doch in ihrer Verbindung miteinander ergeben sie ein hoch differenziertes Persönlichkeitsbild.

Fast immer sind die Daten in relationalen Datenbanken gespeichert. Deren erklärter Zweck besteht aber gerade darin, die Daten unabhängig von ihrer konkreten Verwendung für beliebige spätere – also heute noch nicht bekannte – Verarbeitungszwecke vorzuhalten. Hier liegt ein schwer lösbarer Zielkonflikt, denn für die Verarbeitung personenbezogener Daten gilt das Gebot strikter Zweckbindung, das eine Datenhaltung „auf Vorrat" ausschließt.

Relationale Datenbanken glänzen durch das weitere Leistungsmerkmal, ungefähr alles miteinander verbinden zu können. Dies erschwert die Festlegung von Daten für bestimmte Verwendungszwecke beachtlich.

Schluss-folgerung

Als Fazit lässt sich festhalten,

- dass die Flut der in einem Unternehmen über jeden Beschäftigten gesammelten Daten unaufhaltsam weiter steigt,
- dass die heute verfügbaren Techniken die Verbindung dieser unterschiedlichen Daten untereinander begünstigen und
- dass es eines differenzierten Systems von Regelungen bedarf, um die Persönlichkeitsrechte der Mitarbeiterinnen und Mitarbeiter zu schützen, allein schon um sicherzustellen, dass gewisse Daten nur in einem definierten Verwendungszusammenhang genutzt werden dürfen und darüber hinaus nicht zugänglich sind.

5. Der Verhältnismäßigkeitsgrundsatz

Die im letzten Absatz geschilderten Beispiele zeigen, wie umfangreich und wie detailliert die Sammlungen über persönliche Daten sind, über die Arbeitgeber heute verfügen. Die dahinter stehenden Interessen kann man nun keineswegs durchgehend als verwerflich bezeichnen. In vielen Fällen sind sie begründet und können sogar weitgehend mit den Interessen der Beschäftigten übereinstimmen. Doch dabei handelt es sich fast immer um eng begrenzte Verwendungszusammenhänge. Leider ist die Technik in der Lage, diese Grenzen beliebig aufzuheben und die verschiedenartigen Daten herausgelöst aus ihrem ursprünglichen Kontext unter völlig anderen Gesichtspunkten zu betrachten und miteinander zu verbinden.

Das Bestehen eines Arbeitsverhältnisses zwingt den Arbeitgeber zur Erfassung und Verarbeitung einer Menge von persönlichen Daten der Beschäftigten. Allein schon damit er seinen Beschäftigten Löhne und Gehälter zahlen kann, braucht er eine Reihe von Informationen. Darin liegt ein Eingriff in das Grundrecht der informationellen Selbstbestimmung, dem ein Beschäftigter beim Eintreten in ein Arbeitsverhältnis zustimmen muss.

Wenn aber Grundrechte eingeschränkt werden, so ist dies in einem Rechtsstaat nur unter Einhaltung von Regeln möglich. Eine davon ist der Verhältnismäßigkeitsgrundsatz. Bezogen auf die Verarbeitung personenbezogener Daten bedeutet dies, dass die durch die Verarbeitung bedingte Einschränkung des Grundrechtes der informationellen Selbstbestimmung abzuwägen ist gegen den hinter der Einschränkung stehenden Zweck und so gering wie möglich auszufallen hat. Wir können diese Anforderung auch als Gebot zum sparsamen Umgang mit personenbezogenen Daten bezeichnen.

Notwendige Abwägungen

Konkret für die Verwaltung des Arbeitsverhältnisses bedeutet dann der Verhältnismäßigkeitsgrundsatz, dass nur so viele Daten, wie zur Erfüllung des Zwecks unbedingt erforderlich sind, erfasst und verar-

beitet werden dürfen. Klar, dass wir hier eine Grauzone betreten, in der Ermessensurteile zu treffen sind:

- Welche Daten sind unbedingt nötig?
- Wie viel zusätzlichen Komfort möchte der Arbeitgeber haben?
- Rechtfertigt dies die Erhebung zusätzlicher persönlicher Daten?
- Lässt sich der Umgang mit diesen zusätzlichen Daten auf den ursprünglichen Verwendungszweck verlässlich eingrenzen?

Auch bei der Beantwortung dieser Fragen sind die Urteile des Bundesverfassungsgerichts aus dem Jahr 2008 hilfreich. In seinem Urteil über die geplanten Online-Zugriffe des nordrhein-westfälischen Verfassungsschutzes hat sich das Gericht ausführlich mit dem Verhältnismäßigkeitsgrundsatz befasst und an vielen Punkten den geplanten Gesetzestext als zu unpräzise gerügt. Es hat zum Beispiel festgestellt, dass eine Verletzung der Vertraulichkeit der in den Computern gespeicherten persönlichen Daten nur dann zulässig ist, wenn es „tatsächliche Anhaltspunkte“ dafür gibt, dass eine „konkrete Gefahr für ein überragend wichtiges Rechtsgut“ besteht wie „Leib, Leben und Freiheit der Person“ oder „Güter der Allgemeinheit“, deren Bedrohung die Grundlagen des Staates oder der Existenz der Menschen berühren, wie z. B. die Funktionsfähigkeit „existenzsichernder öffentlicher Versorgungseinrichtungen“.

Dies steht für das im Verhältnis zu den genannten Dingen sicher schlichte Thema Arbeitsverhältnis alles nicht zur Debatte, aber man darf vermuten, dass strenge Maßstäbe anzulegen sind, wenn es um die Interpretation geht, wo die Grenzen der Verhältnismäßigkeit überschritten werden. Kämen gängige Praktiken der Unternehmen auf den richterlichen Prüfstand, wie zum Beispiel die Tatsache, dass unter dem Vorwand des Registrierens verwendeter Softwarelizenzen in personenbezogener Form jedweder Aufruf eines Programms und die Dauer der Programmnutzung erfasst wird und die Betroffenen dies noch nicht einmal wissen, so kann man hier sicher geltend machen, dass mit dem Verhältnismäßigkeitsgrundsatz recht stiefmütterlich umgegangen wurde.

6. Datenschutz und Mitbestimmung

§ 87 Abs. 1 Nr. 6 BetrVG

Die Datenschutzgesetze definieren *allgemeine Schutznormen*, deren Umsetzung im konkreten Fall der *Interpretation* bedarf. Die diesen Gesetzen zugrunde liegende Idee vom Schutz der Persönlichkeitsrechte findet sich jedoch auch im Betriebsverfassungsgesetz. Der bereits erwähnte § 75 BetrVG verweist mit seiner Verpflichtung zur Wahrung der Würde des Menschen im Arbeitsleben auf das Grundrecht der informationellen Selbstbestimmung. Deutlicher ausgestal

findet sich dies in der Formulierung des § 87 Abs. 1 Nr. 6 BetrVG, in der dem Betriebsrat ein Mitbestimmungsrecht eingeräumt wird beim Einsatz „technischer Einrichtungen, die dazu bestimmt sind, Leistung und Verhalten der Arbeitnehmer zu überwachen“.

Wir wollen hier nicht die leidvolle Geschichte des Streits um die Mitbestimmung bei diesem Paragrafen aufrollen, sondern kurz und bündig den – seit 1984 geltenden – Stand der Auslegung dieses Mitbestimmungsrechts durch das Bundesarbeitsgericht wiedergeben:

- Im Sinne des Gesetzes ist eine technische Einrichtung dann zur Überwachung bestimmt, wenn sie dazu objektiv geeignet ist. Es kommt nicht auf die subjektive Absicht des Arbeitgebers an.

- Eine objektive Eignung zur Überwachung liegt dann vor, wenn die technische Einrichtung Daten erfasst oder verarbeitet, die Aussagen über Leistung oder Verhalten der Arbeitnehmer zulassen, die sich auf einzelne Arbeitnehmer oder kleinere Arbeitnehmergruppen beziehen.

Der Ausdruck „technische Einrichtung“ mag verwundern. Doch er stammt aus einer Zeit, in der Computer im Arbeitsleben nur im Hintergrund als große Zentralrechner eine Rolle spielten. Im Jahr 1972 kam die Regelung ins Betriebsverfassungsgesetz und war eigentlich für Fernsehkameras, Produktographen oder Fahrtenschreiber gedacht. Zu diesem Zeitpunkt waren Personal Computer noch nicht einmal erfunden.

Der Filter „Schutz vor Überwachung“ verengt die Sicht auf das Persönlichkeitsrecht, doch spielt dies in der Praxis kaum eine Rolle, weil fast alle differenzierteren persönlichen Angaben Aussagen zumindest über das Verhalten der betroffenen Personen zulassen und damit die Tatbestandsvoraussetzungen der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG gegeben sind.

§ 87 Abs. 1 Nr. 6 BetrVG stellt also die elektronische Verarbeitung personenbezogener Arbeitnehmerdaten unter Regelungspflicht, wobei die genannten Voraussetzungen zu beachten sind. Es handelt sich um ein sehr starkes Mitbestimmungsrecht, denn bei Nichteinigung der Betriebsparteien hat die Einigungsstelle das letzte Wort.

Beispiel

Wir wollen dies an einem Beispiel verdeutlichen. Ein Firmenparkplatzverwaltungssystem, das nur Mitarbeiternamen und PKW-Kennzeichen verarbeitet, sagt sicher nichts über Leistung oder Verhalten der betroffenen Personen, sehen wir einmal von der Spitzfindigkeit ab, dass bereits die Information über den Besitz eines Autos eine Aussage über das Verhalten der betroffenen Person darstellt. Der Arbeitgeber hätte gute Chancen, in einer gerichtlichen Auseinandersetzung feststellen zu lassen, dass sein Betriebsrat beim Einsatz eines solchen Systems kein Mitbestimmungsrecht hat.

Wird das System aber erweitert um die Bewegungsdaten der Autos auf dem Parkplatz, also das mit dem Öffnen oder Schließen der Schranke registrierte Kommen oder Gehen, so ändert sich das Bild. Jetzt werden Aussagen über das Verhalten der betroffenen Personen möglich.

Wir schätzen, dass 95 Prozent und mehr der eingesetzten Softwaresysteme die Tatbestandsvoraussetzungen der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG erfüllen. Heutzutage muss man sich in fast jedes System persönlich einloggen. Die meisten Systeme speichern in jedem angelegten oder bearbeiteten Datensatz das Kennzeichen des Benutzers und sorgen somit dafür, dass die Arbeit mit dem Computer überwachbar wird.

Wie wir bereits im Abschnitt „Konsequenzen für die Arbeitswelt“ beschrieben haben, umfasst die Sammlung persönlicher Daten ein wachsendes breites Spektrum von Themen und verliert immer mehr die Unterscheidbarkeit zwischen Dienstlichem und Persönlichem. Sie berührt also die Persönlichkeitsrechte der Arbeitenden. Unter Wahrung des Persönlichkeitsschutzes eine Abwägung zu treffen zwischen den Interessen des Unternehmens und der betroffenen Arbeitnehmer, ist Aufgabe der Mitbestimmung aus § 87 Abs. 1 Nr. 6 BetrVG.[5] Was dies konkret bedeutet, werden wir in den nächsten Kapiteln detailliert ausführen.

[5] Die hier auf die Betriebsräte bezogenen Aussagen treffen natürlich in nahezu gleichem Umfang für die Personalräte zu, da die Personalvertretungsgesetze alle ähnliche Formulierungen wie § 87 Abs. 1 Nr. 6 BetrVG enthalten.

II. Personaldaten

1. Grundlagen

Wie die einleitenden Überlegungen gezeigt haben, schützt kein Gesetz mit klaren Erlaubnis- und Verbotsvorschriften die Persönlichkeitsrechte der Beschäftigten. Das Datenschutzrecht markiert lediglich allgemeine Grundsätze, die zu beachten sind. Und das Betriebsverfassungsrecht gibt den Betriebsräten mit der Mitbestimmung aus § 87 Abs. 1 Nr. 6[6] eine Verhandlungsmacht, Regelungen zum Schutz der Persönlichkeitsrechte notfalls durch Spruch der Einigungsstelle erzwingen zu können.

Das klassische Feld der Auseinandersetzung um diese Mitbestimmung war die Personaldatenverarbeitung, genauer gesagt waren es die Personalinformationssysteme, ein Streit, der bis in die späten 70er-Jahre des letzten Jahrhunderts zurückreicht. Ein Werbespot des damals führenden Systems PAISY, „Da können Sie auf Anhieb Ihre kranken Türken sehen“, brachte Betriebsräte und Gewerkschaften in Harnisch.

Als dann endlich – ausgerechnet im Orwell-Jahr 1984 – die Mitbestimmung beim Einsatz von Computersystemen vom Bundesarbeitsgericht hinreichend klar definiert worden war, gab es eine wahre Flut von Betriebsvereinbarungen zu dem Thema. Sie folgten alle einem einfachen Input-Output-Schema. Der Input sind die im System gespeicherten Personaldaten. Sie wurden in Form eines Datenkatalogs als Anlage zur Betriebsvereinbarung festgelegt. Was innendrin im System geschah, war nicht von Interesse. Spannend wurde es erst wieder beim Output, bei den Auswertungen, die aus dem System herauskamen. Sie wurden in einem Ausgabenkatalog festgehalten.

Bei den in den Systemen gespeicherten Daten gab es hauptsächlich Streit um die Fehlzeiten, aber auch Leistungsgrad-Daten bei Akkordarbeit und – damals noch relativ selten – bei Daten über die Beurteilung von Arbeitnehmern.

Die Regelung der Ausgaben erfolgte meist nach dem von uns so genannten „Drei-Haufen-Prinzip“. Oft saßen Betriebsräte und ihre damals noch seltenen Sachverständigen vor einem Berg von Auswertungsmustern und schichteten sie in drei verschiedene Papierhaufen: Ganz links die für unbedenklich gehaltenen Auswertungen, die, „Gott

[6] Für diejenigen unter den Leserinnen und Lesern, die erst hier mit der Lektüre dieses Buches beginnen, erinnern wir daran, dass § 87 Abs. 1 Nr. 6 BetrVG festlegt, dass der Betriebsrat mitzubestimmen hat „bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, Leistung und Verhalten der Arbeitnehmer zu überwachen“.

sei's gedankt", meist 90 und mehr Prozent des gesamten Volumens ausmachten, ganz rechts diejenigen Auswertungen, die man entweder überhaupt nicht oder zumindest nicht in der beabsichtigten Form haben wollte, und in der Mitte die Dinge, die man einfach nicht verstand, meist wegen nur schwer enträtselbaren Abkürzungen. Nachdem der Arbeitgeber dann weitere Erklärungen geliefert hatte, löste sich der mittlere Haufen ganz schnell nach links oder rechts auf. Um die wenigen rechts liegen bleibenden Muster wurde dann heftigst gestritten, oft bis in die Einigungsstelle hinein.

Aber die Systeme besaßen noch eine andere Eigenart, die damals den Unterschied zwischen Personalabrechnungs- und Personalinformationssystem ausmachte: das eingebaute Info-System. Bei PAISY hieß diese Systemkomponente PAISY-Info, eine Abfragesprache, mit der man beliebige, nicht durch fertige Programme festgelegte Auswertungen machen konnte. Betriebsräte fragten sich, was die ganze Mühe denn Wert war, in zähen Verhandlungen Auswertung für Auswertung einzeln festzulegen, wenn sich ein Personalreferent (seltener ein Personalchef, denn diese ließen lieber arbeiten) nur vor den Bildschirm setzen brauchte, ein paar Zeilen Befehlscode eingeben musste und dann – vorbei an der mühevollen Mitbestimmung – jede beliebige Auswertung erstellen konnte. Also war klar, dass in den meisten Betriebsvereinbarungen das „Abklemmen" dieser Spontan-Auswertungsinstrumente verlangt und auch durchgesetzt wurde. Etwas technischer ausgedrückt: Der Zugriff auf die Online-Abfrageinstrumente musste gesperrt werden.

„Klassischer" Positivkatalog

Die „klassische" Betriebsvereinbarung zur Personaldatenverarbeitung legte in einem einleitenden Paragrafen kurz den Zweck der Verarbeitung fest, nämlich die Durchführung der Lohn- und Gehaltsabrechnung nebst begleitendem Verwaltungskram (Stammdatenpflege, Bescheinigungen und Meldepflichten, weitere Arbeitgeberleistungen, Übermittlung an die Sozialversicherungsträger usw.) und weitere für konsensfähig befundene Dinge zur Unterstützung der Personalarbeit. Die eigentliche Verarbeitung war dann nach dem Verfahren des „Positiv-Katalogs" in einem System von Anlagen geregelt; die wichtigsten davon waren:

- ein Datenkatalog mit allen für die Verarbeitung erlaubten persönlichen Arbeitnehmerdaten,
- ein Schlüsselverzeichnis, in dem die im System verwendeten verschlüsselten Informationen erklärt wurden,
- als wichtigster Teil der Regelung ein Ausgabenkatalog mit je einem Muster der erlaubten Auswertungen, auf denen oft noch die Häufigkeit der Erstellung und der Verteilerkreis vermerkt waren,

- ein Schnittstellenverzeichnis, in dem zumindest alle Daten, die das System verlassen, aufgeführt wurden und

- ein Verzeichnis der Zugriffsrechte, das Auskunft darüber gab, welcher Personenkreis auf welche Daten und Programmteile zugreifen durfte.

Das Festhalten in einem „Positiv-Katalog“ bedeutete, dass nur die dort genannten Dinge erlaubt waren. Die Arbeitgeber bevorzugten natürlich überwiegend ein Negativverfahren, in dem lediglich festzulegen wäre, was nicht geschehen dürfte – mit der unkalkulierbaren Folge, dass alles, was nicht verboten war, für den Arbeitgeber erlaubt wäre.

In einer typischen Vereinbarung aus der damaligen Zeit folgte dann als entscheidende Regelung die Deaktivierung der Ad-hoc-Abfrageinstrumente (wie damals PAISY-Info, später SAP ABAP-Query), deren Einsatz bestenfalls im nur mit Testdaten arbeitenden Entwicklungssystem für die Entwicklung und das Testen neuer Programmfunktionen erlaubt wurde. Dies geschah dann aber nur mit Testdaten.

Erweiterungen und Veränderungen der Systeme

Weiterhin entscheidend war die Festlegung, dass die Anlagen nur im gegenseitigen Einvernehmen geändert werden konnten, ersatzweise durch Spruch der Einigungsstelle. Neue Daten im System oder neue Auswertungen machten also nicht die Kündigung der ganzen Vereinbarung erforderlich, sondern man musste sich lediglich über die Änderung der entsprechenden Anlage einig werden. Durch diese „Dynamisierung“ des Verfahrens sollte dem Tatbestand Rechnung getragen werden, dass der Computereinsatz eine einem schnellen Wandel unterliegende Technik darstellt. Und die Betriebsräte hatten die Gewähr, dass technische Neuerungen oder Erweiterungen des Funktionsrahmens nicht vorbei an der Mitbestimmung erfolgten – vorausgesetzt die Arbeitgeberseite hielt sich an die Regelung.

2. Überalterte Regelungen

Ein Personalsystem der 1980er-Jahre kam in der Regel mit rund dreihundert verschiedenen Daten zur Person aus. Das heute, im Jahr 2008 führende System SAP Human Capital Management (HCM) – den meisten Lesern sicher bekannter unter seinem früheren Namen Human Resources (HR) – bietet über viertausend Datenfelder zur Speicherung persönlicher Daten.

Wir erinnern uns an eine denkwürdige Sitzung mit einem Betriebsrat, bei der es um die „Modernisierung“ einer Vereinbarung zu einem Personalinformationssystem ging. Die Anlage „Ausgabenkatalog“ bestand aus über 300 Hängeordnern, die zwei Schränke füllten. Der Betriebsrat hatte die Beschäftigung mit diesem Regelwerk an einen Ausschuss delegiert, dessen Mitglieder sich in jeder Betriebsratssitzung eine Abfuhr holten, wenn sie das System zum Thema machen

wollten. Sie sollen doch das Gremium in Ruhe lassen, war die nicht ausgesprochene einhellige Meinung, sie hatten ja schließlich ihren Ausschuss. Die betroffenen Kolleginnen und Kollegen fühlten sich in den politischen Windschatten abgeschoben. So konnte es also nicht weitergehen. Andere Verfahren mussten her, bei denen der Kern des Problems, nämlich der Schutz der Persönlichkeitsrechte, wieder vom regelungstechnischen Moltofill befreit wurde.

3. Neuere Regelungskonzepte

Zu der überwiegenden Mehrzahl der von den Unternehmen gewünschten Auswertungen fiel einem ohnehin kaum mehr ein, als dass sie unnötig waren, aber wo sie die Persönlichkeitsrechte verletzten, war auch nicht klar. Streit entstand immer nur um wenige Daten. Deshalb bildete sich dann in den 1990er Jahren ein Verfahren heraus, das hauptsächlich aus Gründen der Arbeitsökonomie erfunden wurde, nämlich die Festlegung der Auswertungen und das Verbot der Online-Abfrageinstrumente auf besonders überwachungsgeeignete Daten zu begrenzen. Deshalb findet man in vielen neueren Betriebsvereinbarungen Regelungen wie:

Daten, die Informationen über

- das Arbeitszeitverhalten einschließlich Fehlzeiten und Mehrarbeit,
- Beurteilungen,
- leistungsabhängige Entgeltbestandteile, vereinbarte Ziele und Zielerreichungen,
- Pfändungen und Mitarbeiterdarlehen,
- Details der Qualifizierung, Fähigkeiten und Fertigkeiten (Skills),
- Verhalten und Tätigkeiten außerhalb des Unternehmens und
- die Gesundheit

der Mitarbeiterinnen und Mitarbeiter beschreiben, gelten wegen ihrer hohen Überwachungseignung als besonders schutzwürdig im Sinne dieser Vereinbarung. Ihre Verarbeitung wird daher an weitere, im Folgenden näher beschriebene Regelungen gebunden.

Nur für diese Datengruppen wurden dann in der Betriebsvereinbarung weiter einschränkende Regelungen festgelegt, z. B. dass nur fest programmierte Auswertungen erlaubt wurden, die – wie in früheren Zeiten – in einem Ausgabenkatalog dokumentiert waren und dass auf solche Daten nicht mit Hilfe der berüchtigten Online-Abfrageinstrumente zugegriffen werden durfte.

Die Aufzählung der Datengruppen lässt schon erkennen, dass sich der Einsatzumfang der Systeme gegenüber den Anfangszeiten in den 1970er-Jahren gründlich erweitert hatte. Das Arbeitszeitverhalten mit dem besonderen Schwerpunkt Fehlzeiten rückte immer mehr aus dem Fokus zu Gunsten von Themen, die vor allem den Bereich der Personalentwicklung betreffen.

Initiativrecht

Man weiß nun nie, ob man durch die Aufzählung „besonders schutzwürdiger Daten“ alle unter dem Überwachungsgesichtspunkt relevanten Daten im Visier hat. Deshalb enthalten neuere Betriebsvereinbarungen immer einen Passus, der das Initiativrecht des Betriebsrats besonders hervorhebt und die Mitbestimmung sozusagen auf „unverbraucht“ stellt, wie das folgende Beispiel zeigt:

> Bei anstehenden Erweiterungen prüfen beide Seiten, ob die Bestimmungen dieser Vereinbarung eingehalten sind. Ist dies nach Auffassung einer Seite nicht der Fall, so nehmen beide Seiten Verhandlungen auf mit dem Ziel einer einvernehmlichen Regelung.
>
> Änderungen der Anlagen … bedürfen des Einvernehmens zwischen Arbeitgeber und Betriebsrat.
>
> Macht der Betriebsrat geltend, dass die Anwendung des Systems sich zwischenzeitlich verändert hat oder dass sich neuer Regelungsbedarf bezüglich des Schutzes der Persönlichkeitsrechte (im Sinne von § 87 Abs. 1 Nr. 6 BetrVG) ergibt, so hat er das Recht, ergänzende Regelungen zu dieser Betriebsvereinbarung zu verlangen. Über diese ist ebenfalls Einvernehmen zu erzielen.
>
> Kommt in den Fällen, in denen diese Vereinbarung das Einvernehmen beider Seiten vorsieht, eine Einigung nicht zu Stande, so entscheidet eine gemäß § 76 Abs. 5 BetrVG zu bildende Einigungsstelle.

Sollte nun wirklich beim Abschluss der Vereinbarung eine Gefahrenquelle übersehen worden sein, so löst dies keinen bleibenden Schaden aus. Der Betriebsrat kann aufgrund der zitierten Regelung ergänzenden Regelungsbedarf geltend machen, und der Arbeitgeber muss mit ihm darüber verhandeln. Kommt keine Einigung zu Stande, so hat eine verbindlich entscheidende Einigungsstelle[7] das letzte Wort.

Der entscheidende Vorteil des Verfahrens besteht in der Konzentration der Betriebsvereinbarung auf die wesentlichen Punkte. Nach dem

[7] Hier ist der Verweis auf § 76 Abs. 5 BetrVG wichtig. § 76 BetrVG regelt zwei verschiedene Einigungsstellen. In Nr. 5 geht es um die Einigungsstelle bei Themen der erzwingbaren Mitbestimmung; hier ist der Spruch der Einigungsstelle bindend. Abs. 6 regelt eine freiwillige Einigungsstelle, deren Spruch nur eine Empfehlung an die Arbeitgeberseite darstellt.

alten Verfahren hatte man sich mit dem weit umfangreicheren anderen Teil der Systeme herumzuschlagen, bei dem unter dem Gesichtspunkt der Wahrung der Persönlichkeitsrechte keinerlei Regelungsbedarf erkennbar war. Der zweite Vorteil ist die Unverbrauchtheit der Mitbestimmung. Nach dem Betriebsverfassungsgesetz ist mit Abschluss einer Vereinbarung die entsprechende Mitbestimmung erschöpft oder – umgangssprachlich ausgedrückt – verbraucht. Die genannte Regelung hält eine erneute Mitbestimmung offen, wenn der Betriebsrat regelungsbedürftige Änderungen geltend macht.

Diese Regelung hat durchaus auch Vorteile für die Arbeitgeberseite, denn sie lockert die Verhandlungsatmosphäre. Ohne eine solche Öffnung muss ein Betriebsrat peinlich genau darauf bedacht sein, keine Gefahrenquelle zu übersehen, was zur Folge hat, dass die Dinge mit verschärftem Misstrauen betrachtet werden. Man schaut auf das System und hat immer das „worst case scenario“ im Blick. Die „Dynamisierung“ der Mitbestimmung durch die Initiativ-Klausel befreit von dieser Blickverengung, denn selbst, wenn man wichtige Dinge vergessen hat, kann man sie immer noch nachbessern.

Beweisverwertungsverbot

Nicht nur in der Personaldatenverarbeitung, sondern auch bei anderen Themen hat sich eine Regelung bewährt, die meist unter dem Begriff „Beweisverwertungsverbot“ erörtert wird. Sie lässt sich wie folgt formulieren:

Beweisverwertungsverbot

Informationen, die unter Verstoß von Bestimmungen dieser Betriebsvereinbarung gewonnen wurden, dürfen nicht zur Begründung personeller Maßnahmen verwendet werden. Maßnahmen, die auf der Grundlage verfahrenswidrig gewonnener Informationen ausgesprochen wurden, sind zurückzunehmen.

Damit ist die Attraktivität für die Arbeitgeberseite, sich unter Umgehung von Regelungen einer Betriebsvereinbarung Beweismaterial zu verschaffen, deutlich abgesenkt, und der Betriebsrat kann die Rücknahme der Maßnahmen notfalls gerichtlich durchsetzen.

Das Bundesarbeitsgericht hat sich allerdings in einer Entscheidung aus dem Dezember 2007 kritisch mit dem Verwertungsverbot von gegen Bestimmungen einer Betriebsvereinbarung gewonnenen Beweismitteln auseinandergesetzt.[8] In dem Fall ging es jedoch nicht um Computerfragen, sondern um eine fristlose Kündigung, die nach einer unter Verletzung von Bestimmungen der Betriebsvereinbarung durchgeführten Taschenkontrolle ausgesprochen wurde. Das BAG folgte der Auffassung nicht, dass eine personelle Maßnahme allein schon deswegen

[8] BAG, Urteil vom 13.12.2007 – 2 AZR 537/06

rechtsunwirksam sei, weil die Bestimmungen einer Betriebsvereinbarung nicht beachtet wurden. Es sei vielmehr Sache des Gerichts, im Einzelfall zu prüfen, ob und welche Beweismittel es in einem Verfahren zulässt. Anders formuliert: Wenn ein Unternehmen unter Verstoß gegen eine Vereinbarung Beweismittel in einen Prozess einbringt, kann dies vom Gericht nicht im Vorhinein ignoriert werden. Gleichwohl muss das Gericht abwägen, ob der Verstoß des Arbeitgebers unter Würdigung aller Umstände die möglichen Verletzungen der Persönlichkeitsrechte der Beschäftigten rechtfertigt.[9]

Das BAG lässt ausdrücklich offen, ob die Betriebsparteien nicht die Möglichkeit haben, explizit Regelungen bezüglich der Verwertbarkeit von Informationen zu treffen, die entgegen vereinbarter Verfahren gewonnen wurden. Verstößt der Arbeitgeber dann gegen diese Vereinbarung, so ist er in diesem Fall aufgrund der unmittelbaren und zwingenden Wirkung der geltenden Betriebsvereinbarung daran gehindert, eine individualrechtliche Maßnahme mit der mitbestimmungswidrig erlangten Information zu begründen. Damit käme es dann auf eine prozessualrechtliche Verwertbarkeit nicht mehr an.[10] Wir raten also dringend, in Betriebsvereinbarungen zu überwachungsgeeigneten IT-Systemen die vorgeschlagene Klausel zum Verwendungsverbot vereinbarungswidrig gewonnener Informationen aufzunehmen. Ein idealer Ort für eine solche Klausel ist natürlich eine Rahmenvereinbarung für IT-Systeme. Dann würde die Notwendigkeit entfallen, die Regelung für jedes Einzelsystem zu wiederholen.

Kritik verdient allerdings die Auffassung des BAG, allein durch § 23 BetrVG habe der Betriebsrat genügend Sanktionsmittel an der Hand, sich gegen mitbestimmungs- oder vereinbarungswidrig erlangte Informationen zur Wehr zu setzen, Es kann nicht angehen, dass ein Arbeitgeber bewusst Maßnahmen zum Schutz des allgemeinen Persönlichkeitsrechts der Arbeitnehmer umgehen kann, um die vereinbarungswidrig gewonnenen Informationen dann zu seinen Gunsten verwenden zu dürfen.

4. Neue Themenfelder

Wie im Verlaufe dieses Buchs noch ausführlich dargestellt wird, haben sich die Problemfelder der Mitarbeiterüberwachung mittlerweile deutlich verschoben, so dass heutzutage die klassische Personaldatenverarbeitung nur noch eine untergeordnete Rolle spielt. Aber auch innerhalb der Personaldatenverarbeitung gibt es neue Akzente. Sie liegen vor allem in Themen, die früher von der Computerunterstützung verschont blieben. Ein Blick auf das Leistungsspektrum des heute in

[9] Im zitierten Urteil verweist das BAG darauf, dass die Taschenkontrolle mit Einverständnis der gekündigten Mitarbeiterin vorgenommen worden sei. Es hält ausdrücklich offen, wie Sachverhalte zu würdigen sind, in denen eine solche ausdrückliche Zustimmung nicht erfolgt ist.

[10] Vgl. Lerch, Sascha, Lars Weinbrenner in AuR 11/2008, S. 401.

Deutschland führenden Systems SAP HCM (Human Capital Management) macht dies ersichtlich. Das Spektrum umfasst:

Beispiel SAP

- Die Payroll-Funktion, auf deutsch die klassische Lohn- und Gehaltsabrechnung, um die es in den letzten drei Jahrzehnten kaum Auseinandersetzungen gab,
- die Personaladministration zur Unterstützung der Tagesaufgaben einer Personalverwaltung (Stammdatenverwaltung, Bescheinigungs- und Meldewesen, Arbeitgeberleistungen usw.),
- das Zeitmanagement mit Subsystemen für die unterschiedlichsten Formen der Arbeitszeitverwaltung,
- das Workforce Deployment-Modul, zu deutsch Personaleinsatzplanung, zur Unterstützung von Projektplanung und Projektmanagement und einem ausführlichen Berichtswesen über die Rentabilität des Personaleinsatzes,
- das Organisationsmanagement mit einer Abbildung der Aufbauorganisation des Unternehmens bis hin zu Stellenbeschreibungen und selbstverständlich der Zuordnung der Stellen zu Personen,
- das Travel Management, früher bescheidener Reisekostenabrechnung genannt,
- das Veranstaltungsmanagement, unter dessen etwas irreführendem Namen sich die Verwaltung aller Qualifizierungsmaßnahmen der Beschäftigten verbirgt,
- das Kompetenz- oder Skillmanagement, in dem fachliche, methodische und soziale Kompetenzen der Mitarbeiterinnen und Mitarbeiter verarbeitet werden,
- das Performance Management, in dem man Mitarbeitergespräche, Mitarbeiterbeurteilungen, Zielvereinbarungen und Zielerreichungen und deren Verknüpfung mit der Entgeltfindung bearbeiten kann,
- das e-Recruitment-Modul, auf deutsch die Personalbeschaffung, mit der Möglichkeit, Bewerbungen auch online über das Internet abzuwickeln,
- die Nachfolgeplanung mit Entwicklungsplänen zur Vorbereitung auf Führungsrollen und Schlüsselpositionen.

Hier handelt es sich um eine Aufzählung, die keine Vollständigkeit beansprucht und die von kurzer Halbwertzeit ist: In wenigen Monaten können die Programmpakete bereits mit anderen Etiketten erscheinen und sich um neue Merkmale vermehrt haben.

Regelungs-aspekte

Wir können auf die erforderlichen Regelungen zum Schutz der Persönlichkeitsrechte an dieser Stelle nicht näher eingehen – dies wäre Stoff für ein eigenes Buch. Ungefähr jedes der genannten Subsysteme erfordert eine Regelung in einer eigenen Vereinbarung (oder als Anhang zu einer Rahmenvereinbarung zum Personalmanagement). Wir begnügen uns mit einigen Hinweisen:

- Beim Zeitmanagement muss man zwischen Positiv- und Negativerfassung unterscheiden. Eine Positiverfassung ist zwingend nur bei Gleitzeit erforderlich. Hier wird das tatsächliche tägliche Kommen und Gehen erfasst. Die Regelungen konzentrieren sich auf die erlaubten Auswertungen und auf die Zugriffsrechte, vor allem auf die Frage, wer die Details des Arbeitszeitverhaltens zu sehen bekommt.

- Im Kompetenz- oder Skill-Management sollte man das Erfassen so genannter sozialer Skills (Teamfähigkeit, Kommunikationsfähigkeit, Konfliktfähigkeit usw.) ausschließen; diese lassen sich nicht objektiv messen, sondern bestenfalls subjektiv beurteilen. Und solche Inhalte sollten nicht in einem Datenbanksystem universell verfügbar gemacht werden. Weitere Probleme betreffen die Freiwilligkeit der Angaben, die (zu vermeidende) Unterscheidung zwischen Selbst- und Fremdeinschätzung, Auswertungen mit dem Charakter der Rastersuche nach geeigneten Personen für bestimmte Arbeitsplätze und natürlich die Zugriffsrechte.

- Das Performance-Management greift ebenfalls tief in die Subjektivität des Verhältnisses zwischen Mitarbeiterin bzw. Mitarbeiter und Führungskraft ein, insbesondere wenn es sich um ein Zielmanagement mit Beurteilung der Zielerreichung handelt. Wir vertreten nachhaltig den Standpunkt, dass die Ergebnisse solcher Verfahren am besten in Papierform aufgehoben sind, also in Dokumenten, die bei den Personen bleiben, die der Vorgang angeht. Ein elektronisches System darf dann lediglich überwachen, ob die vorgesehenen Gespräche stattgefunden haben und die Termine eingehalten wurden.

Wie gesagt, die hier angesprochene Materie liefert Stoff für ein eigenes Buch. Die entsprechenden Systeme erfordern eigene betriebliche Regelungen.[11]

5. Workflows und Self Services

Neben der funktionellen Ausweitung der Personaldatenverarbeitung ist eine Reihe von technischen Veränderungen eine nähere Betrachtung wert. Bleiben wir beim Marktführer-System SAP, so sind hier an erster Stelle die Employee und Manager Self Services zu nennen.

[11] Weiterführende Hinweise unter http://www.tse.de/papiere/personal/.

Self Services für Beschäftigte

Bei den Employee Self Services handelt es sich sozusagen um die Einführung der Selbstbedienung in der Datenverarbeitung. Die Beschäftigten sollen einen Teil ihrer persönlichen Daten selber in das System eingeben, z. B. Änderungen von Adress- oder Kontoverbindungen, aber auch Urlaubsanträge, Anträge für eine Dienstreise, Skizzen für das betriebliche Vorschlagswesen, Stundenaufschreibungen für Projektarbeiten usw. Im Grunde genommen eignet sich alles, was bisher über Formulare abgewickelt wurde, für den neuen Dienst. Als Vorteil für die Arbeitgeberseite wird von den Systemanbietern die Ersparnis vieler Routinearbeiten angepriesen, beispielsweise für die Personalabteilung. Skeptiker dagegen sehen hierin weitere Schritte zur Abschaffung der Personalbereiche, wie wir später noch genauer sehen werden. Schließlich werden keine Arbeiten eingespart, sondern nur verlagert.

Auch die Datenausgabe über das Selbstbedienungssystem ist möglich. Die Beschäftigten können sich jetzt beispielsweise ihre Lohn- oder Gehaltsabrechnung online am Bildschirm ansehen und sich auf Wunsch selber ausdrucken, und das Unternehmen erspart sich die Zusendung per Post. Anfangs löst dieses Verfahren oft gewaltige Irritationen aus, wenn die Bescheinigungen nicht auf den richtigen Druckern landen.

Workflows

Viele dieser Self Services sind mit elektronischen Workflows gekoppelt. Wenn zum Beispiel jemand seinen Urlaub elektronisch beantragt, dann routet (auf Deutsch: leitet) das System den Antrag an den Vorgesetzten, der ihn genehmigen oder ablehnen kann; der Absender erhält dann eine automatische Mitteilung, meist per E-Mail. Diese Fest-Verdrahtung von Arbeitsabläufen nennt man Workflow. Im Softwaresystem ist hinterlegt, über welche Stationen die Arbeit abzulaufen hat. Änderungen an dieser Organisation sind erst dann möglich, wenn man die Computereinstellungen vorher entsprechend geändert hat. Wie sich diese neue Abhängigkeit vom Computersystem mit der allen Ortes propagierten Forderung nach mehr Flexibilität verträgt, bleibt das Geheimnis der Workflow-Begeisterten.

Hinter jeden Workflow kann man eine oder mehrere Regeln legen. Darin ist festgelegt, was passieren soll, wenn zum Beispiel der Vorgesetzte den Antrag nicht innerhalb einer Frist von, sagen wir, drei Werktagen, beantwortet. Dieser Vorgang nennt sich im Fachjargon Eskalation, und wie damit umgegangen wird, das sagt das so genannte Eskalationsmanagement, das gleichzeitig auch eine Überwachung darüber ermöglicht, ob das Verhalten der beteiligten Personen sich innerhalb der definierten Regeln bewegt hat. Dies zu kontrollieren, ist dann Sache eines entsprechend aufgesetzten Reportings.

Self Services für Manager

Das Gegenstück zu den Employee Self Services sind die Manager Self Services. Sie sorgen dafür, dass alles, was elektronisch zu genehmigen ist, an den richtigen Stellen aufschlägt. SAP preist sein entsprechendes Produkt mit den Worten an: Es „umfasst eine Vielzahl von Worksets

d. h. Business Packages, die sämtliche Werkzeuge und Informationen enthalten, die zur Durchführung von Managementaufgaben wie Budgetüberwachung und Personaleinstellung notwendig sind. Mit diesen Worksets können dezentrale Prozesse auf der Grundlage von Best Practices durchgeführt werden“.[12] An das mit englischen Ausdrücken durchsetzte Business-Deutsch muss man sich gewöhnen, sonst kann man gar nicht mehr mitreden.

In früheren Zeiten erhielten die Linien-Vorgesetzten ihre Reports von den zuständigen Controlling- oder Personalabteilungen. Heute müssen sie sich selber darum kümmern. Hier wurde der Schalter von der Bringschuld der entsprechenden Stabsabteilungen auf die Holschuld der betroffenen Personen umgelegt, Selbstbedienung eben. Die vorgeschlagenen Anwendungs-Szenarien sehen beispielsweise vor:

- Führungskräfte erhalten Einblick in ausgewählte Stammdaten der Mitarbeiterinnen und Mitarbeiter ihres Verantwortungsbereichs.
- Sie können die Zeitkonten ihrer Leute einsehen und deren tägliches Kommen und Gehen überprüfen.
- Wenn die Personalakte in digitalisierter Form vorliegt, können sie die Akten der Personen ihres Zuständigkeitsbereiches durchblättern.
- Falls das Unternehmen entsprechende Systeme betreibt, können sie sich die Fähigkeiten und Fertigkeiten ihrer Mitarbeiterinnen und Mitarbeiter ansehen, in deren Beurteilungen herumblättern, sich die vereinbarten Ziele und Zielerreichungen ansehen, die Fort- und Weiterbildungsmaßnahmen checken und vieles mehr.

Bedeutungsverlust der Personalabteilung

Früher war für die meisten dieser Vorgänge der Kontakt zur Personalabteilung erforderlich. Den braucht man jetzt nicht mehr. Damit fällt leider auch eine wichtige Filterfunktion weg, denn ein Großteil der ehemaligen Aufgaben der Personalabteilung wird jetzt von den Linienvorgesetzten direkt wahrgenommen. In den seltensten Fällen sind sie aber dafür ausgebildet worden. Zu leiden haben darunter auch die Betriebsräte, denen ihre Verhandlungspartner sozusagen gestohlen wurden. Die Verlagerung der Kompetenz für Personalfragen in die Linie führt dazu, dass anstelle mit einer kompetenten Instanz die Betriebsräte es nun mit einer Vielzahl von Verhandlungspartnern zu tun haben, die sich oft nur wenig in Fragen des Arbeits- oder Betriebsverfassungsrechts auskennen. „Es herrscht das Gesetz der freien Wildbahn“, mit diesen Worten beschrieb uns neulich ein Kollege die Situation.

Die genannten Entwicklungen haben es erst ermöglicht, dass vor allem Großkonzerne ihre Personalbereiche als so genannte Shared Services

[12] Quelle: Internet-Site der SAP unter www.sap.com/germany/solutions/business-suite/erp/featuresfunctions/managerselfservices.epx, September 2008.

umorganisiert haben, vergleichbar einem Call-Center. Statt einer Ansprechperson in der Personalabteilung hat man als Beschäftigter nun einen SPOC, einen „Single Point of Contact“, und der besteht aus einer Mailadresse und einer Telefonsammelnummer. Da kann man anrufen, und es wird einem geholfen oder auch nicht. Zitat eines Managers, der die Durchführung von Massenkündigungen abwickeln musste: „Es war außerordentlich hilfreich für uns, dass wir die betroffenen Personen nicht sehen mussten“.

Viele Kolleginnen und Kollegen müssen jetzt ihre Reisekosten- oder sonstigen Unterlagen ins Shared Service Center nach Ungarn oder Rumänien schicken, und wenn sie eine Auskunft über ihren Gehaltstarif haben wollen, dürfen sie sich an das Service Center in Schottland oder in den Niederlanden wenden. Alle beklagen die ins schier Bodenlose gesunkene Qualität der angeblichen Dienstleistung, doch der Trend geht munter weiter.

In finaler Konsequenz haben einige Unternehmen auch noch den letzten Schritt gewagt und die Personalarbeit per Funktionsübertragung an eine Drittfirma komplett „outgesourcet“. Der Linienvorgesetzte ruft dann beim Service-Provider an und sagt, er hätte gerne eine Abmahnung, nennt Name der betroffenen Person und ein paar Gründe für die Maßnahme und erhält postwendend einen aus der Textbausteine-Bibliothek gezupften „gerichtsfesten“ Text – so die Aussage eines Managers, der nicht genannt werden will.

Kritik an Workflows

Mit elektronischen Workflows konnte man lange Zeit keinen Hund hinter dem Ofen hervorlocken, doch die letzten Jahre waren wie ein Dammbruch. Schuld daran sind die Self Services und die – irrige – Meinung der Unternehmen, durch Abwälzen der Arbeit auf die unmittelbar betroffenen Personen administrative Kosten in großen Dimensionen einsparen zu können. Hält man ihnen entgegen, dass eine erfahrene Sekretärin auch eine kompliziertere Dienstreise in wenigen Minuten gebucht hätte und ein im Vergleich dazu hoch bezahlter Ingenieur jetzt eine Dreiviertelstunde damit vertut, so erhält man als Antwort, das seien noch Kinderkrankheiten des neuen Systems, und die Zeit werde es schon richten. Warten wir es ab.

Neben den betriebswirtschaftlichen Fragwürdigkeiten ist die ins schier Unermessliche gesteigerte Abhängigkeit vom Computersystem zu beklagen. Fällt das Netzwerk einmal aus, geht nichts mehr. Voraussetzung der Computerisierung ist aber, dass alle noch erlaubten Vorgänge vorher vorgezeichnet und festgelegt worden sind. Die Standardisierung feiert nie gehabte fröhliche Urstände. Der Raum für Individualität wird systematisch eingeengt. Ein Einkäufer kann dann nur noch Material bestellen, das die Konzernzentrale (meist im fernen Ausland) festgelegt hat.

Uns sind keine Betriebsräte bekannt, die in den beschriebenen Umstellungen der Arbeitsmethodik eine Betriebsänderung sehen. Das mag daran liegen, dass die Prozesse nur schleichend vorankommen. Doch dies darf nicht darüber hinwegtäuschen, dass am Ende der Reise eine ganz andere Arbeitswelt steht: durchnormiert und standardisiert, hierarchisch organisiert und entindividualisiert, mit viel Verlust an Flexibilität und einer festgezurrten Struktur, die Initiative und Kreativität lähmt.

Hervorzuheben ist aber auch die Veränderung unter datenschutzrechtlichem Gesichtspunkt. Waren früher die Personaldaten in strenger Obhut einer Personalabteilung, so sind sie heute über den ganzen Betrieb verteilt und an vielen Stellen für zahlreiche Personen zugänglich. Die Self Services können über das Intranet des Unternehmens an nahezu jedem Computer aufgerufen werden; benötigt wird nur ein Webbrowser; den Rest besorgen die an das Login gebundenen Zugriffsrechte.

Regelungsaspekte

Wir listen im Folgenden ein paar Gesichtspunkte auf, auf die Betriebsräte in entsprechend abzuschließenden Vereinbarungen achten sollten:

- Da noch wenig Erfahrung mit den Auswirkungen der Self Services vorliegen, empfiehlt es sich, jeden Dienst in einer Anlage zur Betriebsvereinbarung über das Personalsystem (oder in einer eigenständigen Regelung) aufzulisten und jede Erweiterung dieser Liste an eine ausführliche Beratung und vor allem an die Zustimmung durch den Betriebsrat zu binden.

- Von Zeit zu Zeit empfiehlt sich die Durchführung eines Erfahrungsaustauschs, wobei erörtert werden kann, welche Services sich bewährt und welche eher zu neuen Problemen geführt haben. So wurde in vielen Vereinbarungen schon festgelegt, dass man Konsensfindungsprozesse nicht über die Workflows im System abwickelt, sondern die Eingaben erst nach gefundenem Konsens ins System vornimmt (beispielsweise den Urlaub erst nach Genehmigung in das System einträgt). Der Grund für solche Korrekturen liegt in der Flut von E-Mails, die das System mit den einzelnen Workflow-Schritten automatisch erzeugt und die von vielen Betroffenen als unzumutbare Belästigung begriffen wird.

- Wenn man auf das Eskalationsmanagement bei den Workflows nicht verzichten mag oder kann, so sollte festgelegt werden, dass in der ersten Eskalationsstufe die betroffenen Personen vom System auf das entstehende Problem hingewiesen werden (z. B. dass bald eine Frist abläuft). Weitere Eskalationen wären regelungspflichtig, wenn es sich dabei um eine Überwachung der von Menschen geleisteten Arbeiten handelt.

- Den Führungskräften per Dauerberechtigung eine Einsicht in die elektronische Personalakte zu erteilen, ist problematisch. Dies sollte umfang- und zeitmäßig streng begrenzt und an bestimmte Vorfälle gebunden werden, beispielsweise ein auf 14 Tage befristetes Einsichtsrecht in ausgewählte Teile der Akte bei innerbetrieblichen Bewerbungen oder Versetzungen.

- Auch die Einsicht in die Zeitkonten ist problematisch. Wenn ein Unternehmen Gleitzeit vereinbart hat, so ist dies das Zugeständnis einer teilweisen zeitlichen Autonomie. Damit verträgt sich nicht die Kontrolle des täglichen Arbeitszeitverhaltens durch Vorgesetzte, jedenfalls solange nicht, wie sich die betroffenen Personen an das vereinbarte Regularium halten. Die hier erlaubten Auswertungen sollten alle einzeln festgelegt werden.

6. Data-Warehouse-Anwendungen

Die klassischen Personalsysteme vergangener Zeiten verfügten alle über ein ebenso klassisches Reporting, d. h. eine Summe von teils regelmäßig (monatlich oder quartalsweise), teils auf Nachfrage im Einzelfall erzeugten Berichten als Listen oder statistische Auswertungen. Von diesem Verfahren kommt man immer mehr ab und verlagert die Auswertungen auf ein zweites System mit einer eigenen Datenbank, das meist auf einem anderen Rechner installiert ist als das „operative“ System. Dieses System ist das Data Warehouse, in der SAP-Welt bekannt unter dem Namen „Business Warehouse“, denn bei SAP ist alles Business.

Vorteile

Zunächst stechen einige Vorteile dieses Verfahrens ins Auge:

- Das operative System wird von der Belastung durch ressourcenfressende Auswertungen befreit, denn diese laufen auf einem eigenen Rechner. Die Mitarbeiterinnen und Mitarbeiter können im operativen System nun ungestörter ihren Tagesaufgaben nachgehen.

- Die Auswertungen sind streng stichtagbezogen, denn in regelmäßigen Intervallen (bei Personaldaten meist monatlich) werden Teile der operativen Daten in das Datenbanksystem des Data Warehouse übertragen.

- Daten können aus unterschiedlichen Quellen unter dem Dach des Data Warehouse zusammengefügt werden.

Mitbestimmungsrelevante Probleme

Der letztgenannte Vorzug ist aber auch problematisch. Hat man sich früher auf die strikte Trennung von Betriebs- und Personaldaten verständigt, so hebt die Vereinigung im Data Warehouse die Trennung wieder auf.

Im Data Warehouse sind die Daten nach so genannten Datenwürfeln („data cubes“, „info cubes“ oder „data marts“) organisiert und werden unterschieden nach Kennzahlen und Dimensionen, wobei jede Kennzahl in Abhängigkeit von jeder Dimension dargestellt werden kann, zum Beispiel die Kennzahl Fehlzeitenquote in Abhängigkeit von der Dimension Zeitachse (Monate – Quartale – Jahre) oder der Dimension Aufbauorganisation (Abteilungen oder Kostenstellen). Grundsätzlich ist in einem Datenwürfel alles mit allem kombinierbar.

Eine zweite besondere Eigenschaft einer Data Warehouse-Anwendung ist eine „Drill down“ genannte Technik. Damit ist gemeint, dass man eine Information immer feiner auflösen kann. Zum Beispiel kann man sich die Fehlzeitenquote in einem Konzern erst für die einzelnen Betriebe ansehen; diese kann man dann nach Bereichen, Hauptabteilungen, Abteilungen und Kostenstellen auflösen. Wenn die Datenbasis es erlaubt, kann man das Auswertungsergebnis sogar bis auf die einzelnen Arbeitsplätze herunterbrechen. Es ist also von entscheidender Wichtigkeit, woraus die kleinste Dateneinheit in einem solchen Datenwürfel besteht. Stehen hier nur zusammengefasste oder summierte Daten über die Kostenstelle, so reicht kein Trick der Welt, diese Daten auf einzelne Arbeitsplätze und damit einzelne Personen aufzulösen (es sei denn, die Kostenstellen bestehen nur aus einzelnen Personen).

Die Umstellung der Auswertungen auf ein Data Warehouse stellt andererseits auch eine große Chance dar, das Reporting neu zu organisieren. Sinn der Anwendung sind statistische Auswertungen, und diese weisen in der Regel keinen direkten Personenbezug auf. Dies kann bei der Übertragung der Daten aus dem operativen System in das Data Warehouse berücksichtigt werden. Denn die Daten werden nicht einfach von einem System ins andere geschaufelt; vielmehr bedarf es teils komplizierter Transformationsprogramme, die sich die Daten aus den operativen Systemen heraussuchen und so zusammenfassen, wie sie im Data Warehouse gebraucht werden. Und genau an dieser Stelle kann man für die Anonymisierung der Daten sorgen, zum Beispiel durch geeignete Summierungsregeln.

Bisher hat die in der Personaldatenverarbeitung führende Firma SAP für ihr Business Warehouse mit ihrem Business Explorer nur ein Auswertungsinstrument zur Verfügung gestellt, das ähnlich funktioniert wie ein Arbeitsblatt des Tabellenkalkulationsprogramms Excel. Doch Ende 2007 hat die SAP für fast fünf Milliarden Euro die französische Firma Business Objects aufgekauft, die bis dato Marktführer für Endbenutzer-Werkzeuge bei Data Warehouse-Anwendungen war; „Business Intelligence“[13] abgekürzt BI, nennt sich diese Rubrik. Die neuen Werkzeuge erlauben grafische Aufbereitungen der Ergebnisse vom Feins-

[13] Es ist zu beachten, dass in diesem Zusammenhang das Wort „intelligent“ nichts mit „Intelligenz“ zu tun hat, sondern eher dem entspricht, was „intelligent“ in der Abkürzung CIA bedeutet, einer Organisation, deren deutsches Pendant bekanntlich Bundesnachrichtendienst heißt.

ten und bieten vor allem die beliebten Ampeldarstellungen. Bei diesen kann man für jede Kennzahl Wertebereiche definieren, die im „grünen Bereich“ liegen, und kritische Werte lassen sich als rot markieren. Dazwischen bleibt die bekannte Gelbzone. Wirft ein Manager einen schnellen Blick auf eine Auswertung und sieht überall grün, kann er sich beruhigt seiner nächsten Aufgabe zuwenden. Stolpert er aber über rote Ampeln, dann kann er sich der Drill-Down-Funktionalität bedienen und sieht sich den Bereich genauer an, bis er auf des Pudels Kern stößt – so jedenfalls sagt es die Herstellerwerbung. Das viele Geld, das SAP in die Hände nahm, lässt erwarten, dass an dieser Technikfront uns in Zukunft noch bahnbrechende Änderungen in Aussicht stehen. Jedenfalls ist klar, dass die in Betriebsvereinbarungen gerne verwendete Methode, jede erlaubte Auswertung in einem Muster festzulegen, nicht mehr verfängt, denn die Systeme sind für Online-Recherchen gemacht, wobei vorher nicht jede einzelne Auswertung festgelegt ist. Es bedarf also neuer Strategien, um dem Schutz der Persönlichkeitsrechte in einer solchen Anwendung Geltung zu verschaffen.

Regelungsaspekte

Als Betriebsrat sollte man unbedingt auf dem Abschluss einer Betriebsvereinbarung bestehen und auf folgende Punkte achten:

- Für den Personalbereich sollte ein eigenes Data oder Business Warehouse eingerichtet werden (getrennt von den betriebswirtschaftlichen Anwendungen). Andernfalls muss man sich um alle Anwendungen kümmern und sehen, wie man den Überblick bei Controllingdaten und Personaldaten noch auf die Reihe bekommt.

- Die Daten sollten in möglichst kleinen Datenwürfeln aus thematisch zusammengehörenden Daten organisiert werden, die für einen konkreten und zu benennenden Verwendungszweck zusammengestellt werden. Bei einer kleinen Anzahl thematisch verwandter Daten ist das Ergebnis der Verknüpfung dieser Daten untereinander noch einigermaßen überschaubar; bei großen Datenwürfeln mit unterschiedlichen Daten ist dies schier unmöglich.

- Natürlich sollte man dafür sorgen, dass die vielen kleinen Datenwürfel nicht untereinander verknüpft werden dürfen, denn sonst war das Bemühen um besseren Überblick vergeblich.

- In keinem Datenwürfel sollte ein die Person direkt identifizierendes Merkmal zugänglich gemacht werden. Die wenigen erforderlichen Auswertungen mit namentlichen Informationen sollten dann im operativen Personalsystem erstellt werden, nicht über das Data Warehouse.

- Kleinste in Auswertungen zugängliche Zeiteinheit für Statistiken sollte der Monat sein; Ausnahmen wären gesondert zu vereinbaren.

- Für die Drill-Down-Funktion sollten ebenfalls jeweils kleinste Einheiten festgelegt werden. Bewährt hat sich der Grundsatz, dass jede kleinste darstellbare Organisationseinheit mindestens fünf Personen umfassen muss; kleinere Einheiten wären zusammenzufassen.

III. E-Mail und Internet

1. Grundlagen

Noch vor 10 Jahren wurden in vielen Unternehmen IT-Offensiven gestartet, um die Beschäftigten mit der Nutzung des Internets vertraut zu machen. In vielen Unternehmen wurden die Beschäftigten explizit zur privaten Nutzung der Arbeitsplatzcomputer aufgefordert. Die Beschäftigten sollten Routine im Umgang mit dem Internet aufbauen: Denn von guten Kenntnissen der Beschäftigten im Umgang mit Suchmaschinen oder vom schnellen Erkennen von Hyperlinks profitierten letztlich auch die Unternehmen.

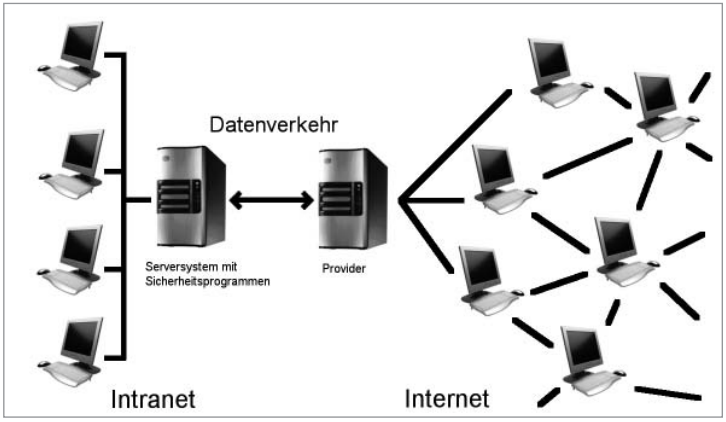
Internet- und vor allem die E-Mail-Nutzung haben mittlerweile die Arbeitswelt durchdrungen und sind an vielen Arbeitsplätzen zum unverzichtbaren Arbeits- und Kommunikationsmittel geworden. Von den mitarbeiterorientierten Ansätzen der Vergangenheit ist leider nicht viel erhalten geblieben. Heute stehen Fragen der Zulässigkeit einer privaten Nutzung und vor allem deren Kontrolle im Mittelpunkt der meisten innerbetrieblichen Auseinandersetzungen.

In Unternehmen, in denen bis heute keine Betriebsvereinbarung zum Umgang mit den elektronischen Kommunikationssystemen abgeschlossen worden ist, ist die private Nutzung der Systeme in den meisten Fällen untersagt. Die Beschäftigten bewegen sich in diesen Fällen in einem hochsensiblen „Minenfeld“ und stets nur einen Mausklick von der Sport- oder Kulturwebseite – und damit von der unerlaubten Systemnutzung – entfernt. Denn das Benutzerverhalten bei der Internet- und E-Mail-Nutzung kann lückenlos überwacht werden, eine entsprechende Konfiguration vorausgesetzt. Nichts ist dann für einen Systemadministrator einfacher, als in den Internetprotokollen zu überprüfen, welche Webseiten Mitarbeiter X zu welchen Uhrzeiten aufgerufen hat. Tauchen dort Webseiten auf, die zu vermeintlich privaten Zwecken aufgerufen worden sind? Sind Suchabfragen wirklich dienstlich motiviert? Enthalten E-Mails „verdächtige“ Betreffzeilen? In wenigen Minuten könnten für beliebige Mitarbeiter Dossiers über deren Systemnutzung in den vergangenen Monaten zusammengestellt werden.

Die Ausgangslage für die Beschäftigten verbessert sich nur vordergründig, falls die private Nutzung trotz offiziellen Verbots vom Arbeitgeber stillschweigend geduldet wird. Denn in diesen Fällen sind die Protokolldateien nichts anderes als Werkzeuge, um willkürlich herausgegriffene Mitarbeiter unter Druck setzen zu können. Allein deshalb ist Betriebsräten der Abschluss einer Vereinbarung zum Thema dringend anzuraten.

Sicherheits-programme

Mit zunehmender Bedeutung des Internet- und E-Mail-Einsatzes sind auch die damit verbundenen Sicherheitsrisiken gewachsen. Um Bedrohungen von Viren oder gezielten Hackerangriffen abzuwehren, kommt in den Unternehmen ein ganzes Arsenal unterschiedlichster Schutzprogramme zum Einsatz. Da alle Internet- und E-Mail-Verbindungen vollständig über ein zentrales Serversystem an der Schnittstelle zwischen Unternehmensnetzwerk (Intranet) und Internet geleitet werden, werden die Schutzprogramme an eben dieser Schnittstelle installiert. An diesem „Flaschenhals“, im Fachchinesisch „Firewall“ genannt, kann die Systemadministration dann den kompletten ein- und ausgehenden Datenverkehr überprüfen.



Leider kann man mit vielen Produkten nicht nur potenzielle Angreifer ertappen, sondern auch die eigenen Mitarbeiter überwachen. Aus diesem Grund skizzieren wir den Regelungsbedarf der am häufigsten eingesetzten Softwaresysteme Webfilter, Virenscanner und Spamfilter am Ende dieses Kapitels.[14]

2. Internet

Private Nutzung

Ausgangspunkt einer betrieblichen Regelung sollte die Forderung nach einer zeitgemäßen privaten Nutzungsmöglichkeit des Internets für die Beschäftigten sein. Nicht selten ist der Arbeitgeber auf Nachfrage prinzipiell bereit, einer privaten Nutzung zuzustimmen.

Allerdings werden in den letzten Jahren auch juristische Bedenken angeführt, wonach ein Unternehmen, das die private Nutzung erlaubt, als Provider anzusehen sei und damit besondere Datenschutzvorschriften des Telekommunikationsgesetzes (§ 88 ff. TKG) zu beachten hätte.

[14] Viele beispielhafte Regelungsentwürfe sind online abrufbar unter http://www.tse.de/vereinbarungen/internet und netze/.

Arbeitgeber als Provider nach TKG?

Für Verunsicherung sorgen zudem die neuen Gesetze zur Vorratsspeicherung von Telekommunikationsdaten, die ab 2009 allen Providern eine umfangreiche Protokollierung der Internet- und E-Mail-Nutzung für den Zugriff von Bundesbehörden bei der Strafverfolgung und im Antiterrorkampf auferlegt und deren technische Umsetzung mit erheblichen Kosten verbunden wäre, vorausgesetzt, das Bundesverfassungsgericht bestätigt ihre Verfassungskonformität.

Die juristischen Einwände können Betriebsräte gut kontern: Die einseitige Auslegung des TKG in der Providerfrage ist rechtlich durchaus strittig. Und eine Verpflichtung der Unternehmen zur Vorratsdatenspeicherung für die Bundesbehörden ist in den entsprechenden Gesetzen explizit ausgeschlossen: § 113a TKG setzt voraus, dass Dienste „öffentlich" zugänglich sein müssen. Das ist bei Unternehmen nicht der Fall, denn sie stellen die Dienste ja nur dem geschlossenen Kreis ihrer Mitarbeiter zur Verfügung. Deshalb kann keine Pflicht zur Vorratsspeicherung bestehen.

Regelungsvorschlag private Nutzung

Um Arbeitgeber und Betriebsrat eine Klärung der verworrenen Rechtslage zu ersparen, bietet sich die folgende Konstruktion an:

- In einer Betriebsvereinbarung wird festgelegt, dass der Internet- und E-Mail-Zugang als *dienstliches Arbeitsmittel* zur Verfügung gestellt werden.

- Weiterhin wird festgelegt, dass eine *private Nutzung geduldet oder erlaubt* wird, wenn sie geringfügigen Umfangs ist und die Arbeitsabläufe und Sicherheit des Netzes nicht beeinträchtigt sowie nicht gegen geltende Rechtsvorschriften verstößt.

Die Liste kann gegebenenfalls um weitere Punkte ergänzt oder präzisiert werden. Was letztlich als Missbrauch gelten soll, ist Verhandlungssache zwischen den Betriebsparteien und sollte selbstverständlich die Erfahrungen der Beschäftigten berücksichtigen.

Internetzugang für alle Beschäftigten

Sind die Fragen zur privaten Nutzung geklärt, bedarf es der Vereinbarung, welche Mitarbeiter überhaupt Zugriff auf das Internet erhalten. Beschäftigte von der Nutzung des Internets auszuschließen, ist ein ausgezeichnetes Mittel, um das Betriebsklima im Unternehmen nachhaltig zu vergiften. In der Regel werden Internetzugänge deshalb an allen vernetzten Arbeitsplatzrechnern eingerichtet. Für Beschäftigte ohne Arbeitsplatzrechner können Computer mit Internetzugang in Pausenräumen oder an anderen betriebsöffentlich zugänglichen Stellen aufgestellt werden. Kann eine entsprechende Regelung nicht erreicht werden, so muss der Arbeitgeber zumindest das Gleichheitsprinzip beachten und den Zugang nach sachlichen Kriterien erteilen. Üben zwei Beschäftigte im Unternehmen also dieselben Tätigkeiten aus, so muss je nach sachlicher Abwägung entweder beiden der Internetzugang gewährt werden oder keinem von beiden.

Eine ähnliche Problematik taucht auf, wenn das Unternehmen die weiter unten beschriebenen Webfilter-Programme einsetzt, um bestimmte Webseiten nur für ausgewählte Beschäftigtengruppen freizugeben bzw. zu sperren.

Umgang mit Protokolldaten

Jeder Webseitenaufruf im Internet hinterlässt digitale Spuren auf den Sicherheitsservern des Unternehmens.

Auswertungsmöglichkeiten von Protokolldaten beim Webseiten-Abruf

```
2008-07-12 12:08:17 – 182ms – 123.123.123.100 – TCP – ok – 1726 –
http://www.tse.de/vereinbarungen/index.php – text/html

2008-07-12 12:08:17 – 317ms – 123.123.123.100 – ok – 14452 –
http://www.tse.de/images/hint_far.gif – image/gif

2008-07-12 12:08:18 – 223ms – 123.123.123.100 – ok – 12776 –
http://www.tse.de/images/technik.gif – image/gif

2008-07-12 12:08:23 – 102ms – 123.123.123.101 – ok – 1221 –
http://www.witze.de/fun/friseur.html – text/html

2008-07-12 12:08:31 – 113ms – 123.123.123.100 – ok – 1655 –
http://www.tse.de/suchmaschine/index.php – text.html

2008-07-12 12:08:39 – 140ms – 123.123.123.100 – ok – 2153 –
http://www.tse.de/suchmaschine/ergebnis.php?suchwort=
Datenmissbrauch – text.html
```

Systemadministratoren können mit Hilfe von geeigneten Sortier- und Filterwerkzeugen in kürzester Zeit die Webseiten-Aufrufe der Beschäftigten auflisten und dabei die kryptischen Protokolleinträge schnell dechiffrieren:

Zunächst wird das Datum und die Uhrzeit in der Form „Jahr-Monat-Tag Stunde:Minute:Sekunde“ protokolliert. Es folgt die Dauer der Übertragung in Millisekunden. Das dritte Datum enthält die IP-Adresse des Arbeitsplatzrechners (123.123.123.100), von dem aus die Webseiten gerade aufgerufen werden. Mit ihrer Hilfe kann der Administrator den Nutzer ermitteln. Es folgen optional ein Fehlercode und die Anzahl der übertragenen Bytes, anschließend die Adresse der aufgerufenen Webseite und die Kennzeichnung, ob es sich um eine Textseite (text/html) oder eine eingebundene Grafik (image/gif) handelt.

Im Beispiel ruft ein Mitarbeiter mit der IP-Adresse 123.123.123.100 am 12. Juli 2008 um 12:08 Uhr eine Webseite auf dem Internet-

Server www.tse.de mit zwei eingebundenen Grafiken auf. Der Aufruf der Witze-Webseite erfolgt wenige Sekunden später von einem anderen Rechner (andere IP-Adresse). Der erste Mitarbeiter ruft eine Suchmaschine auf. In diesem Fall wird der Suchbegriff mitprotokolliert, wie der letzte Protokolleintrag zeigt („Datenmissbrauch“).

In einer Betriebsvereinbarung sollte konkret festgehalten werden, welche Protokolldaten zu welchem Zweck aufgezeichnet und verwendet werden dürfen, wer auf die Protokolldaten zugreifen darf und wann die Daten gelöscht werden müssen. Eine typische Regelung sieht wie folgt aus:

Ausschließlich zum Zweck der Gewährleistung der Systemsicherheit und der technischen Fehleranalyse werden folgende Protokolldaten erhoben:

- IP-Adresse des zugreifenden Rechners,
- Datum und Uhrzeit,
- Webadresse des Objektes, auf das zugegriffen wird,
- Datenmenge und
- Fehlercode.

Die Protokolldaten werden nach spätestens drei Monaten gelöscht bzw. überschrieben. Die Anzahl der Systemadministratoren, die Zugriff auf die Daten haben, ist auf ein Minimum zu begrenzen. Sie sind dem Betriebsrat namentlich zu benennen.

Ein Zugriff auf die Protokolldateien ist demnach nur zu technischen Analysezwecken zulässig. Die zugriffsberechtigten System-Administratoren dürfen daher zum Beispiel Problemen nachgehen, falls bestimmte Webseiten nicht aufrufbar sind oder wenn die außerordentlich erhöhte Aktivität eines Rechners auf einen Virusbefall hinweist. Sie dürfen allerdings nicht ermitteln, welche Webseiten ein einzelner Beschäftigter in bestimmten Zeiträumen aufgerufen hat oder wie lange dieser online gewesen ist.

Diese regulären Zugriffsmöglichkeiten der Systemadministration kann ergänzt werden um eine Missbrauchsregelung, die den Umgang mit als missbräuchlich deklarierten Anfangsverdachtsfällen beinhaltet und das Verfahren sowie eine adäquate Beteiligung des Betriebsrats fixiert. Bewährt hat sich dabei eine einzelfallbezogene Herangehensweise:

Nur beim Vorliegen von konkreten Verdachtsmomenten einer missbräuchlichen Nutzung ist eine individuelle, auf die jeweilige Person bezogene Auswertung der Protokolldaten zulässig. Vor der Auswertung wird der Betriebsrat über den Verdachtsmoment informiert. Ergibt die gemeinsame Bewertung, dass die Verdachtsmomente ausreichend sind, erfolgt eine Auswertung gemeinsam mit dem Betriebsrat unter Einbeziehung des Mitarbeiters. Eventuell daraus resultierende personelle Maßnahmen erfolgen nur im Einvernehmen mit dem Betriebsrat.

Einige Betriebsräte vereinbaren an dieser Stelle allerdings lediglich die Zustimmungspflicht des Betriebsrats zur Auswertung und lehnen eine darüber hinausgehende Beteiligung am Missbrauchsverfahren ab. Sie versprechen sich davon eine stärkere Position für den Fall, dass der Arbeitgeber personelle Maßnahmen gegen den Beschäftigten durchsetzen will.

Nutzungsdaten auf den lokalen Arbeitsplatzrechnern

Auskünfte über das Nutzerverhalten sind nicht nur mit Hilfe der Protokolldaten an den zentralen Sicherheitssystemen des Unternehmensnetzwerks rekonstruierbar; auch auf den Arbeitsplatzrechnern der Benutzer werden von Betriebssystem und Webbrowser zwangsweise Daten über Webseiten-Aufrufe gespeichert. Im Internet finden sich zahlreiche Tipps, wie Benutzer diese Informationen aufspüren und löschen können. Für die Nutzung des Internets in Unternehmen sind sie allerdings meist nur wenig hilfreich. Denn in den meisten Unternehmen haben die Nutzer keine Rechte, tatsächlich alle relevanten Nutzungsdaten zu verändern oder zu löschen. Und wo dies technisch doch möglich ist, existieren meist Arbeitsanweisungen, die entsprechende Aktivitäten untersagen. Erschwerend kommt in jedem Fall die Intransparenz der meisten Betriebssysteme hinzu, so dass sogar ausgewiesene Experten nicht alle nutzungsrelevanten Stellen benennen können.

Auch der Einsatz neuerer Webbrowser verbessert die Situation nicht wesentlich. Zwar verfügen sie in der Regel über einen so genannten „privacy“-Modus zum vorgeblich anonymen Surfen. Gelöscht werden freilich nur *lokale* Informationen wie Webseiten-Aufruf-Historie oder Cookies, die personenbeziehbaren Protokolldaten am zentralen Serversystem des Unternehmens fallen natürlich weiterhin an.

Um die Persönlichkeitsrechte der Beschäftigten zu wahren, sollte daher ein generelles Verbot der Nutzung von Protokolldaten auf den Arbeitsplatzrechnern vereinbart werden. Alle Daten, die die Systemadministration zur Gewährleistung der Netzwerksicherheit benötigt, erhält sie bereits über die Protokollierung der zentralen Sicherheitssysteme. Ein Zugriff auf die lokalen Daten der Arbeitsplatzrechner könnte nur in Ausnahmefällen als Beweissicherungsmaßnahme im Rahmen des

oben angesprochenen Missbrauchsverfahrens durchgeführt werden, soweit der Betriebsrat im jeweiligen Einzelfall zugestimmt hat.

Regelungs-aspekte

Betriebliche Regelungen sollte also mindestens folgende Punkte beinhalten:

- Klärung der privaten Nutzung
- Beachtung des Gleichheitsprinzip beim Internet-Zugang
- Enge Zweckbestimmung und Zugriffsregelungen für Protokolle und Auswertungen
- Verfahren bei Missbrauchsverdacht klären

Zudem ist abzufragen, ob Filterprogramme (Kapitel III 4) oder weitere Netzwerküberwachungssoftware (Kapitel V) im Unternehmen eingesetzt wird. In dem Fall sollte man auch dazu Vereinbarungen abschließen, um Regelungslücken zu schließen.

3. E-Mail

Datenschutzrechtlich hochsensibel ist der Umgang mit E-Mail am Arbeitsplatz. Einerseits erwartet das Unternehmen zu Recht, dass es über wichtige Belange der über E-Mail abgewickelten, dienstlichen Kommunikation informiert wird, andererseits ist Kommunikation in Deutschland grundrechtlich geschützt, auch die dienstliche Kommunikation am Arbeitsplatz.

Gemäß der Rechtsprechung von Bundesverfassungsgericht und Bundesarbeitsgericht ist das heimliche Abhören dienstlicher Telefongespräche unzulässig.[15] Diese Urteile sind auf die Überwachung von E-Mails übertragbar.

Fernmelde-geheimnis für E-Mail

Ein neueres Urteil des Bundesverfassungsgerichts (BVerfG v. 2.3.2006 – 2 BvR 2099/04, vgl. AuR 2006, 118) präzisiert, dass E-Mail-Kommunikation während des Übertragungsvorgangs durch das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG geschützt sei. Nach Eingang der Mail im Postfach des Benutzers greife hingegen das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG). Für die zu treffenden betrieblichen Regelungen ist diese Differenzierung jedoch nicht von Belang.

Die persönliche elektronische Kommunikation ist zu schützen. Eine entsprechende Betriebsvereinbarung sollte daher klarstellen, dass die Beschäftigten zwar die Pflicht haben, den Arbeitgeber über die dienst-

[15] Vgl. BAG v. 30.8.1995 – 1 ABR 4/95 (DB 1996, 333; CR 1996, 155) und BVerfG v. 19.12.1991 – 1 BvR 382/85 (AuR 1992, 158, DB 1992, 786).

lichen Inhalte der E-Mails zu informieren. Der unmittelbare Zugriff auf die Inhalte der Mails ist allerdings dem Absender und dem Empfänger vorbehalten.

Vertreter-regelung und Abwesenheits-E-Mail

Für den Fall von geplanten und ungeplanten Abwesenheiten sollte in der Betriebsvereinbarung eine Vertreterregelung getroffen werden. Unproblematisch sind Lösungen, wonach jeder E-Mail-Benutzer vor einem geplanten Urlaub, einer Dienstreise o. Ä. über eine Abwesenheitsfunktion seines E-Mail-Programms eine automatische Antwortmail aktiviert, die bei jedem E-Mail-Empfang an den entsprechenden Absender versendet wird. Die Autoantwort enthält dann einen Hinweis auf die voraussichtliche Abwesenheit des Empfängers sowie die Mailadresse eines Ansprechpartners für dringende Angelegenheiten.

Die inzwischen seltener anzutreffende Praxis, E-Mails im Abwesenheitsfall ohne weitere Prüfung automatisch an eine dritte Person weiterzuleiten, ist datenschutzrechtlich heikel. Denn der Absender einer E-Mail vertraut in der Regel darauf, dass im geschützten Bereich seiner Kommunikation tatsächlich auch nur der Adressat persönlich auf die versendete E-Mail zugreift. Von der Verwendung dieses Verfahrens muss daher abgeraten werden.

Aus Mitbestimmungssicht erheblich problematisch ist die Frage des Zugriffs auf Postfächer der Beschäftigten im Falle von Krankheit und anderen unvorhergesehenen Abwesenheiten. Denn in diesem Fall könnten zwischenzeitlich wichtige dienstliche E-Mails im elektronischen Postkorb des erkrankten Beschäftigten eingegangen sein. Ein unmittelbares Einsichtsrecht der Vorgesetzten gibt es jedoch nicht und sollte auch in diesen Fällen abgewendet werden. Empfehlenswert ist folgendes Verfahren:

- Die Beschäftigten benennen eine Person ihres Vertrauens, für die im Fall unvorhergesehener Abwesenheit der Zugriff auf die E-Mail-Konten frei geschaltet werden kann.
- Die Vertrauenspersonen sichten die E-Mails nach wichtigen dienstlichen Vorgängen und leiten diese weiter.
- Die Vertraulichkeit der betrieblichen wie auch eventueller privaten Informationen ist bei diesen Zugriffen zu wahren.
- Der erkrankte Benutzer ist so bald wie möglich über den erfolgten Zugriff zu informieren.
- Für das Postfach des erkrankten Benutzers wird die Auto-Abwesenheitsmeldung aktiviert.

Private Nutzung

Wie bei der Internetnutzung muss für eine Betriebsvereinbarung die Frage der privaten Nutzung geklärt werden. Es ist offensichtlich, dass

eine private Nutzung nicht vollständig untersagt werden kann, schon deshalb nicht, weil die Beschäftigten keinen Einfluss darauf haben, wer ihnen Inhalte zusendet und ob diese privater oder dienstlicher Natur sind. Viele Mails enthalten sowieso private und dienstliche Elemente, eine trennscharfe Unterscheidung ist nicht möglich. Überhaupt stellt sich die Frage, weshalb bei der Verwendung von E-Mail andere Grundsätze gelten sollen als in der nicht digitalen Welt: Wenn zwei Beschäftigte sich auf dem Flur begegnen und eine kurze freundliche Information über das verbrachte Wochenende austauschen, wird kaum ein Arbeitgeber etwas dagegen einwenden. Man wird es als angenehmes Feature einer für die Arbeitsatmosphäre förderlichen Unternehmenskultur werten. Selbstverständlich stellen dieselben Inhalte, nur in Form einer E-Mail verpackt, ebenfalls kein Problem für irgendjemanden dar.

Der für die Internetvereinbarung angeführte Regelungsvorschlag zur Umgehung der einschlägigen juristischen Spitzfindigkeiten kann ohne Probleme auf den Umgang mit dem E-Mail-System ausgeweitet werden.

Da aus der E-Mail-Adresse des Beschäftigten unmittelbar Rückschlüsse auf das betreffende Unternehmen gezogen werden können, könnte als Alternative vorgesehen werden, die Beschäftigten in der Vereinbarung aufzufordern, für private E-Mail in erster Linie die Internet-Angebote externer E-Mail-Anbieter mit neutraler E-Mail-Adresse zu nutzen. Die E-Mail-Nutzung könnte dann über Webanwendungen der E-Mail-Anbieter erfolgen. So könnten sich Auslegungsunterschiede über die Grenzen der privaten E-Mail-Nutzung zwischen Betriebsrat und Arbeitgeber erübrigen.

Protokolldaten

Von der Einsichtnahme in die Inhalte der E-Mails unterschieden werden Zugriffe auf die so genannten Verbindungsdaten. Unter Verbindungsdaten versteht man die „äußeren“ Informationen über die Kommunikationsverbindung, also z. B. Zeitpunkt, Übertragungsdauer, Absender- und Empfängeradresse. Diese Verbindungsdaten sind unter Umständen hilfreich, um technische Fehlerquellen im Netzwerk aufzuspüren. Während die Inhalte von E-Mails für die Systemadministratoren tabu sind, sehen Vereinbarungen häufig wie bei der Internetnutzung die Aufzeichnung und Auswertung entsprechender Protokolldaten zu technischen Zwecken vor. Gleichwohl unterfallen auch die Verbindungsdaten den Vorschriften zum Schutz der Persönlichkeitsrechte und eine Auswertung sollte nur in engen Grenzen vereinbart werden.

Ein Vorschlag für den Umfang der Protokolldaten:

- E-Mail-Adresse von Absender und Empfänger,
- Datum und Uhrzeit,

- Datenmenge und
- Fehlercode.

Vor allem die Aufnahme der *Betreffzeile* in die Protokollierung sollten Betriebsräte unbedingt verhindern.

Analog zum Vorgehen bei der Internet-Vereinbarung sollten Speicherfrist und Zugriffsberechtigte festgehalten werden, ebenso ein Verbot der Nutzung von Daten auf den lokalen Arbeitsplatzrechnern.

> Die Protokolldaten werden nach spätestens drei Monaten gelöscht bzw. überschrieben. Die Anzahl der Systemadministratoren, die Zugriff auf die Daten haben, ist auf ein Minimum zu begrenzen. Sie sind dem Betriebsrat zu benennen.
>
> Zugriffe auf lokale Daten der Arbeitsplatzcomputer erfolgen nicht, bzw. nur entsprechend der zwischen Betriebsrat und Arbeitgeber getroffenen Missbrauchsregelung.

Regelungswürdig ist außerdem der Einsatz von Antiviren-Programmen und Spam-Filter-Software. Aus technischer Sicht greifen diese automatisch auf die geschützten Inhalte von E-Mails zum Zweck der Überprüfung zu. Theoretisch könnte daher ein Eingriff in die Persönlichkeitsrechte der Beschäftigten vorliegen. Aber natürlich haben die Beschäftigten auch selbst ein erhebliches Interesse am Spam- und Virenschutz. Wer auf Nummer sicher gehen will, der schließt für beide Systeme eigene Betriebsvereinbarungen ab. Wer hingegen die kleine Lösung für ausreichend hält, der weist in der E-Mail-Vereinbarung darauf hin, dass die Überprüfung der E-Mails durch die Programme ausschließlich automatisch erfolgt, auf den Zweck der technischen Überprüfung begrenzt bleibt und auf keinen Fall durch augenscheinliche Einsichtnahme der Systemadministration in die Mailinhalte erfolgen darf.

Regelungsaspekte

Regelungen zum Umgang mit E-Mail sollten wie angeführt mindestens die folgenden Punkte umfassen:

- Klärung der privaten Nutzung
- Inhalte von E-Mails, auch und besonders von dienstlichen E-Mails, sind zu schützen
- Vertreterregelung, die den Schutz der Kommunikation wahrt
- Enge Zweckbestimmung und Zugriffsregelungen für Protokolle und Auswertungen

- Verfahren bei Missbrauchsverdacht klären (analog den Bestimmungen einer etwaigen Internet-Vereinbarung

- Einsatz von Antivirenprogrammen (Kapitel III 5), Spam-Filtern (Kapitel III 6) und Software zur Netzwerk-Überwachung (Kapitel V) regeln

4. Webfilter-Software

Webseiten filtern? Das klingt harmlos. Leider verbergen sich unter dem harmlosen Etikett oft mächtige Überwachungswerkzeuge mit einem Funktionsumfang, der weit über das reine Filtern von Webseitenzugriffen hinausgeht.

Abkehr vom mündigen Beschäftigten

Die ersten Programme dieser Softwarekategorie wurden als Kinderschutzprogramme eingesetzt. Eltern sollten ein Werkzeug bekommen, um die lieben Kleinen beim Surfen im Internet vor nackter Haut und Schlimmerem zu beschützen. Es hat nicht lange gedauert, bis nicht mehr Kinder, sondern Beschäftigte von Unternehmen im Fokus der Programme standen. Heute sind Webfilter-Programme „big business“ und allen berechtigten Einwänden zum Trotz werden sie immer noch in viel zu vielen Unternehmen eingesetzt. Offenbar verzichtet man in den Chefetagen lieber darauf zu ergründen, ob der Einsatz von Filterprogrammen überhaupt sinnvoll ist, oder ob es nicht doch einen Versuch wert ist, auf den mündigen Benutzer hinter dem Arbeitsplatzcomputer zu setzen.

Kategorisierung

Die Filtersoftware-Industrie sichtet Webseiten und ordnet diese Webseiten einzelnen Kategorien zu. Das kann „Sex“ sein oder „Waffen“, aber auch „Gewerkschaft“, „Jobsuche“ oder „Gesundheit“. Unternehmen, die eine Softwarelizenz erworben haben, können dann entscheiden, welche Kategorien sie sperren möchten und welche Kategorien vermeintlich unbedenklich sind.

Auswertungen

In der Regel kann dann alles „gemonitort“, protokolliert und ausgewertet werden, wenn man keine entsprechende Regelungen trifft – „Reporting That Knows No Limits“ heißt es dann in den Hochglanzprospekten des Marktführers. Und am Ende eines jeden Arbeitstages kann automatisch eine Sünderliste der Beschäftigten mit den meisten abgewiesenen Zugriffsversuchen per Mail versendet werden.

Natürlich passieren bei der Kategorisierung Fehler. Da wird die Website der Bundesregierung schon mal in den gleichen Topf geworfen wie amerikanische Hacker-Sites. Und natürlich gelingt es nicht, alle einschlägigen Webseiten redaktionell zu erfassen. Gerade Server und Webseiten mit verbotenen Inhalten wechseln täglich ihre Namen und Adressen im Netz. Man braucht nicht allzu viel Lebenserfahrung, um zu wissen, dass verbotene Früchte besonders lecker schmecken. Bei nicht wenigen Menschen bewirkt eine Sperre erst, dass sie sich auf die Suche nach deren Überwindung machen.

Regelungs-aspekte

Das deutsche Recht schützt den Arbeitgeber nicht vor Dummheit. Und so soll er nach herrschender Meinung das Recht haben, den Internetzugang der Beschäftigten zu filtern. Falls man als Betriebsrat den Einsatz der Software trotz aller Einwände und Unzulänglichkeiten nicht abwenden kann, empfiehlt sich der Abschluss einer Betriebsvereinbarung mit folgenden Inhalten:

- Das Programm ist so zu konfigurieren, dass keine speziellen Protokolle über abgewiesene Zugriffe der Beschäftigten geführt werden.
- Es gilt der Gleichheitsgrundsatz: Es werden keine unterschiedliche Filterzonen mit unterschiedlichen Freigaben für verschiedene Beschäftigungsgruppen eingerichtet.
- Echtzeit-Anzeigen und Reports werden nicht zur Verfügung gestellt.

In der Vereinbarung können auch die Kategorien der zu sperrenden Webseiten festgehalten werden. Viele Betriebsräte sträuben sich allerdings, denn leicht kann der falsche Eindruck entstehen, dass damit der Betriebsrat die Bevormundungsaktivitäten des Unternehmens unterstützen würde. Ein Lösungsansatz für das Dilemma könnte so aussehen, dass Kategorien zwar nicht grundsätzlich vereinbart werden, dass dem Betriebsrat jedoch im Zusammenhang mit einem umfassenden Informationsrecht die Möglichkeit eingeräumt wird, der Sperrung einzelner Kategorien zu widersprechen.

5. Antiviren-Programme

Seit Computerviren in den 1980er-Jahren erstmals aufgetreten sind, ist die Bedrohung für die Netzwerksicherheit und die Integrität der IT-Ressourcen im Unternehmen immer größer geworden. Die Anzahl der Computerviren und -würmer geht mittlerweile in die Millionen. Professionelle Teams basteln an immer neuen Schadprogrammen, um eine Verbreitung auf weltweit möglichst viele Rechner zu erreichen. Einmal infiziert, ist es ihnen dann möglich, diese Rechner fremd zu steuern, etwa um Spam-Massen-Mailings oder vergleichbare Transaktionen durchzuführen. Auch das Virenschreiben ist zum Geschäft geworden. Im Internet gibt es einen illegalen Markt, in dem die Kontrolle über diese so genannten „Bot-Netze“ zu hohen Preisen vermietet wird.

Den Wettlauf mit neuen Viren und Würmern nehmen die Virenschutzprogramme auf. Sie werden entweder direkt am Arbeitsplatzrechner oder am zentralen Sicherheitssystem installiert. Häufig werden sie auch an beiden Stellen gleichzeitig eingesetzt, und zwar von unterschiedlichen Herstellern, um eine maximale Erkennungsrate zu gewährleisten. Dabei kann im Prinzip jeder Datentransfer und jeder Datenträger, etwa ein USB-Stick, überprüft werden. Das gefährlichste Einfalltor sind aber nach wie vor mit Schadcode versehene E-Mail-Anhänge oder E-Mail-Links, die Sicherheitslücken des Systems nutzen.

Vergleich der Virenmuster

Die Strategie eines Virenschutzprogramms besteht in der Regel aus einem simplen Muster-Abgleich: Es vergleicht, ob ihm bekannte Virenmuster in der zu überprüfenden Datei vorhanden sind. Falls ein Alarm ausgelöst wird, hängt von der Systemkonfiguration ab, was mit der infizierten Datei gemacht werden soll.

Die Virenkontrolle bei E-Mails erfolgt durch Zugriff auf die E-Mail-Inhalte und -Anhänge. Das ist unproblematisch, weil der Zugriff ausschließlich automatisiert durch das System erfolgt, ohne dass eine Person Einsicht in die Kommunikation erhält.

Umgang mit infizierten E-Mails

Datenschutzrechtlich relevant kann jedoch der Umgang mit als infiziert erkannten E-Mails sein. Häufig werden infizierte E-Mails in einen geschützten Quarantänebereich abgespeichert, auf den lediglich die Systemadministration, nicht aber der Absender einer infizierten Mail, zugreifen kann. Hier sollte der Betriebsrat nach Lösungen suchen, die eine Inaugenscheinnahme der Systemadministration ohne Zustimmung der Mailteilnehmer unnötig machen. Dies könnte z. B. durch eine automatische Virenentfernung realisiert werden. Der Einblick in infizierte Mails sollte in jedem Fall nur die Ultima Ratio sein, zuvor ist nach Möglichkeit das Einverständnis des betroffenen Beschäftigten einzuholen. Und selbstverständlich ist die Vertraulichkeit der Nachricht zu wahren.

Regelungsaspekte

Vereinbarungen zum Thema sollten also das Prozedere des automatischen Zugriffs auf die Mails beschreiben, den manuellen Zugriff ausschließen oder zumindest minimieren und die Vertraulichkeit der Nachrichten betonen.

6. Spamfilter-Software

Spam (unerwünschte Werbemail) nervt. Spam belästigt Beschäftigte und kostet dem Unternehmen Arbeitszeit und Speicherplatz. Darf der Arbeitgeber deshalb Anti-Spam-Programme im Unternehmensnetzwerk installieren und konfigurieren, wie es ihm gefällt? Nein – was auf den ersten Blick vielleicht selbstverständlich aussieht, macht beim genaueren Hinsehen eine differenzierte Betrachtung und eventuell den Abschluss einer Betriebsvereinbarung notwendig.

Verfahren zur Erkennung von Spam-Mails

In der Regel wenden Anti-Spam-Programme verschiedene Techniken gleichzeitig zur Erkennung an. Die kombinierten Verfahren bestehen üblicherweise aus:

- der Überprüfung von öffentlichen Listen bekannter Spam-Versender,
- einer Analyse des Nachrichtentextes,
- einer verzögerten Zustellung der E-Mail im Rahmen des so genannten „greylistings“ und

- einem selbstlernenden Spam-Identifikationsprogramm.

Im Falle des Einsatzes eines selbstlernenden Programms muss der Benutzer eigenhändig Spam-Mails markieren. Im Laufe der Zeit „erlernt“ das Programm bestimmte Muster, die mit eingehenden Mails verglichen werden. Ist die E-Mail einem der Muster sehr ähnlich, wird sie als Spam eingestuft.

Falls dieses Verfahren eingesetzt wird, ist die technische Realisierung interessant: Eine Möglichkeit ist, dass für jeden Arbeitsplatzrechner eigene Muster „antrainiert“ werden. Sinnvoller dürfte ein zentrales „Training“ der Antispamsoftware am zentralen Sicherheitsserver sein. Dann wäre zu klären, ob die Beschäftigten weiterhin selbst E-Mails als Spam deklarieren dürfen. Nicht akzeptabel wäre es, wenn die Systemadministration zu diesem Zweck lesenden Zugriff auf Mitarbeitermails erhalten soll.

Umgang mit Spam-Mails

Zu regeln ist weiterhin, was mit einer als Spam gekennzeichneten Mail passieren soll.

- Die unproblematischste Option ist es, die E-Mail zu markieren und dann an den Empfänger durchzustellen, vorzugsweise in ein gesondertes E-Mail-Ablage-Verzeichnis.

- Kritisch ist die Option, die E-Mail zu löschen und dem Empfänger nicht zuzustellen, ein Verfahren, das gegen das Fernmeldegeheimnis verstößt. Eine E-Mail an den persönlichen Account muss grundsätzlich zugestellt werden, anders als bei virenverseuchter E-Mail ist mit der Zustellung auch keine unmittelbare Systemgefährdung verbunden. Dazu kommt das Problem, dass bei falsch markierten Spam-Mails die Mails dann tatsächlich verloren sind.

- Kompromisslinie zwischen diesen beiden Lösungen ist das Markieren und Aussondern der Spam-Mails. E-Mails werden nicht direkt weitergeleitet, sondern irgendwo auf dem Server für eine bestimmte Zeit zwischengelagert und können bei Bedarf von den Beschäftigten eingesehen werden.

Fehlerhafte Kennzeichnung als Spam-Mail

Große Probleme können entstehen, wenn die Spam-Filter zu scharf eingestellt sind. Dann landen erwünschte Mails fälschlicherweise im Spam-Ordner und werden ggf. nicht beachtet. Eine Gegenstrategie ist das Pflegen von so genannten „white lists“. Das sind Adresslisten, die E-Mail-Adressen enthalten, die nie vom System als Spam deklariert werden sollen. In die „white list“ kommen dann z. B. alle Adressen von Geschäftspartnern hinein. Die Gegenstrategie hilft natürlich nicht beim Erstkontakt mit einem neuen Kunden, wenn dessen E-Mail-Adresse bislang unbekannt war.

Geklärt werden sollte in diesem Zusammenhang, ob die Beschäftigten selber „white lists“ pflegen dürfen. Außerdem darf es nicht zu Lasten der Beschäftigten gehen, wenn dienstliche Mails vom System fälschlicherweise als Spam markiert und deshalb übersehen werden.

Fehlinterpretation der Statistiken verhindern

Auch Programme, die zur Spam-Abwehr eingesetzt werden, liefern Reports und Auswertungen. Diese Statistiken können zumindest Laien zu voreiligen und falschen Schlüssen bewegen. „Pass mal auf, wo du dich im Internet so rumtreibst!“ bekommen die geplagten Spam-Opfer dann zu hören. – Blanker Unsinn! – Denn das Surfverhalten hat keinen Einfluss auf die Anzahl von Spam-Mails, die an die Beschäftigten versendet wird.

Der Grund für viele Spam-Mails im Posteingang kann darin liegen, dass eine E-Mail-Adresse auf der Unternehmens-Internetseite veröffentlicht worden ist. Spam-Roboter greifen Webseiten automatisch nach E-Mail-Adressen ab und versenden dann ihren Werbemüll. Virenbefallene Rechner übermitteln ganze Adressbücher an die Spam-Bösewichte. Es gibt viele Möglichkeiten, um ins Netz der Spammer zu geraten und keine, um es wieder zu verlassen. Der Arbeitgeber sollte deshalb versichern, dass er sich mit dem Betriebsrat einig darüber ist, dass sich aus der Anzahl und Art der an die Mitarbeiter versendeten Spam-Mails keine Rückschlüsse auf deren Verhalten ziehen lassen.

Regelungsaspekte

Vereinbarungen sollten sicher stellen, dass beim Einsatz von Antispam-Software die Vertraulichkeit der elektonischen Kommunikation gewahrt bleibt, etwa indem das eingesetzte automatisierte Verfahren beschrieben wird. Für den Verlust von fälschlicherweise als Spam deklarierten Geschäftsmails dürfen Beschäftigte nicht haftbar gemacht werden. Hilfreich ist es, wenn den Beschäftigten Möglichkeiten eröffnet werden, zu „scharf“ eingestellte Spam-Filterregeln zu korrigieren und eigene Whitelists zu pflegen. Und es kann nie schaden, einleitend festzuhalten, dass die Zahl der empfangenen Spam-Mails keine Rückschlüsse auf das (Internet-)Verhalten der Beschäftigten zulässt.

IV. Intranet und Web 2.0

1. Grundlagen

Intranetanwendungen sind so alt wie das Internet. Viele Jahre beschränkte sich die Intranetnutzung der Unternehmen jedoch auf reine Informationsvermittlung. Produktinformationen, der wöchentliche Speiseplan der Kantine, das neueste Grußwort des Vorstandsvorsitzenden wurden inspirations- und lustlos auf den internen Webseiten platziert. Interessant waren die Inhalte nur selten. Und interaktive Inhalte wie Chats oder elektronische Gesprächsforen standen in vielen Unternehmen unter Generalverdacht des unnützen Zeitvertreibs und wurden daher gar nicht erst zur Verfügung gestellt.

Die Zeiten ändern sich. Ausgehend vom Web-2.0-Hype des Internets wird seit einiger Zeit in vielen Unternehmen mächtig Wind um „neue" Intranetanwendungen gemacht. Social-Networking, „user generated content"[16] in Wikis und Webblogs sind die Wundermittel, mit denen der Sprung in die rosige digitale Zukunft endlich glücken soll.

Erfolgreiche Internet-Konzepte

Leider bleibt vom Getöse nach der Umsetzung oft nur ein müdes Lüftchen übrig. Denn die Adaption erfolgreicher Internetideen in den Unternehmensbereich kann nur dann funktionieren, wenn zumindest drei Grundvoraussetzungen gegeben sind:

- Die Verwendung muss freiwillig sein.
- Die Nutzer müssen Zeit haben.
- Die Anwendung muss Spaß machen.

So funktionieren erfolgreiche Internetdienste. Dazu kommt die harte Auslese verschiedener Anbieter mit unterschiedlichen Konzepten, von denen nur die wenigsten langfristig Nutzer an sich binden können.

Fehler bei der Umsetzung im Unternehmens-netzwerk

Bei der Einführung neuer Intranet-Anwendungen entscheiden im Regelfall nicht die zukünftigen Nutzer darüber, mit welcher Software sie arbeiten wollen und mit welcher nicht. Stattdessen werden Direktiven der Chefetage durchgesetzt und gedankenlos über die bestehenden Informations- und Kommunikationsprozesse gestülpt.

[16] Bei „user generated content" werden die Inhalte von Webseiten nicht von speziellen Redaktionsteams, sondern auf freiwilliger Basis von den Benutzern der Seiten geschrieben. Legendärer Vorreiter im Internet ist das Internet-Lexikon Wikipedia.

Zusätzliche Zeit ist für die Nutzung natürlich nicht vorgesehen. Denn die Hochglanzprospekte der Hersteller versprechen dem Unternehmen ja Zeit- und Effizienzgewinn. Spaß soll die Anwendung erst recht nicht machen, jedenfalls nicht absichtlich. Und meistens trifft noch nicht mal das Prädikat „langweilig, aber immerhin schnell“ zu. So manche Intranetanwendung ist allein schon wegen der langen Wartezeiten unbrauchbar.

Kein Wunder, dass sich die meisten Unternehmen unter diesen Voraussetzungen nicht auf ein freiwilliges Zurverfügungstellen der Anwendungen verlassen mögen: Zwang ist Trumpf. Entsprechend frustrierend sind dann die Ergebnisse bei der System-Rückschau nach einem Jahr. Erst recht in einem IT-Umfeld, in dem die Unternehmensleitung auf Überwachung und Kontrolle setzt, statt auf Kreativität und Eigenverantwortung der Beschäftigten.

Alle auf der Intranettechnik basierenden Anwendungen sind grundsätzlich überwachungsgeeignet – bei jedem Aufruf einer Seite können Protokolldaten erzeugt werden. Deshalb haben Betriebs- und Personalräte bei Vereinbarungen nicht nur Einfluss auf den Schutz der Beschäftigten vor Überwachung, sondern auch auf die Rahmenbedingungen des Systemeinsatzes. Sie können daher z. B. die freiwillige Nutzung von Anwendungen vereinbaren. Vorschläge dazu werden für die wichtigsten Intranetanwendungen weiter unten skizziert.

Zunächst soll der Blick jedoch auf den Regelungsbedarf von elektronischen Kalendern gerichtet werden. Auch diese werden natürlich im Umfeld der neuen Web-2.0-Anwendungen eingesetzt. Mitbestimmungsrechtliche Erfahrungen mit elektronischen Kalendern gibt es aber schon länger, so dass auf bewährte und erprobte Regelungsgrundsätze zurückgegriffen werden kann.

2. Elektronische Kalender

Elektronische Kalender werden zum einen als Webanwendung im Intranet genutzt. Häufig werden sie auch als Teil des vom Unternehmen verwendeten E-Mail-Systems (Notes, Outlook) angeboten.

Regelungsaspekte

Eine Regelung sollte vorsehen, dass die Beschäftigten die ausschließliche Oberhoheit über ihre Termine behalten:

- Nur sie selbst sollten darüber entscheiden, welche Termine sie einpflegen.
- Nur sie selbst sollten Einsichts- und Schreibrechte in ihren Kalender an Kollegen vergeben dürfen. (Ausnahmen könnten für Kalender von Arbeitsgruppen vereinbart werden.)

- Insbesondere das Überschreiben von Terminen durch Vorgesetzte sollte technisch ausgeschlossen werden.

Die Bestimmung, dass Beschäftigte über die Aufnahme von Terminen in ihren Terminkalender selbstständig entscheiden, steht in diesem Fall einer freiwilligen Nutzung gleich. Beschäftigte, die den Kalender nicht führen wollen, tragen dann einfach keine Termine ein. Eine verbindliche Verpflichtung zum Führen des Terminkalenders könnte eventuell für Außendienstmitarbeiter erforderlich sein. Der Umfang solcher Ausnahmen sollte in einer Vereinbarung natürlich klar umrissen werden.

Die Termine des Kalenders werden im Regelfall nur für die Zukunft benötigt. Daten, die die Vergangenheit betreffen, sollten nicht bis in alle Ewigkeit aufbewahrt werden. Zu erörtern wäre daher, ob abgelaufene Termine nach Ablauf einer Zeitspanne automatisch aus dem System gelöscht werden sollen oder zumindest den Beschäftigten eine Systemoption eröffnet wird, um alte Termine automatisch löschen zu lassen.

3. Weblogs und Wikis

Weblogs

Ein Weblog, meist abgekürzt als Blog, ist nichts weiter als ein auf einer Webseite geführtes und damit öffentlich (oder betriebsöffentlich) einsehbares Tagebuch oder Journal. Dabei stehen die neuesten Einträge oben und die ältesten unten. Im Unternehmensumfeld werden Blogs immer noch selten angeboten: Das Befüllen des Blogs kostet Zeit. Damit es Leser regelmäßig aufrufen, müssen Blogs regelmäßig Einträge enthalten. Und diese Beiträge müssen nicht nur fachlich relevante Informationen beinhalten, sondern nicht zuletzt auch interessant geschrieben sein. Blogs können von den Lesern kommentiert werden. Unternehmen, die Blogs einsetzen, öffnen diese in der Regel für Internetnutzer und sehen darin ein Instrument zur Kundenbindung.[17]

Wikis

Ein Wiki ist eine untereinander stark verlinkte Sammlung von Internet- oder Intranet-Seiten, an denen die Benutzer in Echtzeit ohne technische Erfahrungen Änderungen vornehmen oder auch neue Seiten erstellen können. So ist es möglich, dass mehrere Menschen gemeinsam an einem Thema arbeiten und ihr Wissen zusammentragen. Das ist auch der Grund, warum die Wissensmanagement-Protagonisten so scharf auf die neue Software-Spezies sind.

Es gibt Dutzende von Softwareprodukten, ein großer Teil davon ist Freeware, also kostenlos. Das Internet-Lexikon Wikipedia[18] basiert auf einer solchen Software. Erst allerdings, seit auch Microsoft eine spärliche Wiki-Version in sein Office-Paket integriert hat, werden Wikis in den Unternehmen in teilweise großem Umfang angeboten.

[17] Eine Link-Liste deutscher Corporated Blogs befindet sich rechts auf http://www.businessblogstudies.blogspot.com/.
[18] Siehe unter http://de.wikipedia.org.

Die meisten Systeme unterstützen eine Versionsverwaltung, d. h. die Benutzer können Änderungen nachvollziehen. Auch lassen sich alte Zustände wiederherstellen. Mit entsprechenden Listen-Funktionen lässt sich auch nachvollziehen, welche User besonders aktiv sind, oder wann Artikel erstellt oder verändert worden sind. Aus Mitbestimmungssicht kritisch können auch Möglichkeiten zur Bewertung der Artikel werden, wenn z. B. Autoren schlecht bewerteter Artikel zur Rede gestellt werden sollen.

Die ursprüngliche Idee von Wikis beinhaltet, wirklich allen Benutzern das Recht zu gestatten, Inhalte zu bestimmten Themen zu schreiben und auch verändern zu können. Im Unternehmensumfeld wird der Zugang zu Wikis jedoch meist auf bestimmte Benutzergruppen eingeschränkt. Wenn der Spaß an der Sache ganz verloren gehen soll, erhalten die User nur eingeschränkte Rechte oder die geschriebenen Artikel werden vor der Veröffentlichung noch von der „Unternehmenszensur“ kontrolliert.

Die Probleme, die bei der Nutzung von Wikis anfallen, hängen zuallererst vom Umfeld ab, in dem sie eingesetzt werden. Stimmt die Unternehmenskultur nicht, so könnte das Führen von Wissenslexika dazu führen, dass die ihres Wissens „beraubten“ Beschäftigten leichter austauschbar sind, denn deren ursprüngliches Wissen wäre mit einem Wiki gegebenenfalls auch von weniger qualifizierten Arbeitskräften abrufbar. Wahrscheinlicher ist allerdings, dass die Wikis nur mit belanglosen Informationen gefüllt werden. Gleichwohl kann ein Wiki für Beschäftigte ein hilfreiches Arbeitsmittel darstellen, das im besten Fall schnelle und kompetente Informationen anbietet.

Regelungsaspekte

Betriebliche Regelungen zum Einsatz von Wikis sollten daher den Aspekt der eingangs des Kapitels erwähnten, freiwilligen Nutzung betonen. Denkbar ist z. B., dass Wikis einzelnen Arbeitsgruppen zur Nutzung angeboten werden, wobei die Gruppen dann selbstständig entscheiden, ob und inwieweit sie ein Wiki für die Projektarbeit nutzen wollen. Besonders Erfolg versprechend soll der Einsatz in technischen Bereichen sein, etwa Wikis für Forscher und Programmierer.

Informieren sollte man sich als Betriebsrat in jedem Fall, ob und welche personenbezogene Listen erstellbar sind. Während die Listen bei überschaubarer Gruppengröße kaum zu Problemen führen dürften, könnten sie bei weiter reichender Verfügbarkeit durchaus zu Verhaltenskontrollen genutzt werden, so dass sie besser deaktiviert werden sollten.

Vorabkontrollen von Artikeln sollten nur für genau benannte Fragen und Themenbereiche zugelassen werden, falls etwa rechtsverbindliche Informationen zur Verfügung gestellt werden sollen und diese vor Veränderungen geschützt werden sollen.

Die Option, Beiträge kommentieren zu können, dürfte in der Regel sinnvoll sein. Einfache Bewertungen, etwa nach einem Schulnoten-Raster, könnten zu Problemen führen und sollten daher nur in Ausnahmefällen zugelassen werden.

Weil zum Wiki-Einsatz in den Betrieben bislang nur wenige Erfahrungen bestehen, wäre auch zu überlegen, die getroffenen Regelungen in einer vorläufigen Pilot-Vereinbarung unterzubringen, um nach Ablauf eines Jahres die Erfahrungen Revue passieren zu lassen und über die getroffenen Regelungen neu zu beraten.

4. Webkonferenzen

Webcams (kleine Videokameras für Computer) und Mikrofone finden zunehmend Einzug in die Unternehmen. Häufig sind sie bereits serienmäßig in Notebooks enthalten, aber Geräte für den Anschluss an Desktop-Computer kosten heutzutage keine 100 Euro mehr.

Videokonferenzen können daher mit Webcams erheblich weniger aufwändig durchgeführt werden als früher. Mit einer entsprechenden Software kann man zudem Präsentationen in die Videokonferenz einbinden, online-Dokumente direkt mit den Teilnehmern diskutieren (am Telefon oder im Chat) oder auch Schulungen durchführen. Im Fachjargon spricht man von Webkonferenzen.

Aktivieren von Kamera und Mikrofon

Zu regeln ist zuoberst, dass alle Teilnehmer einer Webkonferenz zu jeder Zeit die volle Kontrolle über ihre Kamera und die Mikrofonfunktionen haben. Das ist nicht selbstverständlich, denn natürlich gibt es auch bei Webkonferenz-Tools differenzierte Berechtigungsstufen. Als Betriebsrat sollte man sich deshalb genau ansehen, welcher Nutzer welche Funktionen nutzen oder freischalten darf und wer nicht. Die Kameras und die Mikrofone sollten sich außerdem bei Systemabstürzen oder bei Beendigung der Konferenz automatisch abschalten, damit nicht unbeabsichtigt Daten übertragen werden. Und die aktivierte Bild- oder Tonübertragung sollte jederzeit für die Teilnehmer deutlich sichtbar sein.

Eine Vereinbarung sollte festhalten, dass Webcams nur so aufgestellt werden dürfen, dass keine unbeteiligten Personen dauerhaft vom Blickfeld der Kameras erfasst werden. Anwesende Personen sind über die aktivierte Kamerafunktion zu informieren. Falls Freisprechfunktionen genutzt werden, ist der Konferenzteilnehmer ebenfalls zur Information der im Raum anwesenden Beschäftigten zu verpflichten.

Kontrolle von Fernzugriffen

Technisch ist die Nutzung von Online-Präsentationen mit einem (auf die Webpräsentation begrenzten) Zugriff auf die Rechner der Konferenzteilnehmer verbunden. Volle Kontrolle der Konferenzteilnehmer über die Fernsteuerungsfunktionen, etwa die Pflicht zur Freigabe von Fremdzugriffen auf den eigenen Rechner ist daher ebenfalls unerlässlich.

Aus Mitbestimmungssicht ein problematisches Feature ist die Möglichkeit, Meetings aufzuzeichnen. Damit soll z. B. Teilnehmern, die zeitlich verhindert sind, ermöglicht werden, sich nachträglich über die virtuellen Meetinginhalte zu informieren. Auf der sicheren Seite ist man als Betriebsrat, wenn man die Nutzung solcher Mitschnittmöglichkeiten untersagt, mindestens aber davon abhängig macht, dass alle Beteiligten ihr vorher ausdrücklich und in jedem Einzelfall zugestimmt haben.

Reports und Logs

Nach der Webkonferenz, möglicherweise auch schon während der Konferenz, stehen dem Veranstalter vermutlich standardmäßig Reports zur Verfügung, etwa über die Teilnehmer oder über deren Anmeldezeiten. Alle zugelassenen personenbezogenen Auswertungen sollten in einem abschließenden Katalog in der Vereinbarung aufgeführt werden. In diesem Sinne sollten generell nach Beendigung der Webkonferenz weitere kritische Informationen, z. B. Chat-Protokolle, automatisch vom System gelöscht werden.

Abschließend sollte man den Qualifizierungsbedarf der Beschäftigten nicht unterschätzen. Die auf dem Markt angebotene Software ist alles andere als leicht bedienbar, und es ist eine Selbstverständlichkeit, dass die Beschäftigten vor allem die Kontroll- und Anzeigefunktionen der eingesetzten Kameras und Mikrofone kennen und beherrschen müssen.

Regelungsaspekte

Der Vereinbarungsumfang hängt letztlich von den tatsächlich zur Verfügung stehenden Leistungsmerkmalen und Funktionen der eingesetzten Webkonferenzsoftware ab. Sinnvoll erscheint es allerdings, mindestens die folgenden Punkte in eine Vereinbarung aufzunehmen:

- Unternehmensbereiche benennen, in denen die Software eingesetzt werden soll
- Einschalten und Steuerung von Mikrofon und Kameras erfolgt nur durch den jeweiligen Teilnehmer
- Fernzugriff auf Rechner nur mit Zustimmung des Nutzers
- Einsatzbedingungen von Mikrofonen und Kameras
- Regelungen für das Aufzeichnen und Speichern von Meeting-Inhalten
- Umgang mit Reports und Auswertungen

V. Netzwerksicherheit und Rechner-Administration

1. Grundlagen

Wenn das eigene Netzwerk ausfällt, geht in den meisten Unternehmen nichts mehr: Kundenanfragen versickern, Fristen werden versäumt, Beschäftigte sitzen hilflos hinter ihren Rechnern, weil sie Dokumente auf Netzwerk-Laufwerken nicht aufrufen können und ihre Sachbearbeitungsprogramme nur mit Netzwerkanbindung funktionieren.

Das Aufrechterhalten des Netzwerkbetriebs ist daher oberstes Ziel einer jeden IT-Abteilung. Die technischen Risiken werden dabei durch den Einsatz von immer komplexer werdenden Softwareprogrammen nicht geringer. Neue kritische Sicherheitslücken werden zwar von den Softwareherstellern von Zeit zu Zeit durch das Bereitstellen von Versionsupdates, so genannten „Patches“, geschlossen. Aber die Zeit zwischen Entdeckung der Sicherheitslücke und ihrer Schließung können externe Angreifer für Einbrüche in die unternehmenseigene Systemlandschaft nutzen. Nicht ausgeschlossen werden kann weiterhin, dass die Softwaresysteme und die Datensicherheit von den Beschäftigten selbst gefährdet werden. Vorsätzlich, wenn z. B. versucht wird, fremde Passwörter zu erspähen und auszuprobieren, oder aus Unwissenheit, wenn ihnen nicht bekannt ist, dass bestimmte Aktivitäten zu Sicherheitsproblemen führen könnten.

Unternehmen setzen zur Überwachung und zur Abwehr von Cyberattacken hochspezialisierte Programme ein, mit denen die Datenströme des Netzwerks und die eingesetzte Hardware analysiert und auf verdächtige Unregelmäßigkeiten hin untersucht werden. Leider eignen sich die auf dem Markt befindlichen Programme nicht nur zum Aufspüren von Sicherheitsrisiken, sondern auch zur Überwachung der Netzwerkaktivitäten der Beschäftigten, wenn z. B. das Hören von Internet-Radio oder die Übertragung von bestimmten Schlüsselworten, die in einer Verbotsliste hinterlegt sind, Alarm auslösen. Eine betriebliche Regelung dieser „Intrusion-Detection-Systeme“ wird im Weiteren skizziert.

Leider vernachlässigen viele Unternehmen angesichts des großzügigen Technikeinsatzes die organisatorischen Ansätze zur Verbesserung der Systemsicherheit. Dabei wird gerne übersehen, dass die ausgefeilteste Sicherheitssoftware wirkungslos bleibt, wenn Passwörter unter die Tastaturen geklebt werden oder bereits Praktikanten der Zugriff auf sensible Daten der Unternehmenssicherheit ermöglicht wird. In einem eigenen Abschnitt zeigen wir daher Grundzüge eines Sicherheitskonzeptes auf.

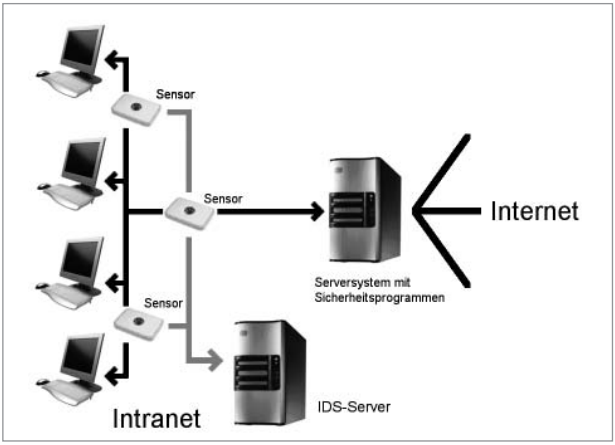
Mit einem anderen Hintergrund werden Systeme zur Fernsteuerung von Arbeitsplatzrechnern und zur Softwareverteilung eingesetzt: Sie sollen die Arbeit der Systemadministration erleichtern und sie von lästiger Routinearbeit befreien, indem sie etwa das automatisierte ferngesteuerte Aufspielen neuer Softwareversionen an den Arbeitsplatzrechnern ermöglichen, ohne dass die Administratoren körperlich die betreffenden Rechner aufsuchen müssen. Auch in diesen Fällen ist der Grat zwischen einem arbeitserleichternden Systemeinsatz und einer missbräuchlichen Überwachung der Kollegen mit den eingesetzten Softwareprogrammen schmal. Denn dieselben Systeme können zum heimlichen Aufschalten auf die Arbeitsplatzrechner verwendet werden oder umfassende Protokolle über die Benutzung von Programmen liefern.[19]

2. Intrusion Detection Systeme (IDS)

Übersetzen lässt sich das Wortungeheuer Intrusion-Detection-Systeme (IDS) etwas umständlich mit „Einbruch-Aufspür-System". IDS-Programme untersuchen den kompletten Netzverkehr innerhalb des Unternehmens sowie die ein- und abgehenden Datenströme auf Hackerangriffe und weitere Aktivitäten, die die Systemsicherheit des Netzes gefährden könnten. Mails, Webseitenaufrufe, Downloads, Chatsysteme – alles wird untersucht. Erkennt das System ein in der IDS-Datenbank hinterlegtes Angriffsmuster auf das Netzwerk, so wird ein Protokolleintrag angelegt und die Systemadministration alarmiert. Je nach System und Konfiguration können auch E-Mail-Benachrichtigungen oder automatisch generierte SMS an den Systemadministrator ausgelöst werden.

Systemarchitektur

Das Gesamtsystem besteht technisch gesehen aus einigen Sensoren, die innerhalb des Netzwerkes installiert werden und dort den Netzverkehr überwachen. Bei Treffern wird das Hauptsystem auf dem IDS-



[19] Mehr Hintergrundinformationen auf http://www.tse.de/papiere/internet und netze/netzwerk/.

Server informiert, in dem die Protokolleinträge zusammenlaufen. Hier können die Daten dann von der Systemadminstration mehr oder weniger eingehend analysiert werden.

Fehlalarme

Das Belauschen des Datenverkehrs erfolgt durch ständige Vergleiche mit bekannten Angriffsmustern (Signaturen). Leider sind die Signaturen nicht immer treffgenau: Deshalb werden in der Standardkonfiguration in der Regel viel zu viele Fehlalarme ausgegeben. Der Aufwand der deshalb erforderlichen Feinjustierung des IDS wird häufig unterschätzt. Eine ungewollte Datenflut durch Fehlalarme ist dann die Folge. Im schlimmsten Fall kann eine schlecht konfigurierte IDS dann selbst zum Sicherheitsrisiko werden, dann nämlich, wenn dieses bei gezieltem Dauerbombardement von Hackern unter der Arbeitslast „in die Knie geht“ und damit das Netzwerk verstopft wird.

Überwachung von Beschäftigten

Ein besonderes Risiko für die Beschäftigten liegt in mit IDS überwachten Netzwerken darin, dass die eingesetzten Signaturen nicht nur zur Abwehr tatsächlich existierender Gefährdungen einsetzbar sind. Mit Signaturen kann der Datenverkehr nach jedem denkbaren Kriterium überprüft werden: Hört der Mitarbeiter Internetradio, benutzt er einen Chat, sind „verbotene“ Worte in einer E-Mail enthalten? Mit wenig Aufwand kann ein versierter Systemoperator Signaturen ändern oder eigene Signaturen aufsetzen.

Ein weiteres Problem kann sich für die Persönlichkeitsrechte der Mitarbeiter ergeben, wenn die IDS-Software anhand von Protokollen oder anderen Merkmalen ein „Normalverhalten“ ermittelt und dieses mit dem tatsächlichen Verhalten der Nutzer vergleicht – Abweichungen werden natürlich protokolliert. Schon könnte der Mitarbeiter, der Internetseiten ausnahmsweise vor 8.00 Uhr morgens aufgerufen hat, unter Verdacht (und im IDS-Protokoll) stehen.

Regelungsaspekte

Es gibt kaum Erfahrungen mit betrieblichen Regelungen. Unser Vorschlag beruht auf einer Momentaufnahme: Die Softwaregattung entwickelt sich jedoch ständig weiter, und es ist nicht auszuschließen, dass in den nächsten Jahren neue kritische Funktionalitäten in die Systeme integriert werden. Wie immer gilt es, sich sachkundig zu machen und sich umfassend zu informieren. Eine Regelung dieses hochsensiblen Systems könnte folgende Eckpunkte enthalten:

- Das IDS-System wird ausschließlich zum Zweck der gezielten Erkennung von Angriffen und sonstigen Ursachen, die die Sicherheit und Leistungsfähigkeit des Netzwerks gefährden, eingesetzt. Eine Analyse des Netzverkehrs von Beschäftigten darf demnach nur dann vorgenommen werden, wenn sicherheitsgefährdende Aktivitäten vorliegen. Ein bloßer Verstoß von Beschäftigten gegen eine wie auch immer ausgestaltete Unternehmensrichtlinie, kann daher nicht Gegenstand weitergehender Analysen sein, wenn diese nicht die Systemsicherheit gefährden.

- Funktionen, die vorgebliches Normverhalten mit dem tatsächlichen Verhalten der Beschäftigten abgleichen, werden nicht eingesetzt.

- Der Umfang der Protokollierung wird vereinbart: Datum und Uhrzeit, Kennung von Sender und Empfänger, Kennung der Ports und des Übertragungsprotokolls, Menge der übertragenen Daten und ID der auslösenden Signatur. Die Protokolldaten werden nach spätestens vier Wochen gelöscht oder überschrieben.

- Der Kreis der zugriffsberechtigten Administratoren wird besonders eng begrenzt und z. B. namentlich in einer Anlage aufgeführt.

- „Stufenverfahren" für die Protokolldatenanalyse festlegen: Die Datenanalyse erfolgt demnach zunächst ohne Identifizierung einzelner Mitarbeiter oder Mitarbeitergruppen durch die Systemadministratoren. In der Vereinbarung werden Auffälligkeiten benannt, die eine weitergehende (auch personenbezogene) Datenanalyse nach sich ziehen können, etwa wenn ein Rechner innerhalb einer kurzen Zeitspanne ein hohes Traffic-Volumen erzeugt oder innerhalb einer kurzen Zeitspanne mit vielen Kommunikationspartnern verbunden ist. In diesem Fall wird der Systemadministrator die Situation direkt mit dem betroffenen Mitarbeiter klären, ohne dass weitere Stellen benachrichtigt werden. Kann eine Klärung nicht erfolgen oder liegt nach Ansicht des Administrators ein schwerwiegender sicherheitsrelevanter Verstoß vor, werden Betriebsrat und Arbeitgeber über den Fall informiert, allerdings ohne Namensnennung. Erst, wenn Betriebsrat und Arbeitgeber in einer gemeinsamen Bewertung zu der Erkenntnis gelangen, dass eine weitere Datenanalyse gerechtfertigt ist, wird der Name des Mitarbeiters deanonymisiert. Dem Mitarbeiter wird umgehend die Möglichkeit gegeben, zu den Vorwürfen Stellung zu nehmen.

- Für den Fall, dass das vereinbarte Verfahren nicht eingehalten wird, wird ein Beweisverwertungsverbot (siehe Kapitel II Ziffer 3) vereinbart.

Problematisch bleibt, dass Betriebs- oder Personalräte nicht überprüfen können, ob sich die Administration tatsächlich an die Bestimmungen der Vereinbarung hält; ein Einwand, den man auch bei 95% aller anderen IT-Systeme anbringen kann. Sie können allerdings im Stufenverfahren eine Deanonymisierung gegenüber dem Arbeitgeber verhindern, und sie können auf das Beweisverwertungsverbot verweisen und personell mitentscheiden, welche Administratoren Zugriff auf das System erhalten.

Intrusion Prevention Systeme

Intrusion-*Detection*-Systeme (Einbruchs-Erkennungs-Systeme erkennen Angriffe, aber sie verhindern sie nicht. Auf dem Markt befindliche Intrusion-*Prevention*-Systeme (Einbruchs-Verhinderungs-Systeme) sollen diese Lücke schließen, und schaffen dabei oft mehr Probleme, als sie lösen: Denn nun wird geblockter Datenverkehr nicht nur protokolliert, sondern es werden vom System Gegenmaßnahmen ergriffen: Dies kostet Rechenpower. Der Automatismus kann den Server überfordern und damit ganze Netzwerkbereiche lahm legen. Der Einsatz automatischer Gegenmaßnahmen ist deshalb mit ganz erheblichen Anpassungen und Überprüfungen der Einstellungen durch die Systemadministration verbunden. Zusätzlicher Regelungsbedarf kann entstehen, wenn die Beschäftigten durch falsch eingestellte Automatismen in der Ausübung ihrer Tätigkeiten behindert werden.

3. Organisatorische Regelungen

Die Sicherheit des Computer-Netzwerks eines Unternehmens ist kein Thema, das ausschließlich technisch gelöst werden kann. Jedes Sicherheitssystem ist leider nur so gut wie sein schlechtestes Teil. Dafür wird von den Verantwortlichen gern das berühmt-berüchtigte menschliche Versagen als Erklärung herbei bemüht. Doch oft sind es strukturelle Schwachstellen, die für den mangelhaften Schutz verantwortlich zu machen sind.

Gemeinsame Verantwortung

Selbstverständlich sollten sich die Beschäftigten an entsprechende Sicherheitsvorgaben beim Umgang mit den Systemen halten. Regelungen und Anweisungen dürfen jedoch nicht einseitig Pflichten und Haftungsrisiken auf die Beschäftigten abwälzen. Stattdessen hat das Unternehmen dafür zu sorgen, dass die Beschäftigten ausreichend qualifiziert werden und ein angemessenes Risikobewusstsein im Umgang mit den IT-Systemen entwickeln. Weiterhin müssen die technischen und natürlich auch die personellen Voraussetzungen geschaffen werden, um einen sicheren Betrieb von Software im Netzwerk zu gewährleisten. Wer auf billige Aushilfskräfte und Praktikanten setzt, spart am falschen Ende. Nur qualifiziertes IT-Personal erreicht adäquate Sicherheitsstandards.

Regelungsaspekte

Die Einflussmöglichkeiten der Mitbestimmung sollen an dieser Stelle nur stichwortartig und auszugsweise skizziert werden:

- Personenbezogene Daten sind grundsätzlich als vertrauliche Information einzustufen. Ein Zugriff ist nur für vom Informationseigner legitimierte Personen vorzusehen. Ein Zugang zu Informationen erfolgt nur in dem Maße, wie es für die Erfüllung der Arbeit erfor-

derlich ist. Auch die Berechtigungsvergabe hat in diesem Sinne zu erfolgen. Obligatorischer Einsatz von Bildschirmschonern mit Passwortschutz.

- Verfahren für Berechtigungen bei Versetzungen oder Verlassen des Unternehmens. Zeitlich befristete Berechtigungen bei Projektarbeit. Vier-Augen-Prinzip. Personalisierungspflicht für alle Accounts, Unzulässigkeit von anonymen Accounts (z. B. Administrator für Windows). Besonderes Genehmigungsverfahren und Geheimhaltungsverpflichtung für Nutzer von Fremdfirmen.

- Verbot der Umgehung von Autorisierungsmechanismen, Hacking-Verbot.

- Passworte sollten von den Benutzern auf ihre Qualität geprüft werden können. Persönliche Kennworte dürfen nicht an andere Personen weiter gegeben werden. Höchstgrenze für fehlgeschlagene Zugangsversuche. Sonderregeln bei biometrischen Verfahren. Keine Speicherung von Passwörtern im Klartext in den Systemen.

- Automatischen, unumgehbaren technischen Virenschutz ergänzen um Handlungsanleitungen für die Beschäftigten für Verdachtsfälle.

- Besonders, wenn unaufmerksames Mitarbeiterverhalten mit großen Haftungsrisiken verbunden ist, ist zu überprüfen, ob nicht mit Hilfe von geeigneten technischen Lösungen ein gleiches oder besseres Sicherheitsniveau erreicht werden kann. (Beispielsweise sollte der BR die Verschlüsselung von Notebook-Festplatten statt einer Mitarbeiterhaftung bei Diebstahl fordern.)

- Automatische Datensicherung. Regelungen für persönliche Speicherbereiche und besondere Verschwiegenheitsverpflichtung der mit Aufgaben der Datensicherung betrauten Personen, falls sie Einblick in vertrauliche, nicht für sie bestimmte Daten erhalten haben.

- Eindeutige Zuständigkeit für Systeme. Deaktivieren nicht gebrauchter Dienste und Programme. Protokollierung sicherheitsrelevanter Ereignisse.

- Besonderer Zutrittsschutz zu den Server-Räumen. Hinreichende Qualifizierung der Beschäftigten.

4. Remote Control – Software zur Fernsteuerung

Eine Vielzahl von Programmen bietet mittlerweile Funktionen an, Rechner fernzusteuern und sich auf die Monitore der Beschäftigten aufzuschalten. Heimlichkeiten und Mitarbeiterüberwachung durch die Hintertüren des Unternehmensnetzwerks müssen dabei unbe

dingt verhindert werden. Zum Glück lassen sich die meisten Produkte entsprechend konfigurieren, und wer den Funktionsumfang mit einer Betriebsvereinbarung an „die kurze Leine“ nimmt, der kann mit einem unproblematischen Einsatz im Unternehmensalltag rechnen.

Der Remote-Control-Zugriff kann, je nach eingesetztem System und Konfiguration, sehr weitreichende Möglichkeiten der Fernsteuerung umfassen. Mit entsprechenden Rechten ausgestattet, kann Einsicht in Dateien und Verzeichnisse genommen werden, Dateien können verändert oder gelöscht werden, der Bildschirminhalt des entfernten Monitors kann übernommen werden, Programme können bedient, aufgerufen oder beendet werden, Rechner können runtergefahren oder neu gestartet werden.

Soweit die Programme lediglich dazu verwendet werden, technische Serversysteme der IT zu warten, ist der Einsatz aus Mitbestimmungssicht unproblematisch.

Regelungsaspekte

Regeln müssen hingegen aufgestellt werden, wenn mit Hilfe der Programme auf die Arbeitsplatzcomputer der Beschäftigten zugegriffen werden soll. Denn ihr Einsatz kann unter bestimmten Umständen tatsächlich sinnvoll sein: Hat ein Beschäftigter Probleme mit seinem Rechner und der darauf laufenden Software, benötigt er also Hilfe, so kann er einem zuständigen Kollegen in der Systemadministration Zugriff auf seinen Rechner einräumen. Dieser muss dann nicht persönlich am störrischen Rechner auftauchen, sondern kann online eine Fehleranalyse vornehmen oder zur Reparatur schreiten. Genau diese Zweckbestimmung sollte in einer entsprechenden Vereinbarung auftauchen.

Grundsatz des Systemeinsatzes sollte weiterhin sein, dass alle Aktionen der Systemverwaltung für den Hilfe suchenden Beschäftigten transparent bleiben, das „Aufschalten“ auf den Rechner nur unter völliger Kontrolle dieses Mitarbeiters durchgeführt werden kann und von diesem explizit freigegeben werden muss. Eine entsprechende Konfiguration kann bei fast allen auf dem Markt befindlichen Systemen vorgenommen werden. Andernfalls bleibt nur die Ablehnung der Systemeinführung. In diesem Sinne sollte der Fernzugriff jederzeit deutlich am Bildschirm des Benutzers signalisiert werden und durch den Benutzer abzubrechen sein.

Vereinbart werden sollte zudem, dass der Bildschirm des Benutzers während des Zugriffs nicht verdunkelt wird und die Inhalte der Zwischenablage für Zugriffe tabu bleiben. Wie so oft sind technische Lösungen rein organisatorischen Regelungen vorzuziehen.

Erfolgte Zugriffe oder Zugriffsversuche können bei den meisten Systemen protokolliert werden, um heimliches Aufschalten im Nachhinein aufzuspüren. Zu vermuten ist allerdings, dass ein Mitarbeiter

der Systemadministration, der sich über alle Bestimmungen hinweg setzt und die Aufschaltfunktion heimlich nutzt, auch die Logs manipulieren würde. Entsprechende Vereinbarungen sind also nur sinnvoll, wenn durch eine entsprechende Arbeitsorganisation in der Systemadministration sichergestellt ist, dass die berechtigten Personen keine Zugriffsmöglichkeit auf die Log- und Konfigurationsdaten des Remote-Control-Systems besitzen.

Erweiterte Funktionen

Zu beachten ist, dass auch der Funktionsumfang dieser Systeme immer mächtiger wird. Viele Systeme unterstützen mittlerweile Kommunikationskanäle wie Chat, Instant Messaging oder Skype in Zusammenhang mit automatischen Statuslisten, die ggf. weitere Regelungen notwendig machen. Und oft sind die Fernsteuerungsprogramme nur die Spitze eines Eisberges und Teil eines weit umfangreicheren Softwarepakets, das im Unternehmen zum Einsatz kommt.

5. Inventarisierung, Lizenzkontrolle und Softwareverteilung

Den Überblick über eingesetzte Software und Hardware zu behalten, fällt im meist über Jahre gewachsenen System-Dschungel eines Unternehmens nicht immer leicht. Irgendwann kommt dann der Zeitpunkt, dass die IT-Verantwortlichen mit Hilfe von neu angeschafften Komplettsystemen „klar Schiff“ machen wollen. In der Regel sollen die Systeme Antworten auf folgende Fragestellungen geben bzw. folgende Aufgaben bewältigen:

- Inventarisierung von Hardware: Welche Rechner hängen mit welchen Teilkomponenten (Prozessor, Speicherchips, Laufwerke etc.) im Netzwerk? Müssen Teilkomponenten ausgetauscht werden?
- Inventarisierung von Software: Welches Betriebssystem und welche Softwareprogramme sind mit welchen Versionsständen auf den Rechnern des Netzwerkes installiert? Werden diese Programme von ihren Benutzern verwendet?
- Lizenzkontrolle von Software: Wie viele Softwarelizenzen wurden zu den auf den Arbeitsplatzrechnern eingesetzten Programmen erworben? Müssen neue Lizenzen erworben werden oder sind Programme auf Arbeitsplatzrechnern überflüssigerweise installiert?
- Verteilung von Software: Automatische Installation und Wartung von neuen Softwareversionen über das Netzwerk. Gegebenenfalls auch Deinstallation von Programmen.

Leider übersteigt der Funktionsumfang der Systeme in den meisten Fällen die Funktionalitäten, die notwendig wären, um die aufgeführten Aufgaben zu bewältigen. Fast immer ist der Umfang der bei den Inventarisierungsvorgängen aufgezeichneten Daten in der Standardkonfiguration sehr detailliert. Sie lassen dann sekundengenaue Rückschlüsse

auf das Verhalten der Beschäftigten zu: Wann wurde ein Programm vom Benutzer aufgerufen? Wann wurde es beendet? Wie oft wurde das Programm in der letzten Woche verwendet?

Die umfangreichen Auswertungsmöglichkeiten machen die Aufgabe für Betriebs- und Personalräte nicht leicht. Und besonders kritisch wird es für die Beschäftigten, wenn der Arbeitgeber mit Hilfe des Inventarisierungssystems unerlaubt installierte Programme aufspüren will und sich arbeitsrechtliche Maßnahmen gegen die „Sünder" vorbehalten will. Beschäftigte, die sich selber Hilfsmittel zur Unterstützung ihrer Arbeit, vielleicht ein alternatives Programm zum Ansehen von PDF-Dateien, installiert haben, können so leicht unter Druck geraten.

Zweck-bestimmung

Regelungen sollten daher zunächst die Zweckbestimmung der Systeme deutlich herausstellen. Und die besteht aus Inventarisierung und/oder Lizenzabgleich. Eine gegen die Beschäftigten gerichtete Missbrauchskontrolle gehört selbstverständlich nicht dazu.

Wichtig ist es außerdem, sich über den Leistungsumfang des installierten Programmpakets vollständig zu informieren. Systemmodule, die im Rahmen der Vereinbarung nicht explizit beschrieben werden, dürfen nicht eingesetzt werden.

Hardware-Inventarisierung

Aus Mitbestimmungssicht vergleichsweise unproblematisch ist die Hardware-Inventarisierung. Ausgestattet mit allen relevanten Informationen über die technische Ausstattung eines Rechners, kann die Systemadministration ggf. schneller auf Probleme und Fehlermeldungen von Beschäftigten reagieren. Zum Beispiel könnte der Grund für lange Antwortzeiten in Anwendungssystemen in defekten Memory-Chips liegen. Ein falsch installierter Treiber kann der Grund für eine fehlerhafte Druckerausgabe sein. Alles keine Informationen, die aus Sicht der Beschäftigten kritisch sind.

Verhindert werden sollte jedoch, dass die An- und Abmeldezeiten der Beschäftigten an den Rechnern aufgezeichnet werden, zumindest aber klargestellt werden, dass diese Zeiten nicht mit Daten aus anderen Systemen (z. B. Zeiterfassung) verknüpft werden dürfen.

Gegebenenfalls ist im Zusammenhang mit der Hardware-Inventarisierung noch eine Überwachungsmöglichkeit der Systemkomponenten verbunden, mit der technische Server auf ihre Verfügbarkeit getestet werden. Gegen Technik, die Technik überwacht, ist nichts einzuwenden.

Software-Inventarisierung und Lizenzkontrolle

Zur Software-Inventarisierung entsteht erheblich größerer Regelungsbedarf. Im Rahmen der automatisierten Suchläufe dürfen nur ausführbare Programme und deren Konfigurationsdaten, darüber hinaus aber keine Inhalte von Dateien, durchsucht werden. Verzeichnisse von gelöschten Dateien („Papierkorb") und temporäre Verzeichnisse werden nicht durchsucht.

Der Umfang der jeweils vorgenommenen Protokolleinträge sollte dokumentiert und auf die tatsächlich benötigten Informationen beschränkt werden. Viele Systeme zeichnen beispielsweise Nutzungszeiten der Softwareprogramme je Anwender auf. Zeitstempel darüber, von wann bis wann Programme aufgerufen worden sind, sind in jedem Fall überflüssig und für die Inventarisierung nicht notwendig. Ausgangspunkt für die Verhandlungen sollten daher nur sehr wenige Protokolldaten sein. Ergänzungen müssen dann von der Arbeitgeberseite vorgetragen und ihre Erforderlichkeit begründet werden. Vorschlag:

- Name der Datei,
- Verzeichnispfad der Datei und
- erste Programmzeile des Programmcodes (dient zur Ermittlung der Versionsnummer der Software).

Weiterhin ist das Ausmaß der erlaubten Auswertungen zu begrenzen. Vor allem Benutzerkennungen dürfen nur im Einklang mit der Zweckbestimmung durch die zuständigen Systemadministratoren verwendet bzw. ausgewertet werden.

Information der Beschäftigten

Das Unternehmen sollte außerdem mit offenen Karten spielen. Empfehlenswert ist deshalb eine Passage, wonach die Benutzer vor dem Suchlauf rechtzeitig informiert werden müssen, auf die Probleme im Umgang mit unlizensierter Software hingewiesen werden und dass die eingesetzte Software im Rahmen der Inventarisierung überprüfbar ist.

Für den Fall, dass unlizensierte Software gelöscht werden soll, könnte festgehalten werden, dass die Nutzer rechtzeitig vor dem Löschvorgang eine E-Mail mit einer entsprechenden Ankündigung erhalten und gleichzeitig darauf hingewiesen werden, was sie tun können, um die Löschung zu verhindern. Es könnte ja sein, dass es sich um ein dringend benötigtes Programm zur Unterstützung der Arbeit der Beschäftigten handelt.

Softwareverteilung

Der Betriebsrat sollte darauf achten, dass die Verteilung von Software und Softwareupdates über das Netzwerk ausschließlich auf automatischem Wege erfolgt. Manuelle Zugriffe auf die Verzeichnisse der Beschäftigten durch die Systemadministration sollten ausgeschlossen werden, zumindest jedoch sollte vor einem Zugriff die ausdrückliche Freigabe der Beschäftigten erforderlich sein (s. Regelungsansatz „Remote Control Software“).

Die Systemadministratoren sind zu verpflichten, über Informationen, die sie im Rahmen ihrer Zugriffe und Auswertungen erlangen, Stillschweigen zu wahren bzw. nur im Rahmen der Zweckbestimmung der Vereinbarung weiterzugeben.

Die wichtigsten Regelungspunkte im Überblick:

Regelungs-aspekte

- Wegen der großen Möglichkeiten zur technischen Überwachung der Beschäftigten durch das System ist eine möglichst eng gefasste Zweckbestimmung besonders wichtig.
- Im Einsatzfeld der Hardware-Inventarisierung genügt unter Umständen die beschreibende Dokumentation des Leistungsumfangs, sofern auf die Aufzeichnung von Benutzer-Aktivitäten verzichtet wird.
- Bei der Software-Inventarisierung und der Lizenzkontrolle ist der Umfang der erzeugten Protokolle und Zugriffsregelungen für Auswertungen zu vereinbaren.
- Unbedingt notwendig ist eine faire Regelung, um die Beschäftigten im Falle des Aufspürens von Fremdsoftware auf ihren Rechnern vor leichtfertigen Missbrauchsvorwürfen zu schützen.
- Die Softwareverteilung sollte im Regelfall automatisch durchgeführt werden. Ausnahmen in Form von manuellen Zugriffen sollten definiert werden.

6. Betriebssysteme Windows, Apple

„Da haben Sie nichts mitzubestimmen. Ist doch nur ein Upgrade vom alten Betriebssystem“, sagte die Geschäftsleitung und hoffte, dass der Betriebsrat weiterschlafen würde ... – Die Geschäftsleitung wurde falsch informiert. Denn die Einführung von Betriebssystemen fällt in den Anwendungsbereich des § 87 Abs. 1 Nr. 6 BetrVG, weil die Systeme sich prinzipiell zur Verhaltensüberwachung der Beschäftigten eignen.

System-protokolle

Betriebssysteme steuern die Rechenleistung und übernehmen die Speicherverwaltung bei der Ausführung von Programmen. Sie werden darüber hinaus mit weiteren betriebssystemnahen Programmteilen ausgeliefert, die eine Vielzahl von Grundfunktionen des Rechnerbetriebs steuern und überwachen. In diesem Zusammenhang werden vom Betriebssystem diverse Systemprotokolle geführt, die technische Informationen über die Benutzung des Computers liefern. Über diese Protokolle haben selbst Experten nur mühsam Überblick, und sie sind noch mühsamer – wenn überhaupt – abschaltbar.[20]

Das Betriebssystem bietet der Systemadministration zudem Zugriffsmöglichkeiten auf die Dateiverzeichnisse der Arbeitsplatzrechner und damit grundsätzlich die Zugriffsmöglichkeit auf die Dokumente der Beschäftigten. Das Recht zur Mitbestimmung der Systeme nach § 87 Abs. 1 Nr. 6 BetrVG steht damit außer Frage.

[20] Für Windows-Systeme vermittelt der Aufruf „Systemsteuerung => Verwaltung => Ereignisanzeige“ einen kleinen Einblick.

Zweck-bestimmung

Der Problematik, dass das Betriebssystem im Verborgenen unüberschaubare Listen aufgerufener Programme, Loginzeiten und weiterer Benutzer-Informationen führt, können die Betriebsparteien nur dadurch begegnen, indem sie die Nutzung dieser Informationen in einer Betriebsvereinbarung ausschließlich zur technischen Fehleranalyse und Fehlerbehebung zulassen. Eine darüber hinausgehende Verwendung ist nicht notwendig und damit insbesondere die Auswertung zur Leistungs- und Verhaltenskontrolle unzulässig.

Schutz persönlicher Speicherbereiche

Sofern noch nicht an anderer Stelle geschehen, kann die Systemeinführung zum Anlass genommen werden, den Schutz von persönlichen Speicherbereichen der Beschäftigten sicherzustellen. In dem Fall erhält jeder Beschäftigte einen persönlichen Speicherbereich auf seinem Arbeitsplatzrechner zur Verfügung gestellt, auf den keine anderen Personen zugreifen können. In diesem geschützten Bereich kann der Beschäftigte dann z. B. halbfertige Dokumente oder Ideensammlungen sichern. Einwänden der Arbeitgeberseite, dass die Verzeichnisse dann unter Umständen für speicherfressende private Fotosammlungen verwendet werden könnten, kann man mit der Vereinbarung einer maximalen Speichergröße der persönlichen Verzeichnisse begegnen.

Es ist durchaus möglich, auch den Zugriff von Systemadministratoren auf die persönlichen Speicherbereiche von Beschäftigten zu unterbinden oder zwangsweise zu protokollieren. In vielen Fällen wird freilich lediglich vereinbart, dass ein Zugriff durch die Systemadministration – ohne ausdrückliche Zustimmung des jeweiligen Beschäftigten – nicht erfolgen darf, aber technisch möglich bleibt.

Mitbestimmungsbedarf löst die Einführung eines neuen Betriebssystems darüber hinaus auch deshalb aus, weil mit der Installation regelmäßig viele Zusatztools zur Verfügung gestellt werden: Neue Windows-Systeme werden beispielsweise standardmäßig mit Programmen zur Fernsteuerung (Remote Control), zum Daten-Backup und zur Datei-Verschlüsselung ausgeliefert, dazu kommen Internetbrowser, Mailprogramm oder ein so genannter Messenger zum Chatten. Möglicherweise sind die Probleme bei der Nutzung dieser Systeme bereits in entsprechenden Vereinbarungen geregelt. Dann ist zu prüfen, ob die vereinbarten Regelungen weiterhin anwendbar sind. Wenn nicht, dann bietet die Systemeinführung einen Anlass, bestehende Betriebsvereinbarungen zu überarbeiten, bzw. sich erstmalig mit der Thematik auseinanderzusetzen.

VI. Telefonanlagen

1. Grundlagen

„Voice-Over-IP“ (VoIP) heißt das Schlagwort, das in vielen Unternehmen zum Austausch der alten Telefonanlagen geführt hat und immer noch führt. Die Nutzung VoIP-fähiger Komponenten zieht dabei für sich genommen kaum neuen Regelungsbedarf nach sich. Allerdings haben sich mit dem Verfall der Kommunikationskosten in den letzten Jahren die Regelungsschwerpunkte der meisten Betriebsvereinbarungen zum Thema Telefonie verschoben. Auseinandersetzungen betreffen mittlerweile nur noch selten die Abrechnung privater Telefongespräche. Stattdessen gerät der Einsatz neuer Leistungsmerkmale in den Fokus betrieblicher Regelungen:

Telefonanlagen mit „ACD“-Funktionalität sollen in den Telefon- oder Service-Centern von Unternehmen für eine ausgewogene Verteilung an die Beschäftigten sorgen. Leider ist ihr Einsatz mit umfangreichen Auswertungsmöglichkeiten verbunden. Und die Beschäftigten geraten nicht nur durch Statistiken unter Druck. Verschnaufpausen werden oft nicht geduldet. Qualifizierungsmaßnahmen sind häufig nur schlecht getarnte Vehikel zur Leistungsüberwachung der Beschäftigten. Für Betriebsräte ergibt sich hier ein weites Feld für notwendige Vereinbarungen.

Ebenfalls regelungswürdig sind Techniken, mit denen Telefondaten mit Anwendungsprogrammen verkoppelt werden können („Computer-Telephony-Integration“, CTI). Häufig sind die eingesetzten Systeme auf Grundfunktionalitäten beschränkt, die etwa das Anwählen von Telefonverbindungen mit Hilfe des Computers ermöglichen. In Einzelfällen können jedoch auch komplexe Anwendungsprogramme verknüpft werden. Dann sind vertiefende, prüfende Blicke auf die zum Einsatz kommenden Systeme notwendig.

Das Gleiche gilt beim geplanten Einsatz von „Dialern“, die anhand von Listen automatisch Telefonnummern anwählen. Oft müssen die Beschäftigten dann im wahrsten Sinne des Wortes „ohne Atempause“ die von der Maschine initiierten Gespräche annehmen und telefonieren.[21]

2. Telekommunikationsanlage

Ausgangspunkt einer jeden Betriebsvereinbarung zur Telefonie ist die in Artikel 10 des Grundgesetzes verankerte Unverletzlichkeit des

[21] Weitere Informationen für Betriebsräte rund um die Telefonie finden Sie unter http://www.tse.de/papiere/call center und telekommunikation/.

Fernmeldegeheimnisses. Das Bundesverfassungsgericht hat dabei in seinen Urteilen bekräftigt, dass das Fernmeldegeheimnis auch bei Telefongesprächen von Beschäftigten im Unternehmen zu beachten ist (BVerfG v. 19.12.1991 – 1 BvR 382/85, vgl. AuR 1992, 158).

Wahrung des Fernmelde-geheimnisses

Als Ziel einer Vereinbarung sollte daher der Schutz des gesprochenen Worts sowie der Schutz der Beschäftigten vor einer unzulässigen Verhaltens- oder Leistungskontrolle definiert werden. In diesem Zusammenhang sollte festgelegt werden,

- dass Lautsprechereinrichtungen nur mit Einverständnis aller Gesprächsteilnehmer genutzt werden dürfen,
- dass auf Anrufbeantwortern gespeicherte Mitteilungen nur von berechtigten Adressaten abgehört und gelöscht werden können und
- Funktionen zum unbemerkten Mithören, Aufzeichnen, Raumüberwachen etc. nicht zur Verfügung gestellt werden.

Auf „Nummer Sicher“ gehen Arbeitnehmervertretungen, wenn die an den Endgeräten (Telefonapparate, Headsets) aktivierten Leistungsmerkmale in abschließender Form aufgezählt und in einer Anlage vereinbart werden.

Private Telefonate

Viele Vereinbarungen aus den 1990er Jahren sehen eine Pflicht zur Kennzeichnung privater Telefongespräche durch die Anwahl einer Kennziffer vor. Diese Handhabung hat sich im Lauf der Jahre überholt: Im Zeitalter der Flatrates sind die Verwaltungskosten für die persönliche Zuordnung der Telefongebühren und den monatlichen Abzug vom Gehalt in der Regel größer als die eigentlichen Telefonkosten. Eine gesonderte Erfassung und Abrechnung von Privatgesprächen ist daher überflüssig.

Stattdessen bietet es sich an, im Vereinbarungstext klarzustellen, dass die Telefone zwar für dienstliche Gespräche zur Verfügung gestellt werden, dass die gelegentliche private Nutzung jedoch geduldet wird.

Fehlt eine entsprechende Passage, so sind private Telefonate nur dann erlaubt, wenn die Gespräche „dienstlich veranlasst“ sind. Mitteilungen, dass man später von der Arbeit nach Hause kommt, wären erlaubt, die Ticketbestellung für das Fußballspiel am Wochenende nicht. Im Einzelfall kann auch eine betriebliche Übung entstanden sein, nach der den Beschäftigten ein „Gewohnheitsrecht“ zu gelegentlichen privaten Telefongesprächen erwachsen sein könnte.

Gesprächs-daten

Zentraler Bestandteil jeder Vereinbarung sind Bestimmungen zur Verbindungsdatenerfassung und -auswertung. Die bei jedem Gespräch anfallenden Daten liefern Informationen darüber, wer wann welche

Rufnummer gewählt hat. Im Unternehmen sind diese Informationen relevant, um die anfallenden Telefonkosten auf die Kostenstellen zu verteilen.

Ein empfehlenswertes Konzept sieht vor, zunächst festzulegen, welche Daten je Gespräch aufgezeichnet werden:

- interne Rufnummer der Nebenstelle, Kostenstelle,
- Datum, Uhrzeit und Dauer des Telefonats,
- Gebühreneinheiten des Telefonats und
- angewählte Rufnummer.

Gespeichert werden in diesem Fall nur die Daten ausgehender Telefonate. Interne sowie eingehende Gespräche verursachen keine Kosten und werden deshalb auch nicht protokolliert. Die Telefonanschlüsse von Betriebsarzt und Betriebsrat sind von der Protokollierung auszunehmen. Viele Regelungen sehen darüber hinaus das Unkenntlichmachen der letzten Ziffern der Rufnummern vor, so dass der Gesprächsempfänger nicht unmittelbar ermittelt werden kann.

Auswertung

Ausgewertet wird lediglich die monatliche Gesamthöhe der Kosten je Kostenstelle. Weitere Auswertungen, insbesondere Auswertungen über Einzelverbindungen können in begründeten Einzelfällen gemeinsam mit dem Betriebsrat nach dessen Zustimmung erfolgen. (Gegebenenfalls kann man sich auch auf die Darstellung der monatlichen Gesamtkosten je Beschäftigten einlassen, aber nie einen pauschalen Freibrief für Einzelverbindungsauswertungen ausstellen.) Falls eine Zuordnung von privaten Telefongesprächen zur Kostenabrechnung vorgesehen ist, müssen die Beschäftigten eine Einzelverbindungsübersicht zur Kontrolle derjenigen Telefonate erhalten, die ihnen zugeordnet worden sind.

Für die protokollierten Daten ist eine Speicherfrist, z. B. drei Monate, festzulegen. Nur summierte Daten dürfen darüber hinaus ausgewertet werden. Der administrative Zugang zum System und zu den Auswertungen ist restriktiv zu vereinbaren, die Zugriffsberechtigten sind auf die Einhaltung des Fernmeldegeheimnisses und dieser Vereinbarung zu verpflichten.

Regelungsaspekte

Wie gesehen, sollte eine Vereinbarung zum Einsatz von Telefonanlagen mindestens die folgende Punkte regeln:

- Einhaltung des Fernmeldegeheimnisses
- Regelung für private Telefonate

- zulässiger Umfang des Aufzeichnens von Protokolldaten
- zulässige Auswertungen mit eng gefasster Zweckbestimmung

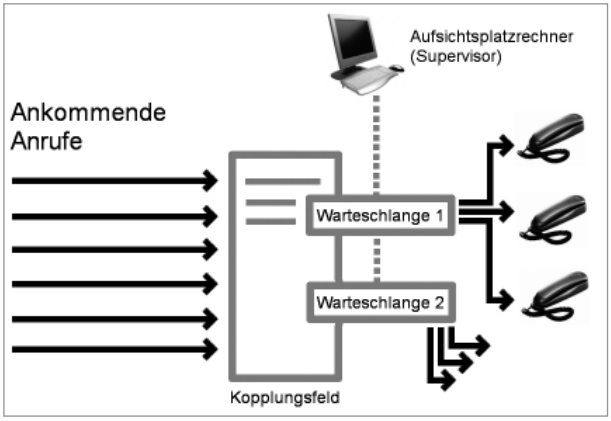
In jedem Fall sollten sich Betriebs- und Personalräte informieren, ob mit dem Einsatz einer Telefonanlage auch der Einsatz neuerer Telekommunikations-Technologien, wie im weiteren Verlauf dieses Kapitels beschrieben, verbunden ist. In diesem Fall entsteht weiterer Regelungsbedarf.

3. Automatische Anrufverteilung (ACD)

Systeme zur automatischen Anrufverteilung („Automatic Call Distribution“, ACD) ergänzen bestehende Telefonanlagen oder sind in neueren Anlagen bereits integriert. Mit ihrer Hilfe können eingehende Anrufe nach definierten Regeln auf eine Gruppe von telefonierenden Beschäftigten, neudeutsch „Agenten“ genannt, verteilt werden („Routing“).

Routingregeln

Diese Zuteilungsregeln können zum Beispiel vorsehen, dass immer der Agent mit der längsten Wartezeit ein neues Gespräch zugestellt bekommt. Falls alle Agenten im Gespräch sind, landet der Anrufer zunächst in einem Wartefeld. Die Anlage könnte aber auch versuchen, ein eingehendes Gespräch in erster Priorität an den Agenten zu vermitteln, der zuletzt mit dem Anrufer gesprochen hat. Nur wenn der Agent nicht anwesend ist oder gerade telefoniert, wird das Gespräch dann an einen Kollegen weitergeleitet. Die ACD-Anlage kann weiterhin Sprachwahldienste beinhalten oder den Kunden je nach Servicewunsch zur Eingabe von Ziffern in dessen Telefonapparat auffordern. Es ist sogar möglich, Anrufe mit Hilfe der ACD-Anlage an dezentrale Telearbeitsplätze zu verteilen, ganze Anrufströme von einem Standort an einen anderen Standort umzuleiten oder sie gemeinsam bearbeiten zu lassen. Unter Umständen kann daher auch die Verlagerung von Arbeitsplätzen zum Thema der Mitbestimmung werden.



Echtzeit-Anzeigen

Die aktuelle Steuerung der Anrufe erfolgt an speziellen Supervisor-Arbeitsplätzen. Hier wird angezeigt, welche Agenten zurzeit am System angemeldet sind, ob sie telefonieren oder sich in Nachbearbeitung befinden. Viele Systeme bieten darüber hinaus weitere Leistungsdaten über die Agenten an, etwa Berichte über die Anzahl ihrer seit Anmeldung getätigten Gespräche, deren Durchschnittsdauer oder die Zahl der vom Agenten initiierten Gesprächsweiterleitungen. Jede Regelung muss daher eine Passage enthalten, die alle kritischen Anzeigen und Auswertungen ausschließt.

Zweifelhafter Nutzen

Der Einsatz von ACD-Anlagen ist gerade für kleinere Organisationseinheiten nicht unbedingt sinnvoll. Abgesehen vom zeitlichen Aufwand für Installation und Betrieb der Anlage und den aus Mitbestimmungssicht problematischen Überwachungsmöglichkeiten, kann eine ACD-Anlage die hohen Erwartungen der Verantwortlichen häufig nicht erfüllen: Wenn im telefonischen Kundenservice zu wenige Mitarbeiter eingesetzt werden, kann auch die beste Anrufverteilung die Engpässe nicht abschaffen. Und mit einem Blick auf die Arbeitsplätze der Kollegen verschafft sich ein Teamleiter sicherlich einen besseren Überblick über die aktuellen Verfügbarkeiten der Kollegen, als mit Hilfe von Statusanzeigen auf dem Rechnermonitor.

Regelungsaspekte

Ist aber die Entscheidung im Unternehmen für die Einführung einer ACD-Anlage gefallen, so lauten die wichtigsten Punkte für eine Betriebsvereinbarung:

- Ausgewogene Anrufverteilung: Das eingesetzte Routingverfahren sollte erläutert und ggf. vereinbart werden. Dabei sollte die Direktdurchwahl der Kunden zu den Agenten möglich bleiben, damit eine persönliche Kundenbeziehung aufrechterhalten werden kann.

- Nahezu alle Systeme bieten die Möglichkeit an, ein Routing nach Skills (Qualifikationsmerkmalen) vorzunehmen, die für die Agenten im System hinterlegt werden. Gespräche, die über eine bestimmte Service-Rufnummer reingekommen sind, werden dann nur an die Agenten weitergeleitet, die den entsprechenden Skill besitzen. Dies ist nur dann unproblematisch, wenn es sich bei den Skills lediglich um wenige fachliche Qualifikationen, z. B. um Produktkenntnisse handelt und die Beschäftigten ein Beschwerderecht über ihre Zuordnung haben. Soziale Skills („Kundenfreundlichkeit“, „Stressresistenz“) haben hier allerdings nichts zu suchen.

- Die Anmeldung an und die Abmeldung von der ACD-Anlage sollte durch die Agenten selbst gesteuert werden.

- Die von der Anlage differenzierten Zustandsanzeigen sollten auf das notwendige Maß begrenzt werden. Bewährt hat sich: Bereit, Gespräch, Nachbearbeitung, Pause (ohne Angabe von Pausengründen), Abgemeldet.

- Höchst kritisch sind, wie oben beschrieben, die Echtzeit-Anzeigen („Monitoring“) am Arbeitsplatz des Supervisors. Damit es zu keinen Missverständnissen kommt, ist es anzuraten, alle zulässigen Anzeigen (z. B. über den Servicelevel der letzten 30 Minuten, aktueller Zustand der Bedienplätze ohne Historie) mit je einem Bildschirmausdruck zu dokumentieren und in einer Anlage zu vereinbaren.

- Besondere Aufmerksamkeit erfordern auch Auswertungen über längere Zeitabschnitte („Reporting“). Bei der Bildung von relevanten Kennzahlen besteht die Gefahr, dass man die eigentlichen Ziele, die man bewerten möchte, angesichts der Vielzahl möglicher Auswertungen aus dem Auge verliert. Das Reporting darf jedoch nicht zur Arbeitsbeschaffungsmaßnahme für Controller-Heerscharen verkommen. Jede Kennzahl, für die Daten im Call-Center Reporting erhoben oder ausgewertet werden, sollte daher einem definierten Ziel entsprechen. Dabei sollten die Kundenzufriedenheit und Aspekte der Kundenbindung eine wichtige Rolle spielen.

- Die unter diesen Vorgaben vereinbarten Reports sollten in einer Anlage dokumentiert werden. Auswertungen, die sich auf einzelne Mitarbeiter beziehen, werden nicht durchgeführt. Auswertungen von Kleingruppen mit weniger als sechs Mitarbeitern sollten wegen des hohen Überwachungsdrucks auf die einzelnen Gruppenmitglieder ebenfalls ausgeschlossen werden (wobei die Zahl Sechs natürlich Verhandlungssache ist).

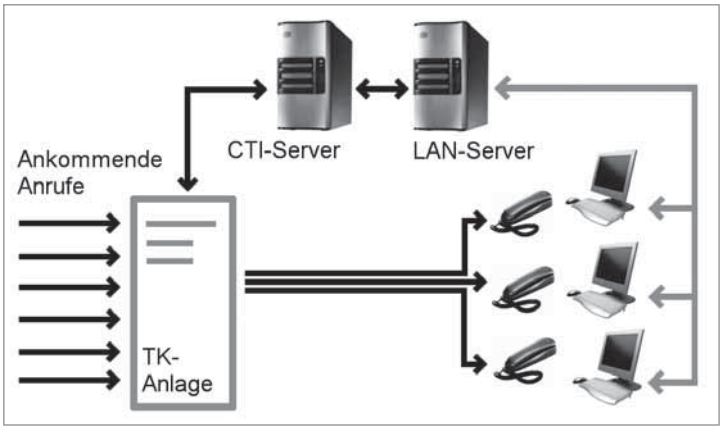
- Kennzahlen über die aktuelle Anrufsituation, die den Mitarbeitern zur Selbststeuerung ihres Telefonierverhaltens angezeigt werden sollen, sind ebenfalls zu vereinbaren.

Coaching

Ein besonderes mitbestimmungsrelevantes Problem stellt die Qualifizierung („Coaching“) von Beschäftigten an Telefonarbeitsplätzen dar. Natürlich sollen die Agenten lernen, wie sie sich in bestimmten Gesprächssituationen optimal verhalten und sich in ihrer Arbeit weiterentwickeln. Leider reduzieren sich die unter der Überschrift „Qualifizierung“ geplanten Maßnahmen der Arbeitgeber in der Realität allzu häufig auf Werkzeuge zur Beurteilung der Arbeitsleistung der Agenten. Vereinbarungen sollten daher auch Aussagen zum Coaching enthalten, dabei Testanrufe („mystery calls“) oder das heimliche Mithören oder gar Mitschneiden von Telefongesprächen durch Teamleiter verbieten. Sinnvolle Qualifizierungsansätze haben keinen bewertenden Charakter, sondern haben das Ziel, den individuellen Schulungsbedarf der Agenten festzustellen. Unter dieser Voraussetzung sind Gesprächsanalysen mit Experten, möglichst nicht mit dem direkten Vorgesetzten, auf freiwilliger Grundlage denkbar. Individuelle Coaching-Ergebnisse sollten dann bei der gecoachten Person verbleiben, lediglich die Teilnahme an vereinbarten Schulungen kann dokumentiert werden.

4. Computer-Telephony-Integration (CTI)

Computer-Telephony-Integration ist die Verbindung von Telefonnetz und Computernetz: Sprachkommunikation und Datenverarbeitung werden synchronisiert. Während des Telefonierens besteht somit zeitgleich Zugriff auf Kunden- und Produktdaten sowie auf weitere Services, die den Agenten über ihre Computer zur Verfügung gestellt werden können.



Grundfunktionen

In seiner einfachsten Form wird über CTI eine Anruferidentifizierung vorgenommen: Die von der Telekommunikationsanlage erkannte Telefonnummer wird an ein Serversystem weitergeleitet, dieses ermittelt den mit der Rufnummer korrespondierenden Namen des Anrufers. Nach der Identifizierung des Anrufers können bestimmte Informationen aus Datenbanken auf dem Bildschirm dargestellt werden (z. B.: Name und Kontakthistorie des Anrufers). CTI kann bereits die Verbindungsdaten eingehender Telefone auswerten und durch Zugriff auf eine Kundendatenbank ausgewählte Kundeninformationen anzeigen oder bei noch unbekanntem Kunden die Eingabe der Daten veranlassen. Komplexere CTI-Anwendungen verknüpfen die Kundendaten direkt mit einem Sachbearbeitungsprogramm, so dass die explizite Eingabe der Kundennummer o. Ä. nicht mehr erforderlich ist. Die Königsdisziplin der CTI-Technik ist dabei das Synchronisieren von Gesprächsübergabe und Bildschirmübergabe im Fall einer Weitervermittlung von Telefongesprächen an Kollegen, die nur selten so reibungslos funktioniert wie von den Verantwortlichen gewünscht und von den Herstellern propagiert wird.

Eine weitere, häufig eingesetzte Grundfunktion ist die Wählhilfe für die Agenten. Statt die Rufnummern mit Hilfe des Ziffernblocks des Telefonapparats einzugeben, initiieren die Agenten Gespräche durch Anklicken des Gesprächspartners im Adressbuch ihres Computers oder durch Anwahl einer Person aus einer angezeigten Liste. Der Ver-

bindungsaufbau erfolgt dann automatisch. Diese Funktionalität kann auch aus anderen Anwendungen heraus bereitgestellt werden.

Regelungsaspekte

CTI-Funktionen, die im oben beschriebenen Sinne lediglich

- die Anzeige von Informationen über den aktuell einkommenden Anruf (Rufnummer, hinterlegter Kundenname, etc.) auf den Bildschirmen der Agenten oder
- die Steuerung von Telefonfunktionen (Ruf annehmen, Ruf weiterleiten, Rückruf initiieren etc.) durch eine EDV-Anwendung

umfassen, lösen in der Regel keinen besonderen Regelungsbedarf aus, sofern über ihren Einsatz zwischen den Betriebsparteien grundsätzlich Einvernehmen herrscht.

Komplexe CTI-Anwendungen erfordern allerdings einen differenzierten Blick auf das jeweils eingesetzte Einzelsystem. Durch die Kopplung von Telefonsystem und Computernetz besteht prinzipiell die Möglichkeit, dass alle Daten, die beim Telefonieren anfallen, an die CTI-Anwendung übermittelt werden können.

Wenn man als Betriebsrat nicht aufpasst, werden auch schon mal elektronische Stoppuhren in die Programme eingebaut, die die Dauer eines Telefongesprächs und eine eventuelle Nachbearbeitung unter dem unverfänglich erscheinenden Verwendungszweck „Ermittlung von Prozesszeiten“ automatisch erfassen und in einem umfänglichen Reporting zugänglich machen. Sogar die Bewegungen der Maus beim Bedienen der Anwendungsprogramme lassen sich messen und auswerten.

CTI-Systeme sollten also mindestens im Hinblick auf die verwendeten mitarbeiterbezogenen Daten aus der Telefonanlage überprüft werden, darüber hinaus dürften weitere Bestimmungen erforderlich sein, die den speziellen mitbestimmungsrechtlichen Problemen der jeweils eingesetzten Anwendung gerecht werden.

5. Dialer

Dialer unterstützen das aktive Telefonieren für ausgehende Gespräche („Outbound“). Sie können interaktiv oder vollautomatisch Verbindungen herstellen und erkennen, ob der Gesprächspartner erreichbar ist und diesen Anruf entgegen nimmt, ob der Anschluss besetzt ist oder z. B. ein Anrufbeantworter antwortet.

So genannte Power-Dialer arbeiten ganze Listen von anzuwählenden Telefonaten ab. Noch während des laufenden Gesprächs eines Agenten wird vom System die nächste Gesprächsverbindung zu einem Kunden aufgebaut. Kommt die Verbindung zustande, stellt das Dialer

System dem Agenten das Gespräch automatisch zu. Telefoniert der Agent länger als von der Dialer-Software vorgesehen und kann er deshalb das ihm zugedachte Gespräch nicht annehmen, versucht das Dialer-System, einem anderen Agenten das Gespräch zuzuteilen. Der unglückliche Kunde wird in dieser Zeit mit Pausenmusik berieselt oder zu einem späteren Zeitpunkt noch einmal angewählt.

Für Beschäftigte ist die Telefonie bei Einsatz von automatischen Power-Dialern mit einer besonders hohen Stressbelastung verbunden. Die extrem auf hohe Gesprächskontaktzahlen ausgerichtete Technik macht die betreffenden Beschäftigten in vielen Fällen zu kleinen Rädern im Mahlwerk der Technik.

Regelungsaspekte

Wo Betriebsräte den Dialereinsatz nicht verhindern können oder wollen, sollte das System so eingerichtet werden, dass keine systeminitiierten Gespräche stattfinden (also alle Gespräche von den Agenten selbst veranlasst werden) oder zumindest eine rechtzeitige akustische Signalisierung eines bevorstehenden Gesprächs erfolgt

Im letzteren Fall sollte vereinbart werden, dass zwischen zwei Gesprächen eine Mindestzeit festgelegt wird, in der den Agenten kein neues Gespräch zugeteilt wird. In diesem Zusammenhang ist auch zu überprüfen, ob die im System eingestellten Nachbearbeitungszeiten ausreichend sind.

Die Zeiten, in denen per Dialer telefoniert wird, sind einzuschränken, z. B. auf vier Stunden wöchentlich je Mitarbeiter. Für im Dialerbetrieb arbeitende Agenten sind besondere Arbeitspausen, z. B. zehn Minuten nach jeweils 50 Minuten, zu vereinbaren.

Personenbezogene und kleingruppenbezogene Auswertungen sollten nicht zur Verfügung gestellt werden.

6. Voice over IP („VoIP“)

Bisher existierten in den Unternehmen zwei Kommunikationsinfrastrukturen isoliert nebeneinander: Das Netzwerk für die Datenkommunikation und das herkömmliche Telefonnetz für die Sprachkommunikation. Diese Trennung wird durch die Einführung neuer Technologien auf der Basis des Internetprotokolls IP aufgehoben.

Vor- und Nachteile

Der Einsatz neuer Telefonanlagen auf Basis der VoIP-Technik kann daher im Idealfall zu Kosteneinsparungen im laufenden Betrieb führen, da nur noch ein Netzwerk administriert werden muss. Zuvor muss allerdings in vielen Unternehmen massiv in die bestehende Netzwerk-Infrastruktur investiert werden, denn diese ist zumeist nicht für den erforderlichen Datendurchsatz beim Telefonieeinsatz ausgelegt.

Der Einsatz von Voice-Over-IP-Anlagen ist mit weiteren Vorteilen verbunden: Endgeräte sind leichter administrierbar. Neue Anwendungsmöglichkeiten sind in der Regel einfacher umzusetzen, zum Beispiel die Einbindung von E-Mail, Fax etc. in das hinterlegte Routing der Anlage.

Dem stehen die Nachteile einer immer noch nicht völlig ausgereiften Technologie gegenüber und Sicherheitsrisiken, die jedoch prinzipiell auch herkömmliche Telekommunikations-Architekturen betreffen.

Betriebs- und Personalräte werden sich mit den Sicherheitsaspekten nur am Rande herumschlagen müssen. Sie sollten sich das vom Unternehmen vorgenommene Sicherheitskonzept aber erläutern lassen.

Regelungsaspekte

Im Weiteren gilt es, bei der Konfiguration der Anlage darauf zu achten, dass die Persönlichkeitsrechte der Mitarbeiter gewahrt werden. Dabei unterscheiden sich die Anforderungen beim Einsatz einer VoIP-Anlage nicht von herkömmlichen Telefonanlagen.

7. Mobiltelefone

Gleichbehandlung

Für Beschäftigte, die häufig außerhalb ihrer eigentlichen Arbeitsstätte eingesetzt werden, sind Mobiltelefone ein unverzichtbares Arbeitsmittel geworden. Nur noch selten gilt die Benutzung eines „Diensthandys“ als Privileg von besonders ausersehenen Beschäftigten. Dennoch sollten Betriebsräte darauf achten, dass der Anspruch auf das Zurverfügungstellen eines Mobiltelefons nach sachlichen Kriterien erfolgt und die Beschäftigten dabei nicht ungleich behandelt werden.

Grundsätzlich ähneln die Einsatzbedingungen und damit die mitbestimmungsrechtlichen Probleme denen der Festnetztelefonie, die zu Beginn dieses Kapitels erläutert worden sind.

Fernmeldegeheimnis

An herausgehobener Stelle steht auch bei der Mobiltelefonie der Schutz des gesprochenen Worts. Da die Mobiltelefonie jedoch fast immer direkt über einen externen Mobilfunk-Provider abgewickelt wird, sind die technischen Möglichkeiten der Systemadministration zum missbräuchlichen Abhören von Gesprächen allerdings begrenzt. Dennoch bleibt es eine gute Idee, die Prinzipien des Fernmeldegeheimnisses einer Vereinbarung voranzustellen.

Abhören von Handy-Telefonaten

Mit großem technischen Aufwand können Geräte eingesetzt werden, die Handys Mobilfunkzellen vorgaukeln (IMSI-Catcher), so dass die Gespräche über diesen Umweg geführt werden und abgehört werden können. Neuer ist der Ansatz, Gespräche mit einem Frequenzscanner zu erfassen. Die Verschlüsselung der

Gespräche soll Berichten zufolge mittlerweile innerhalb von Minuten geknackt werden können. Das funktioniert zurzeit nur beim älteren Handy-Standard GSM. (http://www.computerwoche.de/cwriskboard/1856494/)

Wahrscheinlicher sind allerdings Gefahren, die darauf beruhen, dass auch Handys – ebenso wie große PCs – mit einem Betriebssystem ausgestattet sind. Damit sind sie prinzipiell für Computerviren und Trojaner angreifbar, etwa durch fingierte Kurznachrichten (SMS oder MMS), die Sicherheitslücken des Betriebssystems oder die Unwissenheit des Benutzers ausnutzen. Die so manipulierten Mobiltelefone ermöglichen dann das unbemerkte Mithören von Gesprächen, indem sie z. B. bei Verbindungsbeginn automatisch und unbemerkt eine Konferenzschaltung zu einem dritten Anschluss herstellen. (http://www.morgenpost.de/printarchiv/magazin/article706183/Lauschangriff_aufs_Handy.html)

Keine Ortungsdienste

Bei vielen Mobilfunk-Providern kann ein Servicemerkmal aktiviert werden, das eine Ortung des Mobiltelefons ermöglicht und beispielsweise auf einer Internetseite den aktuellen Aufenthaltsort des Handys (und damit seines Besitzers) auf einer Karte darstellt (siehe auch Kapitel VII 8). Wegen der hohen Überwachungseignung und dem darüber hinaus zweifelhaften Nutzen dieser Funktion im betrieblichen Umfeld, ist in einer Vereinbarung darauf zu bestehen, dass entsprechende Leistungsmerkmale nicht aktiviert werden.

Auswertungen

Während die Kosten einzelner Telefonate bei der Festnetztelefonie oft kaum noch ins Gewicht fallen, sind die Kosten für Telefonate mit dem Handy immer noch fühlbar, man denke nur an die überteuerten Roaming-Kosten für Handy-Telefonate im Ausland. In vielen Unternehmen wird aus diesem Grunde genauer auf die Mobilfunkabrechnung geschaut. Betriebsräte sollten den Umfang der zulässigen Auswertungen, die von den Mobilfunkprovidern angefordert werden dürfen, abschließend regeln. Als Orientierung können dabei die für die Festnetztelefonie aufgestellten Regelungsvorschläge dienen. Insbesondere sollte auch bei der Mobiltelefonie kein Freibrief zur Einsichtnahme in die Einzelverbindungen der Beschäftigten ausgestellt werden.

Zusätzliche Online-Dienste

Gegebenenfalls entsteht mit der Nutzung weiterer Funktionen der Handys auch ein weiterer Regelungsbedarf. Außer zu Telefongesprächen können Mobiltelefone mittlerweile ebenfalls für den ortsunabhängigen Abruf von E-Mails, zur Terminverwaltung oder zur Verbindung mit dem Internet genutzt werden. Betriebsräte sollten daher den Umfang der zur Verfügung gestellten Online-Dienste in Erfahrung bringen, um ggf. ergänzende Bestimmungen zu vereinbaren.

Da viele dieser Dienste mit zusätzlichen Kosten verbunden sind und teilweise auch versehentlich ausgelöst werden können, empfiehlt es sich, hierzu eine Passage in dem Vereinbarungstext unterzubringen, die klar stellt, dass

- das Mobiltelefon so konfiguriert und dem Beschäftigten zur Nutzung übergeben wird, dass eine versehentliche Nutzung von Diensten (z. B. Internet) ausgeschlossen ist.

- Andernfalls haftet das Unternehmen für entstandene Kosten.

Beschränkte Haftung

Die Frage der Haftung sollte auch für den Fall des Verlusts oder der Beschädigung des Handys geregelt werden. Da Handys als häufig verwendete Alltagsgegenstände besonders anfällig für Beschädigungen und Missgeschicke sind und sie zudem bei Langfingern äußerst beliebt sind, sollte klargestellt werden, dass die Beschäftigten nur im Fall von Vorsatz oder grober Fahrlässigkeit haften.

Bereitschaftsdienste

Je nach „Betriebskultur" kann die Nutzung von Diensthandys mit zusätzlichem Arbeitsdruck auf die Beschäftigten verbunden sein. Dann nämlich, wenn – meist nur inoffiziell – erwartet wird, dass der Beschäftigte das Mobiltelefon ständig eingeschaltet hält und für den Arbeitgeber somit rund um die Uhr verfügbar und ansprechbar bleibt, auch am Abend und vielleicht sogar am Wochenende oder im Urlaub. Andererseits ist der Handy-Einsatz für „offizielle" Bereitschaftsdienste der Beschäftigten unbestritten hilfreich.

Vereinbarungen können mit entsprechenden Formulierungen die notwendigen Differenzierungen vornehmen. Für Bereitschaftsdienste könnte eine Pflicht zur Nutzung der Geräte vereinbart werden. Darüber hinaus könnte klargestellt werden, dass das Diensthandy nur zur Kommunikation während der Arbeitszeit verwendet werden soll und dass die Beschäftigten nicht verpflichtet sind, Gespräche außerhalb der Arbeitszeit anzunehmen. Freilich greifen solche Regelungen nur, wenn sie von der Belegschaft mitgetragen werden.

Regelungsaspekte

Zusammengefasst sollte sich eine Vereinbarung zur Mobiltelefonie mit mindestens den folgenden Regelungsaspekten befassen:

- Einhaltung des Fernmeldegeheimnisses

- Genaue Regeln für die vom Mobilfunk-Provider angeforderten Auswertungen und Listen und deren Nutzerkreis

- Ausschluss von Ortungsdiensten oder ähnlichen Services. Ausnahmen sind genau zu definieren.

- Klärung der privaten Nutzung

- Recht zum Ausschalten von Diensthandys außerhalb der Arbeitszeit

8. Local Based Services / GPS

Die Mobiltelefonie oder – für gehobenere Ansprüche – die GPS-Technik via Satellitenortung öffnen weit über das Telefonieren hinaus durch die Verbindung mit den Softwaresystemen der Computertechnik neue Anwendungsmöglichkeiten. Die bei jedem Telefonat erzeugten Verbindungsdaten der digitalen Telefonie enthalten die Information über die Funkzelle und damit den Ort des Geschehens. In Großstädten liegt die Dichte der Zellen oft schon unter 100 Metern. Durch Auswertung der Abstrahlwinkel benachbarter Zellen kann die Ortsbestimmung sogar bis auf den Meterbereich heruntergerechnet werden. Noch genauere Informationen liefert die Satellitenortung.

Local Based Services nennt sich das flugs aufgemachte neue Geschäftsfeld um die elektronische Ortung. Vorzugsweise wird es Fuhrparkunternehmen zur Steuerung ihrer Kfz-Flotten angedient. Auch jedes Unternehmen, das einen Außendienst betreibt, kann die Services in Anspruch nehmen, z. B. um den Standort des letzten Einsatzes abzufragen und dem betroffenen Mitarbeiter dann einen neuen Auftrag möglichst in der Nähe des letzten Standortes zuzuteilen. Beim sog. Incident Management, zu deutsch der Organisation von Notdiensten bei unvorhergesehenen Störfällen gleich welcher Art, sind die Services fast schon ein Muss. Die „coolsten“ Anwendungen erlauben es, die aktuellen Standorte der Außendienstmitarbeiter auf einer Art Radarschirm vor dem Hintergrund einer geografischen Karte sichtbar zu machen. Man braucht sie bloß noch anzuklicken, und man kann den Mitarbeitern neue Aufträge zuweisen oder detailliertere Infos über ihren aktuellen Einsatz oder sogar ihr ganzes bisheriges Tagesgeschäft abfragen.

Regelungsaspekte

Betriebsräte, die den Einsatz solcher Systeme per Vereinbarung regeln wollen, haben sich mit einer Vielzahl sehr konkreter und sehr situationsspezifischer Details auseinanderzusetzen. Dennoch lassen sich einige Eckpunkte für den Abschluss einer betrieblichen Regelung formulieren:

- Zunächst sollte man den Verwendungszweck der Anwendung so präzise wie möglich festlegen und – wenn irgend möglich – auf die Funktion der bloßen Einsatzsteuerung begrenzen.

- Das Abfragen der Positionsdaten kann man auf eine Überwachung des Augenblicks begrenzen, im Klartext: nur die Positionsdaten des aktuellen Einsatzes werden verwendet, Daten zeitlich zurückliegender Einsätze werden nicht gespeichert bzw. überschrieben oder gelöscht. Speichert man die komplette Historie, so entstehen Bewegungsprofile, wodurch die Überwachungsmöglichkeiten durch das System auf eine neue Ebene gehoben würden.

- Die Mitarbeiterinnen und Mitarbeiter sollten die Möglichkeit haben, die ortungsgeeigneten Geräte abschalten zu dürfen, zumindest während Pausen oder außerhalb der Regelarbeitszeit. Das Konzept der Arbeitgeber zielt bekanntlich auf das „ubiquitous computing“, zu deutsch: jederzeit und überall erreichbar zu sein. Das muss man nicht mitmachen.

- Besondere Aufmerksamkeit verdient das Reporting solcher Systeme, das oft mit Hilfe nachgelagerter Datenbanksysteme erfolgt (sog. Data Warehouses). Werden die Standorte in die Auswertungssysteme übernommen, so kann man durch Kombination mit den Zeit-Informationen die Bewegungsabläufe detailliert rückverfolgen, so lange das die Datenspeicherung hergibt. Auf jeden Fall sollte man dafür sorgen, dass in den Auswertungen keinerlei direkter Personenbezug mehr erfolgt. Auf die genauen Ortungsinformationen kann man getrost verzichten. Die Genauigkeit der Zeitinformationen kann man ebenfalls herunterschrauben, denn meist genügt das Tagesdatum vollauf und die Uhrzeiten kann man weglassen. Für Ausnahmen von diesen Grundsätzen müsste der Arbeitgeber schon nachvollziehbare Gründe liefern, die in der entsprechenden Regelung als Zweckbindungen festgehalten werden sollten.

Ähnliche Probleme kommen auf die Betriebsräte zu, wenn die zurzeit noch nur sporadisch eingesetzte RFID-Technik (Radio Frequency Identification) weitere Verbreitung findet. Dabei handelt es sich um Chips, die sich bei einer Aktivierung durch elektromagnetische Strahlung einer bestimmten Wellenlänge aktivieren lassen und dann per Funk mitteilen, wer oder was sie sind, denn sie haben eine weltweit eindeutige Identifizierungsnummer, egal ob es sich um einen Ausweis, ein Preisschild oder eine ganze Palette mit Waren handelt (siehe Kapitel VIII 2).

VII. Videoüberwachung

1. Grundlagen

Das Bundesdatenschutzgesetz regelt in § 6b die Videoüberwachung von „öffentlich zugänglichen Räumen“; nicht öffentlich zugängliche Räume sind davon nicht erfasst. Für den Einsatz von Kameras in „normalen“ Bürogebäuden und Produktionshallen gibt es daher keine Regelung im BDSG. Die Überwachung ist nach den allgemeinen Rechtsgrundsätzen nur im Rahmen der Durchsetzung des Hausrechts bei begründetem Interesse des Arbeitgebers zulässig, sofern keine schutzwürdigen Interessen von Betroffenen überwiegen. Eine anderweitige Aufzeichnung/Verarbeitung/Auswertung kann strafbar sein.

Der enge Rahmen für die Nutzung von Videokameras in Unternehmen wird von der Rechtsprechung des Bundesarbeitsgerichts unterstrichen.[22] Zwar darf der Arbeitgeber im begründeten Einzelfall Videokameras zur Kontrolle der Mitarbeiter nutzen, z. B. um Diebstahl aufzuklären. Grundsätzlich kann man jedoch davon ausgehen, dass die dauerhafte und verdachtsunabhängige, erst recht die heimliche Überwachung von Mitarbeitern mit Videokameras einen unverhältnismäßigen Eingriff in die Persönlichkeitsrechte der Beschäftigten darstellt.

Der rechtliche Rahmen für eine Vereinbarung ist damit abgesteckt. Tatsächlich werden jedoch in den meisten Unternehmen die Betriebs- und Personalräte nicht mit dem Ansinnen der Geschäftsleitung konfrontiert, Kameras zur Mitarbeiterüberwachung einzusetzen. Stattdessen werden in der Regel Sicherheitserwägungen des Unternehmens zur Begründung angeführt. Ob diese nachvollziehbar oder vorgeschoben sind – in jedem Fall obliegt die Einführung und der Betrieb von Videokameras der Mitbestimmung. Denn natürlich kann eine Überwachung der Beschäftigten auch unbeabsichtigt oder stillschweigend in Kauf genommen werden, und davor sollte eine gute Vereinbarung die Beschäftigten schützen.

2. Leistungsmerkmale der Videosysteme

Fast alles ist machbar. Die Jubelprospekte der Hersteller umfassen beispielsweise folgende Features:

- Live-Ansichten von mehreren Dutzend Kameras im Kontroll-Center,
- Speicherung der Videoaufnahmen, manuell oder automatisch ausgelöst, und natürlich dauerhaft und ohne Speicherlimit (digital auf Festplatte und damit besonders schnell kopierbar),

[22] Vgl. BAG-Beschluss v. 29.6.2004 – 1 ABR 21/03 (AuR 2005, 454, DB 2004, 2377).

- 360° schwenkbare, ferngesteuerte Kameras, Heranzoomen,
- Bewegungserkennung, Gesichtserkennung, Alarmierung per SMS, E-Mail, Mobiltelefon,
- Fernzugriff über das Internet und
- Kopplung an Schließanlagen.

Bei betrieblichen Regelungen kommt es für Betriebs- und Personalräte also einmal mehr darauf an, nach dem Gebot der Zweckbindung unter Beachtung des Verhältnismäßigkeitsprinzips die technisch *möglichen* auf die tatsächlich *benötigten* Funktionen einzuschränken. Es sei denn, es gelingt, die Installation einer Videoüberwachungsanlage grundsätzlich zu verhindern.

3. Einwände

Bei kaum einem anderen System sind die Beeinträchtigungen der Persönlichkeitsrechte der Beschäftigten so unmittelbar spürbar wie bei Videoüberwachungsanlagen. Menschen, die beobachtet werden, sind befangen und verhalten sich nicht mehr ihrer Natur entsprechend – eine Erfahrung, die jeder schon mal selbst gemacht hat.

Andererseits sind die Erwartungen der Unternehmen häufig vollkommen überzogen und unrealistisch. Risiken werden hingegen gerne übersehen:

- Die technische Kontrolle gewährleistet zum Beispiel nicht, dass in Gefahrensituationen kurzfristig Hilfe kommt. Voraussetzung hierfür ist ein jederzeit verfügbares, personell aufwändiges Alarmsystem. Existiert dieses nicht, so erweist sich ein eventuell bestehendes subjektives Sicherheitsgefühl als trügerisch. Technische Fehlalarme können darüber hinaus zum „Abstumpfen“ des Wachpersonals führen.
- Aus Angst vor der Dokumentation unsachgemäßer Hilfeleistung kann eine dringend gebotene Hilfeleistung unterbleiben.
- Es gibt keine seriösen Untersuchungen, dass die erhoffte Präventionswirkung tatsächlich eintritt.
- Der Beweiswert von Bildaufnahmen ist wegen der äußerst einfachen Manipulationsmöglichkeiten fragwürdig.
- Untersuchungen für Großbritannien zeigen erheblichen Missbrauch beim Einsatz der Technik auf, z. B. durch Heranzoomen auf weibliche Brüste etc.

- Einhergehende Einsparungen im Personalbudget und Outsourcing an externe Wachdienste führen zu einem Verlust der Einflussnahme auf Wachpersonal und deren Ausbildungsniveau.

4. Regelungsaspekte

Notwendigkeit der Kameraanlage?

Betriebs- und Personalräte sollten sich beim Abschluss einer Vereinbarung überzeugen lassen, dass der Einsatz einer Kameraanlage tatsächlich nachvollziehbar ist und das damit verbundene Anliegen des Arbeitgebers die erheblichen Eingriffe in die Persönlichkeitsrechte der Beschäftigten rechtfertigt. Sie sollten insbesondere die Einbindung in ein umfassendes Sicherheitskonzept fordern. Die technische Überwachung darf nicht alleinige Maßnahme sein, nur zu gerne wird die Qualifizierung der Beschäftigten vernachlässigt.

Zweck

Ein Einsatz sollte nur im Rahmen einer hinreichend konkreten Zweckbestimmung erfolgen: Ein verändertes allgemeines Sicherheitsinteresse ist eine nur schwache Begründung. Stattdessen ist die Gefährdungslage konkret zu benennen und zu begründen.

Standorte

Kameras müssen für die Beschäftigten sichtbar angebracht werden. Die Standorte der Kameras und insbesondere ihr maximaler Schwenkbereich sind genau zu dokumentieren. Im Schwenkbereich der Kameras dürfen sich keine Arbeitsplätze der Mitarbeiter befinden. Es sollten nur die Bereiche überwacht werden, für die eine Gefahrenanalyse ein besonderes Gefährdungspotenzial ergeben hat. Für Bereiche, in denen Beschäftigte überwiegend „privat“ agieren (Betriebskantinen etc.), sind Kameras abzulehnen.

Datenspeicherung

Ist die Datenspeicherung tatsächlich notwendig oder reicht das aktuelle Kamerabild aus (z. B. um ein entferntes Einlasstor zum Werksgelände per Summer durch den Wachdienst freizugeben)? Falls Daten gespeichert werden sollen, muss dies nicht permanent geschehen. Die Speicherfunktion kann zeitlich und ggf. auf das Auslösen von Alarmzuständen (z. B. Bewegungsmelder, Scheibenbruchdetektoren) beschränkt werden. Aufzeichnungen sollen regelmäßig und automatisch gelöscht oder überschrieben werden.

Umgang mit den Kameras

Es sollten organisatorische Maßnahmen vereinbart werden, dass z. B. das Draufzoomen (auf ein Gesicht etc.) nur bei konkret erkannter Gefahr erlaubt ist.

Die Vereinbarung sollte besondere Maßnahmen zur Sicherung des Zugangs zu den Datenspeichern und den datenspeichernden Geräten vorsehen. Standalone-Systeme und Vier-Augen-Zugangsberechtigungen sichern den kontrollierten Zugriff auf Archivaufnahmen. Der Zugriff sollte an enge Kriterien gebunden werden und den Betriebsrat im jeweiligen Einzelfall einbeziehen. Überwachte Personen sind spätestens nach einer unberechtigten Auswertung zu informieren.

Automatische Gesichts-erkennung

Ein besonderer Überwachungsdruck wird durch den Einsatz von Gesichtserkennungssystemen aufgebaut. Wie Feldstudien zeigen, sind auch neuere Erkennungssysteme in erheblichem Maße fehleranfällig. Der automatische Bildabgleich führt zwar dazu, dass viele Personen aus einem vorgegebenen Raster fallen, auf der anderen Seite erhöht sich der Überwachungsdruck auf unbescholtene Restpersonen im Raster enorm. Der Einsatz der Technologie sollte daher abgelehnt werden.[23]

[23] Die besonderen Probleme des Einsatzes von Gesichtserkennungssystemen werden im Abschnitt „Biometrische Systeme“ erläutert.

VIII. Chipkarten und Biometrische Systeme

1. Grundlagen

Chipkarten im Scheckkartenformat sind ein Massenprodukt. Sie sind kostengünstig herzustellen, sind leicht administrierbar, und sie sind vielseitig: Theoretisch kann eine Chipkarte mit jedem System im Unternehmen verbunden werden, für das eine Authentifizierung der Beschäftigten erfolgt. Benötigt werden dazu nur ein entsprechendes Kartenlesegerät und eine Schnittstelle zu dem jeweiligen Anwendungsprogramm.

In der Praxis kommen freilich meist nur die folgenden Systeme zur Anwendung (einzeln oder kombiniert):

- Zeiterfassung,
- Zutrittskontrolle, Schließsystem,
- Loginkontrolle für Computer und
- Abrechnungssystem für die Kantine.

Wir beginnen mit einem Überblick über die in diesem Zusammenhang verwendete Chipkarten-Technologie „RFID“ („Radio Frequency Identification“ – Radiowellen-Identifikation), die ein berührungsfreies Auslesen der abgespeicherten Informationen ermöglicht. Anschließend werden die oben angeführten Systeme und ihr mitbestimmungsrechtlicher Regelungsbedarf erläutert.

Keine Datenverknüpfung der Systeme untereinander

Bei betrieblichen Regelungen ist erhöhte Aufmerksamkeit gefordert: Vor allem wenn die Teilsysteme im Rahmen einer Gesamtlösung von einem Hersteller kommen – aber nicht nur dann – besteht die Gefahr, dass die Datenströme der Teilsysteme miteinander kombiniert werden. Dann wären mitarbeiterbezogene Analysen möglich, um z. B. mit zwei Mausklicks zu ermitteln, welche Mitarbeiter sich während des Kantinenaufenthalts nicht am Zeiterfassungssystem abgemeldet haben oder wie lange ein bestimmter Mitarbeiter nach dem Einstempeln am Zeiterfassungssystem durchschnittlich benötigt, um mit seiner Arbeit am Arbeitsplatzrechner zu beginnen. Aus diesem Grunde gehört in jede Vereinbarung das prinzipielle Verbot, Bewegungsdaten aus den jeweiligen Systemen für andere Systeme verfügbar zu machen. Ausnahmen müssen dann im Einzelfall speziell erläutert und vereinbart werden.

Für Zonen und Einsatzbereiche, in denen besonders hohe Sicherheitsanforderungen herrschen, kann die Authentifizierung mittels Chipkarte ergänzt oder ersetzt werden durch weitere Maßnahmen, mit denen die Identität der Personen sichergestellt werden soll, zum Beispiel durch Eingabe einer persönlichen PIN-Nummer oder durch den Einsatz biometrischer Erkennungssysteme wie Fingerabdruck-Scanning, Iriserfassung oder videografische Gesichtskontrolle. Leider halten die Systeme oft nicht ein, was sie versprechen. Zum Abschluss des Kapitels gehen wir in diesem Zusammenhang auf die besonderen Gefahren der biometrischen Kontrollsysteme ein.

2. Mitarbeiterausweise mit RFID-Chips

RFID ist die Abkürzung für Radio Frequency Identification. Mithilfe von speziellen RFID-Chips können Informationen und Daten kontaktlos zu Lesegeräten gesendet werden. Jeder produzierte RFID-Chip verfügt dabei über eine eindeutige Identifikationsnummer.

Technik

RFID-Chips können überall dort eingesetzt werden, wo die Identifikationen erfolgen sollen. Pilotversuche laufen unter anderem bei den großen Einzelhandelsketten: RFID-Chips werden als Etiketten an den Waren angebracht. Etikettierte Ware im Einkaufswagen sendet ihren Preis automatisch an die Kasse, oder es kann überwacht werden, dass Produkte in die Regale nachgefüllt werden sollen. Die Anwendungsmöglichkeiten sind vielfältig. Der Einsatz der Technologie ist sehr umstritten, da das Missbrauchspotenzial schwer abschätzbar ist.[24]

Es gibt verschiedene Typen von RFID-Chips – wichtigstes Unterscheidungsmerkmal ist, ob der Chip über eine eigene Stromversorgung verfügt (aktiver Chip) oder nicht (passiver Chip). Beim Einsatz zur Mitarbeiteridentifikation werden passive Chips eingesetzt. Diese Chips senden nur dann Signale, wenn sie in Reichweite eines Lesegeräts geraten. Aus diesem Grunde sind Gefahren für die Gesundheit der Beschäftigten nach dem derzeitigen Stand der Wissenschaft als gering einzuschätzen.

Die Reichweiten passiver RFID-Chips sind dabei für verschiedene Zwecke unterschiedlich ausgelegt. Chipkarten für Beschäftigte reagieren in der Regel im Umkreis von maximal 50 cm auf die korrespondierenden Lesegeräte.

Heimliches Auslesen der Karten

Die Karten senden Daten selbstständig, sobald sie in die Nähe eines Lesegerätes geraten. Problematisch ist, dass dies dem Nutzer nicht signalisiert wird. Er kann die Sendefunktion auch nicht abschalten, ohne den Chip zu beschädigen. Die Standorte von Lesegeräten in den Unternehmen sollten den Mitarbeitern deshalb bekannt sein; bei einer

[24] Eine umfangreiche Zusammenfassung der Probleme im Alltag der Konsumenten bei Foebud e.V.: http://www.foebud.org.

entsprechenden Lesegerätedichte könnte das Unternehmen Bewegungsprofile seiner Beschäftigten ermitteln.

Denkbar ist weiterhin, dass die Karten auch dann sendeaktiv werden, wenn sie in die Nähe von unternehmensfremden Lesegeräten geraten, z. B. an der Tankstelle nebenan. Ob der Chip Informationen in diesen Fällen versendet und wenn ja, ob in unverschlüsselter Form, hängt von der Bauart des Chips ab: Es gibt Chips, die überprüfen, ob das Lesegerät Informationen anfordern darf. Und es gibt Chips, die Informationen auch dann nur verschlüsselt übermitteln.

Freilich: Selbst wenn Informationen unverschlüsselt an Fremdgeräte versendet werden würden, würde ein Schnüffler in der Regel als einzige Information die Kartensystemnummer erhalten, denn Personalnummer oder Mitarbeitername werden nicht direkt auf dem Chip gespeichert – die Zuordnung der Kartensystemnummer zu den Beschäftigten erfolgt beim Unternehmen mithilfe spezieller Softwaresysteme, an die Außenstehende nicht herankommen.

Regelungsaspekte

Betriebs- oder Personalräte sollten die Sendereichweite der RFID-Chips klären und dafür sorgen, dass die Zahl der Standorte der Lesegeräte übersichtlich bleibt und die Beschäftigten nicht unbemerkt „durchleuchtet“ werden. Zu klären ist außerdem, dass die Daten vom Chip nur an authentifizierte Lesegeräte übermittelt werden und dass der Datentransfer möglichst verschlüsselt stattfindet.

Zu vereinbaren sind die genauen Dateninformationen, die auf den Chipkarten abgespeichert werden. Und natürlich können die Chipkarten auch bedruckt und mit einem Foto versehen werden. Oft werden sie dann sichtbar getragen und dienen im Unternehmen als Mitarbeiterausweis. Alle Informationen, die auf die Chipkarte aufgedruckt werden, sollten daher auch vereinbart werden.

Unter Umständen sollte geklärt werden, was bei Kartenverlust passiert und wie mit Haftungsfragen umgegangen wird

3. Zeiterfassung

Chipkarten

Erster Ansatzpunkt einer betrieblichen Regelung ist die Dokumentation des Gesamtsystems. Dazu gehört auch die Beschreibung der eingesetzten Chipkarten, insbesondere der auf ihnen abgespeicherten Daten.

Zeiterfassungsgeräte

Die Bedienung der Zeiterfassungsterminals durch die Beschäftigten muss schnell, intuitiv und ohne Missverständnisse möglich sein. Ob dies der Fall ist, kann man als Betriebsrat am besten nach einem Selbstversuch an einem Testsystem beurteilen. In punkto Funktionsvielfalt gilt „Weniger ist mehr!“, denn zu viele Informationen verwirren.

Es ist daher keine schlechte Idee, in einer Regelung festzuhalten, dass z. B. nur die folgenden aufgeführten Funktionen über vier Buchungstasten aufgerufen werden können

- Kommen,
- Gehen,
- Dienstgang und
- Saldo-Anzeige des Zeitkontos.

Fehlbedienungen der Geräte sollten den Beschäftigten unmittelbar durch akustische und optische Warnmeldungen signalisiert werden.

Unbedingt sollten die genauen Standorte der Zeiterfassungsgeräte in einer Anlage dokumentiert werden, denn hier gibt es häufig Kontroversen zwischen Arbeitgeber und Betriebsrat. Nicht selten versucht der Arbeitgeber mit Einführung der neuen Technik, durch die „Hintertür" neue Aufstellorte der Geräte (vom Betriebseingang näher an die Arbeitsplätze heran) durchzusetzen. In jenem Fall wäre zusätzlich über Zeitgutschriften für die Wegezeit zu verhandeln.

Technisch sehen alle Zeiterfassungssysteme vor, dass Beschäftigten bestimmte Terminals zugeordnet werden können, so dass sie nur an diesen Stellen den Betrieb betreten und ihre Arbeitszeit buchen können. Zumindest bei kleineren Betrieben ist diese Regelung unnötig einschränkend und sollte daher ausgeschlossen bleiben. Vielleicht kann man Ausnahmen für große Gebäude in Betracht ziehen, doch dafür müsste es triftige Gründe geben, die im Vereinbarungstext berücksichtigt werden sollten.

Ein wesentlicher Punkt einer jeden Vereinbarung zur Zeiterfassung ist natürlich die Frage, welche Daten erfasst werden, wie sie gespeichert und wie sie ausgewertet bzw. weiterverwendet werden.

Buchungen

Der Umfang der mit dem Buchungsvorgang verbundenen Datenerfassung ist festzuhalten und zu beschränken:

- Ausweisnummer,
- Datum und Uhrzeit der Buchung und
- Art der Buchung (Kommen, Gehen usw.).

Positiv- und Negativ-Erfassung

Grundsätzlich ist bei den Buchungen zu unterscheiden, ob das System zur *Positiverfassung* oder *Negativerfassung* verwendet werden soll. Bei der Positiverfassung werden tatsächlich Anmelde- und Abmeldestempel im System verbucht, während bei der Negativerfassung Meldungen

an das System nur in den Fällen erfolgen, in denen Abweichungen von der geplanten Arbeitszeit vorliegen. Anderenfalls nimmt das System dann an, dass die betroffenen Personen so gearbeitet haben, wie dies für sie geplant war. Bei festen Arbeitszeiten ist dieses System ökonomischer und auch aus Datenschutzgründen empfehlenswert. Aber auch bei der Positiverfassung kann vereinbart werden, dass Arbeitszeiten nicht sekundengenau abgerechnet werden.

Nicht selten ist auch der Umgang mit Pausenzeiten zwischen den Betriebsparteien strittig. Vorzuziehen sind Lösungen, bei denen die Pausenzeiten pauschal von der Arbeitszeit abgezogen werden, so dass entsprechende An- und Abmeldungen für Pausen an den Erfassungsgeräten nicht notwendig sind. Im Fall einer abweichenden Pausendauer könnten die Beschäftigten ggf. entsprechende Korrekturbuchungen vornehmen. Bei einer Stempelpflicht für Pausenzeiten ist wiederum zu prüfen, ob man als Betriebsrat die Standorte der Zeiterfassungsterminals mittragen kann.

Systemarchitektur

Ob und inwieweit auch Aussagen zu den erlaubten Auswertungen vorgenommen werden sollen, ist in erster Linie eine Frage der Systemarchitektur: Viele Zeiterfassungssysteme werden tatsächlich nur für die Vornahme der Buchungen eingesetzt. Die Rohdaten werden auf Plausibilität geprüft und am Ende des Tages in das Lohn- und Gehaltsabrechnungssystem überführt. In diesen Fällen sollten betriebliche Regelungen vorsehen, dass Auswertungen im Zeiterfassungssystem komplett abgeschaltet werden. Alle zulässigen Auswertungen werden dann im Gehaltsabrechnungssystem definiert und dort geregelt. Die transportierten Rohdaten sind anschließend aus dem Zeiterfassungssystem zu löschen.

Soll die Verarbeitung der Daten tatsächlich vom Zeiterfassungssystem vorgenommen werden, so sind mindestens die vom System verwendeten Zeitarten zu vereinbaren. Sensibel sind naturgemäß besonders die Fehlzeiten, sie sollten nicht zu detailliert aufgeschlüsselt werden. Weiterhin sollten alle zulässigen Auswertungen in einer Anlage mit Verteilerkreis und Häufigkeit der Erstellung übernommen werden. Hier können auch Auswertungen hinterlegt werden, deren Empfänger der Betriebsrat ist, z. B. Überstundenübersichten. Möglichkeiten zur freien Abfrage der Zeitdatenbank sind abzuschalten. Der Datenexport nach Excel oder vergleichbare Programme ist zu untersagen.

Berechtigungen

Der Zugriff auf Korrekturbuchungen und die Verarbeitungfunktionen des Systems ist auf die zuständigen Zeitbeauftragten zu begrenzen. Mit der Systemverwaltung betraute Personen sollten Zugriff auf arbeitnehmerbezogene Daten nur zum Zweck der Fehlerbehandlung erhalten.

Keine Datenverknüpfung mit anderen Systemen

Und in jedem Fall sollte klargestellt werden, dass die Zeitdaten nicht mit Daten anderer Systeme verknüpft werden, es sei denn, Betriebsrat und Arbeitgeber haben im Einzelfall abweichende Regelungen getroffen.

Regelungsaspekte

Vereinbarungen zu Zeiterfassungssystemen gründen auf den betrieblichen Regelungen zur Arbeitzeit. Nahezu jedes Arbeitszeitreglement kann durch die technischen Systeme abgebildet werden. Arbeitszeitfragen müssen daher in einer Vereinbarung zum System in der Regel nicht geklärt werden. Geregelt werden sollten indes die folgenden Aspekte:

- Zeiterfassungsgeräte: Anzeigen, Bedienung und vor allem die Aufstellorte.
- Buchungen im System: Negativerfassung ist der Positiverfassung vorzuziehen, Pausen sollten möglichst pauschal abgezogen werden.
- In der Regel werden die Daten des Zeiterfassungssystems an SAP oder ein anderes Gehaltsabrechnungssystem zur Verarbeitung weitergeleitet. Wie oben beschrieben ist der Datenfluss der Zeitdaten zu fixieren.
- Zu klären ist der Umfang der Zugriffs-Berechtigungen.
- Falls zur Bedienung Chipkarten eingesetzt werden, sind nähere Bestimmungen zu deren Einsatz sinnvoll.

4. Zutrittskontrolle

Gerade in jüngster Zeit führen viele Unternehmen oft besondere sicherheitsgefährdende Bedrohungslagen an. In der Regel halten diese Analysen einer Belastung nicht stand. Betriebs- und Personalräte sollten dem Arbeitgeber auch deshalb nicht alles, was technisch möglich ist, gestatten. Mit einer entsprechenden Vereinbarung kann man dem überflüssigen Überwachungszauber einen Riegel vorschieben und erhält im Ergebnis stattdessen eine moderne und leicht administrierbare Schließanlage.

Grundsätzlich steigt durch den Einsatz einer elektronischen Schließanlage die Gefährdung der Persönlichkeitsrechte der Beschäftigten. Denn durch Protokolldateien, die vom System im Hintergrund angelegt werden können, wird die Benutzung von Türen nachvollziehbar und überwachbar. Im Laufe von Tagen und Wochen könnten so komplette Laufwege der Beschäftigten aufgezeichnet und ausgewertet werden.

Zentrale Protokolle

Ob und welche Daten gespeichert werden, lässt sich technisch auf unterschiedliche Weise realisieren. Aus Mitbestimmungssicht ist es

besonders problematisch, wenn die Informationen über die Türbetätigungen der Beschäftigten von den Schließzylindern in ein zentrales Datenbank-System übermittelt werden. In diesem Fall können mit entsprechenden Auswertungswerkzeugen Bewegungsprofile von Beschäftigten in Sekundenschnelle erzeugt und ausgewertet werden.

Lokale Protokolle

Möglich wäre es, Daten über die Türbenutzung jeweils lokal an den jeweiligen Schließzylindern zu halten und den Zugriff auf die Daten dann nur in speziellen Situationen vorzunehmen. Auf diese Weise ließe sich zumindest ein Vollzugriff über Daten aller Türen verhindern.

Keine Protokolle

Glücklicherweise lassen sich diese Funktionen jedoch auch komplett ausschalten: Im „Normalfall“ funktionieren die den Beschäftigten zur Nutzung übergebenen Chipkarten dann als reine Schlüsselkarten und es erfolgt keine Protokollierung der Benutzung von Türen.

Die Protokollierung kann in einer Vereinbarung jedoch für hochsensible Bereiche, z. B. Serverräume, zugelassen werden. Dann sollte jedoch der Umfang der gespeicherten Daten festgehalten werden. Außerdem ist zu klären und zu erörtern, ob nur das Betreten oder auch das Verlassen von Bereichen protokolliert werden soll.

Auswertungen

Besonders kritisch ist die Frage, wer zu welchen Zwecken auf die erzeugten Protokolldaten zugreifen darf. Im Rahmen des Einsatzes von Schließsystemen kommen eigentlich nur begründbare Missbrauchsfälle in Betracht. Oft wird eine gemeinsame Bewertung der Anhaltspunkte mit den Betriebsräten vereinbart, um unkontrollierte Überprüfungen durch die Arbeitgeberseite von vornherein zu verhindern. Möglicherweise bietet das eingesetzte Produkt sogar die Möglichkeit, eine unberechtigte Auswertung der Daten technisch auszuschließen, falls etwa zwei getrennte Passworte für die Freigabe der Auswertungsfunktionen erforderlich sind.

Keine Datenverknüpfung mit anderen Systemen

Selbstverständlich sollte auch beim Einsatz eines Zutrittskontrollsystems ausgeschlossen werden, dass es mit weiteren Systemen (z. B. Videoüberwachung, Zeiterfassung) verbunden wird.

Regelungsaspekte

Aus dem oben Angeführten lassen sich die folgenden Mindestinhalte für eine Vereinbarung zur Zutrittskontrolle aufführen:

- Reduktion der Chipkarte auf die Schlüsselfunktion, d. h. möglichst keine Protokollierung. Ausnahmen für besonders sensible Bereichen sind zu definieren.
- Regelung zu den Auswertungen der Protokolle
- Keine Verknüpfung der Daten mit anderen Systemen

- Falls zur Bedienung Chipkarten eingesetzt werden, sind nähere Bestimmungen zu deren Einsatz sinnvoll.

Da im Zusammenhang mit der Einführung eines neuen Zutrittkontrollsystems häufig weitere Sicherheitssysteme angeschafft werden, sollten Betriebsräte unbedingt klären, ob dies auch in ihrem Betrieb der Fall ist.

5. Login-Kontrolle

Die Anmeldung von Benutzern an den Arbeitsplatzcomputern per Benutzername und Passwort ist den Verantwortlichen in den IT-Abteilungen der Unternehmen ein Gräuel. Denn allzu häufig stehen Passworte unter der Tastatur der Beschäftigten oder lassen sich leicht erraten. In diesem Fall stehen „Haus und Hof“ und damit Computerdaten offen. Eine Situation, vor der sich ein Unternehmen so gut es geht schützen will.

Ein Ansatz sieht vor, die Eingabe des Benutzernamens bei der Systemanmeldung zu ersetzen durch die Identifikation per Chipkarte. Wenn man die Chipkarten-Identifikation mit der verpflichtenden Abfrage eines Passworts verkoppelt, ist zur Anmeldung im System also Besitz (die Chipkarte) und Wissen (Kenntnis des Passworts) notwendig und man erreicht einen Zugewinn an Sicherheit.

Im Idealfall ist mit der System-Anmeldung die Freischaltung für einzelne Anwendungssysteme des Benutzers verknüpft. Im Fachjargon spricht man vom „Single-Sign-On“, also der „einmaligen Anmeldung“ für viele Programme. Dessen Realisierung ist freilich hohe Kunst und obwohl viele IT-Abteilungen entsprechende Projekte verfolgen, sind die Erfolge aufgrund zu zahlreicher alter Anwendungssysteme häufig bescheiden.

Betriebsräte können dem Einsatz eines Chipkarten-Systems zur Login-Kontrolle jedoch im Allgemeinen gelassen entgegensehen.

Informationen auf der Chipkarte

Eine Regelung sollte zunächst festhalten, welche Informationen auf der Chipkarte abgespeichert sind. Möglicherweise wird der Schlüsselcode für das Login-System gesondert erzeugt und zusätzlich zu weiteren persönlichen Daten auf der Karte abgespeichert.

Systemprotokolle

Üblicherweise ist mit der Verwendung des neuen Anmeldeverfahrens keine Änderung des Login-Verhaltens verbunden. Es laufen lediglich die „üblichen“ Systemprotokolle im Hintergrund des Betriebssystems, mit dem Rückkopplung gegeben wird, ob Anmeldungen erfolgreich waren oder abgewiesen werden mussten. Falls zusätzliche Protokolle, die möglicherweise zentral auf dem Server zur Auswertung bereit liegen, erzeugt werden sollen, ist die Notwendigkeit zu hinterfragen und zu erörtern.

Der Zugriff auf Systemprotokolle gleich welcher Art sollte jedoch in jedem Fall nur für Zwecke der Fehleranalyse und der Gewährleistung der Systemsicherheit erlaubt werden. Sofern dazu in einer EDV-Rahmenvereinbarung keine Aussagen getroffen worden sind, kann die Einführung des Login-Systems zum Anlass genommen werden, eine entsprechende Regelung im Vereinbarungstext zu verankern.

Missbrauch der Karten

Die Integrität der Beschäftigten wird beschädigt, wenn Mitarbeiter der Systemadministration oder gar externe Personen unbemerkt Dubletten der Chipkarten anlegen könnten und sich auf diese Weise unter falscher Identität an den Systemen anmelden könnten. Auf die vom Missbrauch betroffenen Beschäftigten würde in diesem Fall ein erheblicher Erklärungsdruck ausgeübt werden. Der Arbeitgeber sollte deshalb technisch sicherstellen, dass keine Kopien der ausgegebenen Karten erstellt werden können und jede Identifikationsnummer einzigartig ist. Gegebenenfalls ist das Verfahren für das Erzeugen und Speichern der Informationen zu erläutern. Falls in diesem Zusammenhang Pin-Nummern oder vergleichbare Passworte erzeugt werden, ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass diese ausschließlich den berechtigten Karteninhabern bekannt gemacht werden.

Anmeldung mit Token

Besonders sicherheitskritisch sind Login-Prozesse von außerhalb in das Unternehmensnetzwerk, z. B. um als Außendienstmitarbeiter ein Notebook im Netzwerk anzumelden. Immer noch wird in vielen Unternehmen ein Anmeldeverfahren verwendet, das die Eingabe von Benutzernamen und einem Passwort voraussetzt. Problematisch daran ist, dass Passworte häufig leicht zu knacken sind. Sei es, weil die Nutzer Passworte aus ihrem Umfeld wählen (Name der Katze usw.) oder unter ihrem Notebook notieren. Aber auch bedachtsam gewählte Passworte sind von Hackern mit entsprechenden Programmen unter Umständen ohne allzu großen Aufwand zu knacken.

Die Verwendung einer Chipkarte zur Benutzeridentifikation ist in dieser Hinsicht schon ein erheblicher Sicherheitsgewinn, denn die Kenntnis des Nutzernamens reicht für Angriffsversuche nicht mehr aus; ein Angreifer muss sich im Besitz der Chipkarte des Nutzers befinden. Besonders sicher beim Einsatz von Mobilrechnern sind dabei Login-Verfahren, bei denen die Beschäftigten mithilfe eines kleinen Anzeigegeräts („Token“) für wenige Minuten einen eindeutigen Authentifizierungscode für die Anmeldung erzeugen können.

6. Abrechnungssysteme für die Kantine, Parkplatz-Ticketing und andere Systeme

Der Einsatz von Chipkarten auf Mitarbeiterausweisen oder vergleichbaren Identifikationskarten kann im Prinzip beliebig auf weitere betriebliche Systeme ausgeweitet werden. Notwendig ist dazu nur ein Kartenlesegerät und eine Software-Schnittstelle, die die Authentifikation der Nutzer ermöglicht.

Regelungsaspekte

Betriebs- und Personalräte sollten sich in diesen Fällen darüber informieren, ob bei der Benutzung der Karten überhaupt eine Protokollierung im System vorgenommen wird: Wenn die Karten auf die Funktion eines Schlüssels reduziert werden, wie zum Beispiel zum Öffnen einer Schranke zum Betriebsparkplatz, ist eine Protokollierung vollkommen unnötig. In diesem Fall stehen keine Daten zu Verfügung, die zur Kontrolle der Beschäftigten verwendet werden könnten. Ein Systemeinsatz ohne Protokollierung ist daher immer das Regelungs-Optimum für eine Vereinbarung.

Wenn bei der Bedienung allerdings personenbezogene Daten anfallen, so ist zu prüfen, ob die Datenhaltung dezentral in den Systemen vorgenommen werden kann. Wenn das der Fall ist, stellt sich die Frage, wann und zu welchen Zwecken auf diese Informationen zugegriffen werden darf und welche Personen die Zugriffsrechte besitzen. Das alles sollte detailliert geregelt werden.

Den weitesten Regelungsbedarf löst ein System aus, bei dem die Authentifizierungsinformationen zentral gespeichert werden und dort der Weiterverarbeitung harren. Auch hier bedarf es einer Regelung, unter welchen Umständen die gespeicherten Daten verwendet werden dürfen, welche Auswertungen in welchem Auswertungsrhythmus zulässig sind und welche Personen zugriffsberechtigt sind.

Beispiel

Besondere Vorsicht ist angebracht, wenn der Arbeitgeber einen Abgleich der erhobenen Daten mit Daten aus anderen Systemen plant: Mithilfe von Zeitstempeln der bedienten Teil-Systeme kann man das Verhalten von Beschäftigten kontrollieren oder Bewegungsprofile rekonstruieren:

- 7:50 Uhr – Mitarbeiter xy benutzt die Parkplatzschranke
- 7:58 Uhr – Mitarbeiter xy meldet sich am Zeiterfassungssystem an
- 8:02 Uhr – Mitarbeiter xy benutzt den Fahrstuhl
- 8:03 Uhr – Mitarbeiter xy öffnet die Tür zu den Büroräumen der 3. Etage
- 8:22 Uhr – Mitarbeiter xy loggt sich an seinem Rechner ein (Warum dauert das 19 Minuten?)

- 9:13 Uhr – Mitarbeiter xy loggt sich wieder aus
- 9:22 Uhr – Bestellvorgang in der Kantine
- usw.

Im Regelfall ist die Zusammenführung der Daten der Teilsysteme sachlich nicht zu begründen bzw. aufgrund der erheblichen Gefahr einer missbräuchlichen und unangemessenen Überwachung der Beschäftigten durch die Mitarbeitervertretung abzulehnen.

7. Biometrische Erkennungssysteme

Seit mehreren Jahren sind biometrische Erkennungssysteme auf dem Markt, deren Hersteller mit ihrem Einsatz eine zuverlässige Identifizierung und Authentifizierung von Benutzern versprechen. Jeder Mensch verfügt über einzigartige Merkmale, vom Aussehen über Bewegungen bis hin zu Aussprache und Geruch. Die zurzeit am häufigsten eingesetzten Erkennungssysteme sind:

- Gesichtserkennung durch Kameras,
- Iriserkennung durch Kameras und
- Fingerabdruckerkennung durch Scan-Systeme.

Die Hersteller der biometrischen Systeme versprechen anhand der abgetasteten Merkmale eine eindeutige Identifikation von Personen (zumindest in der Theorie – zur Kritik unten mehr Informationen). Um einen Vergleich zu ermöglichen, müssen dabei Daten von Gesichtern und Fingerabdrücken im Erkennungssystem hinterlegt und abgespeichert werden.

Schwachstellen

Leider verschweigen die Herstellerfirmen die oft eklatanten Schwächen der Systeme. Und auch die Anwender halten sich in der Regel mit öffentlicher Kritik bedeckt, denn jeder Hinweis auf die Schwächen eigener Sicherheitssysteme wäre ja wieder ein weiteres Risiko. Dennoch findet man mit wenig Mühe im Internet viele Informationen über fehlgeschlagene Biometrie-Projekte. So scheitert etwa die zuverlässige Identifizierung von Personen mithilfe von Gesichtserkennungsverfahren bereits dann, wenn die Lichtverhältnisse nicht optimal sind oder wenn Gesichter nur außerhalb eines festgelegten Winkelbereichs erfasst werden können.[25]

[25] Als Beispiel sei hier ein 2007 vom Bundeskriminalamt erfolglos abgebrochener Versuch zur Gesichtserkennung im Hauptbahnhof Mainz angeführt: http://www.bka.de/kriminalwissenschaften/fotofahndung/.

Für republikweites Aufsehen hat ein Bericht des Fernsehmagazins „plusminus“ aus dem Jahre 2007 gesorgt, in dem gezeigt wurde, wie man als Laie mit etwas Sekundenkleber, Holzleim, Folie, einer Digitalkamera und 30 Minuten Zeit ein teures Fingerabdruck-Scansystem überlisten kann. Ausgangspunkt ist dabei eine gewöhnliche Kaffeetasse oder ein Glas, auf dem die „Zielperson“ seinen Fingerabdruck hinterlassen hat. Im Fernsehbeitrag[26] gelang es, mit einem gefälschten Fingerabdruck auf Kosten anderer Einkäufe an einer modernen Fingerabdruck-Kasse vorzunehmen. Trotz der eklatanten Schwächen bezeichnet der Hersteller das System im Beitrag übrigens als sicher. Kein Wunder, dass man angesichts dessen als Betriebsrat ins Grübeln kommen sollte, denn dieselbe Technologie wird auch für Sicherheits-„Lösungen“ im Unternehmen angeboten.

Regelungsaspekte

Falls im Unternehmen biometrische Systeme eingeführt werden sollen, ist also zunächst zu hinterfragen, ob der Technikeinsatz tatsächlich den notwendigen Sicherheitsanforderungen entspricht oder ob das System ineffizient arbeitet oder im schlimmsten Fall sogar manipuliert werden kann.

Aus Sicht der Betriebsräte gibt es darüber hinaus weitere schwerwiegende Einwände:

Biometrische Daten sind höchstpersönliche Daten. An Ihre Speicherung und Verwendung sind ganz besonders hohe Datenschutz-Anforderungen zu stellen. Falls die Daten in die Hände Dritter gelangen, sind die negativen Folgen für davon betroffene Personen in ihrem Ausmaß nicht ansatzweise abzuschätzen: Im Unterschied zu Passworten sind Fingerabdrücke, Irisinformationen o. Ä. nämlich nicht austauschbar. Eine fehlerhafte Konfiguration, ein Dateneinbruch, eine Unachtsamkeit im Umgang mit den Daten können daher lebenslange Beeinträchtigungen des Trägers nach sich ziehen. Möglicherweise wären die Daten sogar zur Manipulation von Ausweisdokumenten verwendbar. Ab Ende 2009 können Fingerabdruckdaten in Personalausweisen gespeichert werden.

Bei einigen Personen ist das Fingerabdruckprofil zu wenig ausgebildet ist, um beispielsweise per Scan-Verfahren verwendet werden zu können. Und wer sich nach dem Urlaub unrasiert mit 7-Tage-Bart am Gesichtserkennungssystem anmelden will, muss damit rechnen, Alarm auszulösen.

Sicherlich wird die Industrie in den kommenden Jahren besser funktionierende Produkte entwickeln und anbieten. Auf dem Stand der Technik des Jahres 2008 sind die uns vorgeführten Systeme bislang jedoch nicht zustimmungsfähig gewesen.

[26] Der bemerkenswerte Beitrag ist im Internet unter http://www.daserste.de/mediathek_blank/play.asp?cid=12635 abrufbar.

IX. Betriebsdaten

1. Grundlagen

Eine alte Forderung der IG Metall war es, die Betriebsdaten strikt von den Personaldaten zu trennen – und dieses Anliegen ist in vielen Betriebsvereinbarungen auch umgesetzt worden, bis mit der Erfindung der Data oder Business Warehouses die säuberlich getrennten Daten wieder unter einem Dach versammelt wurden.

Die Forderung nach Datentrennung hatte ihre großen Erfolge in der Zeit vor dem Internet. Denn mit der Verbreitung der Internet-Techniken machte das Verknüpfen und Verbinden von Daten einen regelrechten Quantensprung. Programmiersprachen wie Java erlauben es einem Systementwickler, Programme zu schreiben, die sich die Daten von überall auf der Welt zusammenholen, aus unterschiedlichsten Quellen, und das ohne große Mühe. Einzig und allein fehlende Zugriffsrechte und Nichterreichbarkeit können diesem Sammeleifer noch im Wege stehen.

Was sind Betriebsdaten?

Unter Betriebsdaten versteht man alles, was an Daten über Zustände und Prozesse in einem Betrieb anfällt. Da geht es vordergründig um Produktionsdaten, vor allem um Daten, die den Arbeitsfortschritt beschreiben (Beginn, Ende, Dauer einzelner Arbeitsschritte), aber auch Stückzahlen, Unterbrechungen des Produktionsablaufs und Angaben über die Qualität gefertigter Produkte fallen darunter. Bei einer anderen Gruppe von Betriebsdaten geht es um die Kosten für einzelne Arbeiten, Maschinen oder sonstige Einrichtungen, den Verbrauch von Material oder Energie. Wieder andere Daten beziehen sich nur auf Maschinen und deren innere oder äußere Zustände (Drehzahlen, Temperaturen, Immissionen usw.). Eine Vielzahl unterschiedlichster Programme kümmert sich um die Verarbeitung dieser Datenflut.

Die dank des fortgeschrittenen Computereinsatzes „gläserne Produktion“ findet in der betriebsverfassungsrechtlichen Praxis leider keine vergleichbare Beachtung wie der „gläserne Mensch“, obwohl die produktionsnahen Systeme oft eine wesentlich detailreichere Kontrolle der Leistung oder des Verhaltens erlauben als die im Personalbereich eingesetzten Systeme.[27]

2. Produktionssteuerungssysteme

Produktionsplanung

Eine wichtige Gruppe der betriebsdatenverarbeitenden Systeme sind die Produktionsplanungs- und -steuerungssysteme (PPS). Dabei wird

[27] Vereinbarungsentwürfe unter http://www.tse.de/vereinbarungen/produktion/.

zunächst der Produktionsablauf geplant. Alle Maschinen und Anlagen sind im System mit ihren Kapazitäten beschrieben. Ebenso sind für alle denkbaren Arbeitsschritte Plandaten hinterlegt. Sie entstehen entweder durch direkte Messung nach anerkannten Verfahren wie REFA oder durch Schätzungen und Beobachtungen. Jeder Produktionsauftrag wird in Arbeitsfolgen und einzelne Arbeitsschritte zerlegt. Das System errechnet dann den Produktionsplan unter Berücksichtigung der Maschinenkapazitäten. Bis hierher handelt es sich nur um die Produktionsplanung auf der Grundlage von Soll-Daten. Eine Menge Arbeit muss in die Einrichtung eines solchen Systems hineingesteckt werden, bis es in der Lage ist, Aufträge einigermaßen verlässlich zu planen. Oft gehen zwei oder drei Jahre ins Land, bevor man den Fortschritt bestaunen kann. Ein Grund auch dafür, dass Betriebsräte oft nicht mitbekommen, was sich hier tut, zumal das Thema Überwachung erst dann ins Spiel kommt, wenn den Soll-Daten die Ist-Daten über den tatsächlichen Produktionsablauf gegenübergestellt werden, mit anderen Worten, wenn die Produktionsplanung um eine Produktionssteuerung erweitert wird. Und dazu braucht man Rückmeldungen aus der Produktion und ein Betriebsdatenerfassungssystem, um diese Rückmeldungen zu erfassen.

Produktionssteuerung

Bescheiden ausgelegte Systeme begnügen sich mit einfachen Fertigmeldungen von Produktionsaufträgen oder einzelnen Auftragsfortschritten. An diesen haben in der Regel mehrere Beschäftigte gearbeitet und meist unterschiedliche Personen, so dass die Überwachungseignung nicht hoch ist. Der Arbeitgeber ist aber in der Lage, festzustellen, ob die Arbeiten noch im Plan liegen.

Ein etwas genaueres Verfahren ist das Meilenstein-Verfahren. Hier ermittelt man kritische Stellen im Produktionsablauf und stellt dort Rückmeldeterminals auf. Meist lassen sich diese Daten auch nicht auf einzelne Personen beziehen. Vor allem erlauben sie keinen direkten Soll-Ist-Vergleich der Arbeiten, weil nicht jeder einzelne Arbeitsschritt dem System gemeldet wird. Ein solches System lässt sich immer im Frieden mit den Betriebsräten regeln.

Kritischer wird es, wenn jeder einzelne Arbeitsschritt an das System zurückgemeldet werden soll. Geschieht dies in zeitversetzten Sammel-Rückmeldungen, so ist auch in diesem Fall nur eine eingeschränkte Kontrolle möglich. Die Überwachung wird aber perfekt, wenn Anfang und Ende einer jeden Arbeit zeitgenau an das System gemeldet werden muss. Dann haben wir die gläserne Arbeit, bei der jeder Arbeitsschritt mit der Planung verglichen werden kann.

Fast alle käuflichen Systeme sind in der Lage, die Rückmeldungen in personenbezogener Form vorzunehmen. Damit ist dann das Maximum möglicher Kontrolle erreicht: Die Zeit für jede geleistete Arbeit kann dann mit der geplanten Zeit vergleichen werden, und das Ergebnis dieser Überwachung lässt sich direkt einer Person zuordnen.

Regelungs-aspekte

Es würde den Rahmen dieses Buches sprengen, wenn wir hier darstellen wollten, wie man mit der Vielfalt der handelsüblichen Systeme unter dem Gesichtspunkt des Schutzes vor den Gefahren einer technischen Überwachung umgehen sollte. Wir beschränken uns auf einige Grundsätze:

- Wenn nicht wichtige Gründe dagegen sprechen, sollte eine Rückmeldung jeder einzelnen Arbeit vermieden werden. Die sanfteste Methode ist der Verzicht auf die Meldung von Uhrzeiten bei der Fertigmeldung. Auch ein „Meilensteinverfahren“ kommt in Betracht.

- Ein direkter Personenbezug ist nur erforderlich, wenn die verbrauchten Zeiten im Rahmen eines Leistungslohnsystems weiterverwendet werden müssen. Ansonsten darf eine persönliche Identifikation nur zur Überprüfung der Berechtigung verwendet werden.

- Statt Beginn und Ende einer einzelnen Arbeit zeitgenau zurückzumelden, ist es für die meisten Zwecke der Produktionssteuerung völlig ausreichend, nur das Ende der Arbeiten (oder nur deren Beginn) an das System zurückzumelden.

- Die Überwachungsgenauigkeit sinkt beträchtlich, wenn die Rückmeldungen zeitverschoben (z. B. am Ende einer Schicht) erfolgen. Die Wahl des Zeitpunktes für die Rückmeldungen hängt von der gewünschten Genauigkeit für die Terminverfolgung ab. Hier sind Kompromisse möglich.

- Die Feinsteuerung der Produktion erfolgt meist in zur Auftragsverarbeitung vorgelagerten Systemen, die oft über einen Leitstand verfügen. Hier kann man die Speicherdauer für die detaillierten Informationen relativ kurz wählen und dafür sorgen, dass nur zusammengefasste Informationen an das Hauptsystem weitergegeben werden.

- Vor allem in Konzernen und größeren Unternehmen werden Systeme eingesetzt, bei denen Informationen über die Feinsteuerung der Produktion an konzern- oder unternehmenszentraler Stelle erfolgen sollen. Einem solchen Verfahren sollte man als Betriebsrat nicht zustimmen, sondern dafür sorgen, dass die Daten „vor Ort“ bleiben.

- Oft werden Produktionsunterbrechungen und Störungen separat erfasst, in vielen Fällen ergänzt um eine Angabe des Unterbrechungsgrundes. Auch hier sollte man dafür sorgen, dass die Erfassung ohne direkten Personenbezug erfolgt und dass keine Unterbrechungsgründe gewählt werden, die ein persönliches Verhalten der Beschäftigten beschreiben.

3. Andere betriebsdatenverarbeitende Systeme

Produktionssteuerungssysteme sind nicht die einzigen betriebsdatenverarbeitenden Systeme mit hohem Überwachungspotenzial. Ähnliche Problemlagen gibt es bei

- Projektsteuerungssystemen,
- Qualitätssicherungssystemen,
- Instandhaltungssystemen,
- Trouble-Ticket-Systemen in Service Centern und
- Systemen zur Unterstützung des Customer Relationship Managements oder des Außendienstes,

um nur einige Beispiele zu nennen. Bei allen Systemen sollte man zuerst prüfen, ob ein direkter Personenbezug unbedingt erforderlich ist.

Regelungsaspekte

Wenn sich dieser direkte Personenbezug nicht vermeiden lässt, dann sollte man festlegen, dass die persönliche Kennung einer Mitarbeiterin oder eines Mitarbeiters nur im Einzelfall, z. B. zur Kenntlichmachung einer Ansprechperson, verwendet werden darf und dass keine statistischen Auswertungen mit Personenbezug erstellt werden dürfen.

Lässt sich auch dies nicht vermeiden, dann bleibt nur, jede zulässige Auswertung einzeln festzulegen.

X. Globalisierungsfolgen

Viele Unternehmen, vor allem die multinationalen Konzerne, ziehen ihre Datenverarbeitung nach weltweit einheitlichem Muster auf. „Harmonisierungsprojekte“ nennen sich diese oft zwei- und dreistellige Euro- oder Dollar-Millionensummen kostenden Vorhaben. So werden dann zum Beispiel 43 verschiedene, weltweit verstreute SAP-Installationen zu einer „integrierten Lösung“ zusammengefasst.

1. Weltweite Zentralisierungstendenzen

Der Aufwand eines solchen Projekts ist beachtlich, da nicht nur die bisher unterschiedlichen Anwendungen standardisiert, sondern auch alle Nummernsysteme (Auftrag-, Artikel-, Materialnummern usw.) vereinheitlicht werden müssen.

Die Vorteile für den Konzern liegen auf der Hand. Wartung und vor allem Releasewechsel lassen sich einheitlich organisieren, aber dies dürfte nicht das Hauptmotiv sein. Einzelne Unternehmen des Konzernverbunds lassen sich wesentlich leichter filetieren und fusionieren. Im Klartext bedeutet dies, dass es nun keine großen Probleme macht, dem einen Betrieb im deutschen Großkummerfeld die Buchhaltung wegzunehmen und in Schottland anzusiedeln oder große Teile der Personalarbeit herauszulösen und in Rumänien zu „allozieren“. Shared Services nennt sich diese Strategie, der die Betriebsräte oft noch nicht einmal mit der ohnehin schon relativ stumpfen Waffe des Interessenausgleichs und Sozialplans begegnen können, weil die Mengengerüste klein und die Prozesse schleichend sind. Es bleibt den Betriebsräten meist nur noch, ihre „Haut“ so teuer zu verkaufen, wie möglich.

Die mit diesen internationalen Projekten verbundenen Konzentrationsprozesse bergen eine Reihe weiterer Risiken und Nebenwirkungen. Sie sind stets verbunden mit dem Verlust lokaler Autonomie. Die Umsetzungen der Konzepte sehen oft so aus, dass es den Einkäufern vor Ort nicht mehr möglich ist, sich an bewährte lokale Lieferanten zu wenden, denn im System ist durch einen zentralen Katalog längst festgelegt, dass nur noch an einer Stelle eingekauft werden kann, für die sich eine fremde Zentrale entschieden hat, wobei die behaupteten Preisvorteile durch den gebündelten Einkauf oft nur behauptete Vorteile sind, auf jeden Fall aber mit Zeitverlust bezahlt werden müssen. Damit sind wir beim zweiten nachhaltigen Nachteil der neuen Globalisierungsstrategie, dem Verlust von Flexibilität. Das weltweit mit Workflows durchzogene System beschneidet nicht nur die lokalen Wahlfreiheiten, es lässt auch nur noch die zentral festgelegten Bearbeitungsweisen zu. Wollte man einmal davon abweichen, was die langsam und lang gewordenen

Genehmigungswege schon so gut wie verhindern, so muss erst das System umgebaut werden, doch davor steht die Wacht der Standardisierer. Die betroffenen Unternehmen verlieren ihre Anpassungsfähigkeit an veränderte Umweltbedingungen, und ihre Lernwege werden lang. Wenn es stimmt, dass der Untergang des real existiert habenden Sozialismus nichts oder nur wenig mit der Thematik Sozialismus – Kapitalismus zu tun hatte, sondern auf einen Mangel an Lern- und Anpassungsfähigkeit zurückgeht, dann ist die Zukunft vor allem der multinationalen Konzerne alles andere als rosig. Dies gilt umso mehr, wenn man bedenkt, dass Märkte immer auch lokal sind und mit jedem Filetieren und Fusionieren von Unternehmen ein Stück Identifizierung der Beschäftigten mit dem Unternehmen verloren geht, was bekanntlich nicht zu einer Steigerung der Produktivität führt.

2. Die datenschutzrechtliche Kehrseite

Die Thematik hat aber auch eine datenschutzrechtliche Seite. Unternehmen und Konzernzentrale sind in Bezug auf den Betrieb Dritte im Sinne des Datenschutzgesetzes. Dies ist zu beachten, wenn es um personenbezogene Arbeitnehmerdaten geht. Dieser Personenbezug besteht nicht nur bei den personalwirtschaftlichen Systemen im engeren Sinn, sondern zieht sich durch viele logistische, produktionsnahe und die computertechnische Infrastruktur betreffende Systemteile durch.

Rechtlich wird die aus dem Betrieb herausgelagerte Datenverarbeitung als Auftragsdatenverarbeitung organisiert, ein nach § 11 Bundesdatenschutzgesetz (BDSG) auch für die Verarbeitung personenbezogener Daten zulässiges Verfahren. Dort heißt es, dass der Auftragnehmer die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen darf (§ 11 Abs. 3 BDSG). Auftraggeber ist der vom Konzern abhängige Betrieb, Auftragnehmer ist die mächtige Konzernzentrale. Es ist offenkundig, dass die realen Machtverhältnisse genau umgekehrt liegen.

Vielfach sind die Vertragsverhältnisse aber noch tiefer verschachtelt. Ein Betrieb in Deutschland erhält Order von der deutschen Konzern-Holding, die wiederum mit der internationalen Zentrale in einem Vertragsverhältnis steht, welche oft mehrere weitere Dritte mit der Verarbeitung beauftragt. Oft benötigen die Betriebsräte Monate, bis der Weg des Auftragsverhältnisses nachgezeichnet ist. Jedenfalls können die Betriebsräte darauf bestehen, dass die Vertragskette lückenlos nachgewiesen wird. Denn das Gesetz sagt, dass der Auftrag schriftlich zu erteilen ist, wobei die Datenerhebung, Verarbeitung oder Nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Außerdem ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen (§ 11 Abs. 2 BDSG).

Erschwert wird das Verfahren weiter, wenn die Zentrale in einem Land ohne Datenschutzgesetz angesiedelt ist, z. B. in den USA.

Datenverarbeitung in den EU-Staaten

Die Richtlinie 95/46/EG (Datenschutzrichtlinie) verbietet den Unternehmen grundsätzlich, personenbezogene Daten aus Mitgliedsstaaten der Europäischen Union (EU) in Staaten zu übertragen, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auf die USA zu, da es dort keine umfassenden gesetzlichen Regelungen gibt, die den Standards der EU entsprechen.

Datenverarbeitung in den USA

Um aus dieser Zwickmühle herauszukommen, wurde zwischen 1998 und 2000 das sog. Safe-Harbor-Verfahren entwickelt. US-Unternehmen können diesem Vertrag beitreten und sich in einer Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die Safe Harbor Principles und die dazugehörenden – verbindlichen „Frequently Asked Questions“ (FAQ) zu beachten. Im Jahr 2000 hat die EU anerkannt, dass bei den Unternehmen, die dem Safe-Harbor-System beigetreten sind, ein ausreichender Schutz besteht. Die Betriebsräte sollten sich die entsprechenden Verträge vorlegen lassen und bei den notorisch erforderlichen Übersetzungen in die deutsche Sprache auch auf die Korrektheit der Übersetzung achten.

Wenn Unternehmen sich vorbehalten, die nach dem Safe-Harbor-Abkommen getroffenen Datenschutzregelungen zu ergänzen, abzuändern oder nicht länger anzuwenden, so sollte der Betriebsrat für den Fall der Änderung oder Aufhebung sich im Gegenzug ein außerordentliches, nicht befristetes Kündigungsrecht der entsprechenden Betriebsvereinbarung(en) – mit Ausschluss der Nachwirkung – einräumen lassen.

Vertrackte Situationen entstehen, wenn die in den USA angesiedelte Zentrale weitere Verträge mit Einrichtungen in anderen Ländern ohne Datenschutzrecht macht, z. B. Indien oder China. Die Unternehmen haben in solchen Fällen kaum mehr anzubieten, als vertraglich die entsprechenden Einrichtungen zu verpflichten, Regelungen einzuhalten, die als dem Safe-Harbor-Verfahren gleichwertig dargestellt werden. Ratlosigkeit kehrt regelmäßig ein, wenn dann die Betriebsräte die Frage stellen, wie denn die Einhaltung solcher Regelungen überprüft werden könne.

Über die Auftragsdatenverarbeitung hinaus gibt es noch eine Steigerung des Problems, und die heißt Funktionsübertragung. Während das traditionelle Shared-Service-Center nur Verarbeitungsaufgaben übernimmt, beispielsweise die Bearbeitung der Reisekosten oder das Ausstellen von Bescheinigungen, sieht die nächste Stufe die Auslagerung der Personalfunktionen vor. Natürlich haben wir es hier mit einer Betriebsänderung zu tun, wenn z. B. eine in Indien gegründete Tochterfirma eines multinationalen Konzerns jetzt direkte Aufgaben der ehemaligen Personalabteilung übernimmt.

Der „Tanker hat Kurs auf den Eisberg“ genommen, so sehen viele Betriebsräte die Situation und trösten sich mit der Hoffnung, dass sie in irgendeiner Form den wohl nicht mehr vermeidbaren Kollisionsschaden überstehen.

XI. Und was ist zu tun?

Nach den vielen Ausführungen zum schier nicht enden wollenden Thema Überwachung und Arbeitnehmer-Datenschutz stellt sich für Betriebs- und Personalräte nun die Frage, was zu tun ist.

An vielen Stellen ist deutlich geworden, dass der Abschluss einer Betriebsvereinbarung (oder Dienstvereinbarung) die angemessene Reaktion darstellt. Doch wie kommt man dahin?

Zunächst gilt es, überhaupt das Problem zu erkennen. Die entscheidende Frage lautet hier: Wo liegen die Gefahren für die Persönlichkeitsrechte der Beschäftigten? Hat man dies geklärt, so stellt sich gleich die nächste Frage, nämlich die nach dem betriebsverfassungsrechtlichen (oder personalvertretungsrechtlichen) Regelungsbedarf.

Oft verfügt die Arbeitnehmer-Interessenvertretung in eigenen Reihen nicht über den erforderlichen Sachverstand. Doch dagegen lässt sich etwas tun.

1. Sachverständige

Beratung

Unterstützung finden Sie bei den Beratungsstellen des DGB, aber auch unabhängige Sachverständige helfen Ihnen weiter.

Der Arbeitgeber ist nach § 80 Abs. 2 BetrVG verpflichtet, den Betriebsrat „rechtzeitig und umfassend“ über den Systemeinsatz zu informieren. Das heißt, er muss zu allen relevanten Fragen Antworten liefern, zum Beispiel: Welche Daten werden verarbeitet und zu welchem Zweck? Wie sehen die Speicherfristen aus? Welche Auswertungen sollen erzeugt werden? Wer soll Zugang zu den Auswertungen erhalten? Wie sieht das Berechtigungskonzept aus? Wie wird qualifiziert? Welche Schnittstellen gibt es zu vor- und nachgelagerten Systemen? Welche Auswirkungen hat die Systemeinführung auf die Tätigkeiten der Mitarbeiter? Und ... und ... und ...

Die kurze Frageliste ist bei weitem nicht abschließend und hängt nachvollziehbarerweise vom jeweils eingesetzten System ab.

An zweiter Stelle ist entscheidend, ob sich der Betriebsrat aufgrund der ihm verfügbaren Informationen ein Bild über das System und die dafür notwendige Regelung machen kann.

Wenn das nicht der Fall ist, dann muss er vor Einschaltung eines externen Sachverständigen andere Informationsmittel wählen: In Frage kommt z. B. das Studium von Fachliteratur und insbesondere die Inanspruchnahme des innerbetrieblichen Sachverstandes.

Wenn nach diesen Schritten weiterhin die entscheidenden Fragen nicht zufriedenstellend beantwortet worden sind, kann der Betriebsrat nach § 80 Abs. 3 BetrVG die Bestellung eines externen technischen Sachverständigen verlangen.

Beschluss des Betriebsrats

Der Betriebsrat muss dazu einen entsprechenden Beschluss fassen. Dieser umfasst das Thema, die Person des Sachverständigen, die Kosten seiner Inanspruchnahme und den Zeitpunkt.

Wenn Sie mit dem Gedanken spielen, Sachverständige einzusetzen, rufen Sie diese vorher an. Erst nach einem Gespräch mit ihnen lässt sich der Zeitrahmen für die Beratungen einigermaßen realistisch einschätzen.

Bevor der Sachverständige allerdings für den Betriebsrat tätig werden kann, bedarf es hierüber einer „näheren Vereinbarung“ mit dem Arbeitgeber. Stimmt der Arbeitgeber dem Einsatz zu, trägt er die Kosten der Inanspruchnahme. Stimmt er nicht zu, kann der Betriebsrat die Zustimmung durch einen Arbeitsgerichtsbeschluss ersetzen lassen. Dies allerdings ist ein Verfahren, das sich durch die Instanzen der Arbeitsgerichtsbarkeit hinziehen kann.

2. Einigungsstelle

Erfolg versprechender ist hier ein anderer Weg. Beharrt der Arbeitgeber auf seiner Weigerung, dem Betriebsrat einen Sachverständigen zu genehmigen, so kann der Betriebsrat die Verhandlungen für gescheitert erklären und die Einigungsstelle anrufen. Dazu muss er einen entsprechenden Beschluss fassen. Er sollte sich bei diesem Verfahren der Unterstützung durch den gewerkschaftlichen Rechtsschutz oder einen Rechtsanwalt seiner Wahl sicher sein.

Der Beschluss zur Einrichtung einer Einigungsstelle umfasst

- die Erklärung des Scheiterns der Verhandlungen,
- die Benennung des Themas (in der Regel die Bezeichnung des Systems, zu dessen Einführung und Anwendung man eine Betriebsvereinbarung abschließen will),
- die Benennung einer Person, die der Einigungsstelle vorsitzen soll (in der Regel ein Arbeitsrichter) und

- die Angabe über die Zahl der gewünschten Beisitzer. Auf diesem Weg kann sich der Betriebsrat dann als externen Beisitzer den Sachverstand beschaffen, der zuvor vom Arbeitgeber abgelehnt worden ist.

Kann sich der Betriebsrat mit dem Arbeitgeber nicht einigen, so muss er den Antrag auf Einrichtung der Einigungsstelle beim zuständigen Arbeitsgericht stellen. Die Einrichtung einer Einigungsstelle erfolgt in der Regel sehr schnell. Das Arbeitsgericht kann den Antrag nur dann ablehnen, wenn offensichtlich kein Mitbestimmungsrecht besteht; ansonsten ist die Einigungsstelle gehalten, selber ihre Zuständigkeit zu prüfen.

Gegen die Entscheidung des Arbeitsgerichts ist nur die Beschwerde zum Landesarbeitsgericht möglich, und dieses entscheidet erfahrungsgemäß auch innerhalb weniger Wochen. Fassen wir die einzelnen Stationen zusammen:

- Beschluss des Betriebsrats über das Scheitern der Verhandlungen und Anrufen der Einigungsstelle.

- Mitteilung des Beschlusses an den Arbeitgeber mit gleichzeitigem Vorschlag für das Thema der Einigungsstelle, der Person des Vorsitzenden und der Zahl der Beisitzer unter Angabe einer Frist für die Zustimmung.

- Kommt eine Einigung mit dem Arbeitgeber nicht zu Stande, Antrag auf Einrichtung der Einigungsstelle beim zuständigen Arbeitsgericht, wiederum mit Angaben zum Thema, zur Person des Vorsitzenden und zur Zahl der Beisitzer. Dabei sollten der Gegenstand des Verfahrens und der bisherige Verhandlungsablauf dargestellt werden.

- Als Beisitzer können sowohl betriebsinterne als auch betriebsexterne Personen benannt werden. Die Auswahl der Beisitzer entscheidet jede der beiden Parteien für sich. Außerdem kann der Betriebsrat einen Verfahrensbevollmächtigten hinzuziehen.

- Die Kosten der Einigungsstelle hat der Arbeitgeber zu tragen. Diese umfassen den Geschäftsaufwand des Verfahrens, die Vergütung des Vorsitzenden sowie der externen Beisitzer.

3. Ausblick

Software wird immer komplexer. Mittlerweile handelt es sich nicht mehr nur um Unterstützung beim Ausfüllen simpler Formulare, sondern in zunehmendem Maße werden Systeme eingesetzt, um Entscheidungen zu begleiten oder Entscheidungen gar selbst nach einprogrammierten Vorgaben vorzunehmen (IDS, Zugangskontrolle, Videoüberwachung).

Für die meisten Betriebsräte ist dabei unmittelbar ersichtlich, dass eine Betriebsvereinbarung zum Beispiel zur Kameraüberwachung nicht nur den Umgang mit den aufgezeichneten Video-Daten regeln muss, sondern auch den konzeptionellen Rahmen umfassen muss: Ist der Einsatzzweck gerechtfertigt und verhältnismäßig? Wo dürfen Kameras stehen? Welche Leistungsmerkmale dürfen genutzt werden?

Genauso verhält es sich bei nahezu allen neuen Anwendungen. Bei der Suche nach sinnvollen Lösungen ist stets zu beachten, dass Regelungen schon an den grundlegenden Konzepten ansetzen und diese hinterfragt werden sollten. Sie sollten nicht nur die technische Umsetzung von bereits fixierten Konzepten umfassen. Wirksamer Persönlichkeitsschutz kann viel besser erreicht werden, wenn bereits der Rahmen des Softwareeinsatzes von vornherein einen Missbrauch unattraktiv macht.

Das Infragestellen von Konzepten ist umso wichtiger, weil viele Systeme nicht per se die Persönlichkeitsrechte der Mitarbeiter bedrohen. Es kommt vielmehr auf die jeweilige Konfiguration an. So kann ein System in dem einen Unternehmen eine wertvolle – auch aus Betriebsratssicht nachvollziehbare – Hilfe im Arbeitsalltag darstellen, bei der die Kontrollmöglichkeiten auf ein erträgliches Maß heruntergepegelt worden sind. Das gleiche System könnte, anders konfiguriert, in einem anderen Unternehmen zu einem Überwachungsinstrument pervertieren.

Vernetzte Anwendungen, vor allem Webanwendungen mit Personendaten, sind auf der ganzen Welt über das Internet abrufbar. „Gefahr“ für den Persönlichkeitsschutz droht daher nicht mehr nur wie in den vergangenen Jahrzehnten durch unternehmensinterne Aktivitäten, sondern auch durch Datenmissbrauch bei eingeschalteten externen Dienstleistern und Anbietern sowie durch unbekannte Dritte (Hacker). Die Unternehmen unterschätzen meist die Gefahren. Die Betriebsräte haben deshalb das Recht und die Pflicht, auch diesen Aspekten in den Vereinbarungen Rechnung zu tragen.

Außerdem sind für die Zukunft noch schnellere Versionswechsel mit jeweils neuen Leistungsmerkmalen und schnelleren Systemeinführungen zu erwarten. Denn zunehmend werden in Unternehmen Anwendungen installiert, die nur noch auf einem Server installiert werden müssen, clientseitig wird – wartungsfrei – der unternehmensübliche Internet-Browser eingesetzt. „Software On Demand“ heißt ein Konzept, mit dem immer mehr Anbieter punkten. Dabei ist die Software gar nicht mehr im Unternehmen selbst installiert, sondern wird „gemietet“. SAP zum Beispiel plant sein, vor allem für den Mittelstand, vorgesehenes Zukunftsprodukt „Business By Design“ nach diesem Konzept. Bezahlt wird nur noch nach Aufwand. Die Anforderungen an den Betriebsrat steigen also weiter.

Stichwortverzeichnis

Bezeichnung	Seite
Anrufbeantworter	70, 76
Aufschalten	58, 63
Auftragsdatenverarbeitung	104, 105
Automatische Anrufverteilung	72
Betriebliche Übung	70
Betriebsdaten	99, 100, 102
Betriebssysteme	14, 41, 67
Biometrie	97
Blog	51, 53
Bundesdatenschutzgesetz	83, 104
Bundesverfassungsgericht	7, 8, 11, 12, 16, 38, 42, 70
Business Warehouse	32, 33, 34, 99
Chat	51, 55, 56, 58, 59, 64, 68
Chipkarten	87, 88, 89, 93, 94, 95, 96
Coaching	74
Computergrundrecht	9
Data cubes	33
Data Warehouse	32, 33, 34
Dialer	69, 76, 77
Echtzeit-Anzeigen	47, 72, 74
Einigungsstelle	17, 19, 20, 21, 23, 108, 109
Einzelverbindungen	71, 79
E-Mail	14, 28, 36, 37, 38, 42, 43, 44, 45, 47, 48, 49, 50, 52, 58, 59, 66, 78, 79, 84
Fernmeldegeheimnis	42, 49, 70, 71, 78
Fernsteuerung	55, 58, 62, 63, 64, 68
Firewall	37
Gesichtserkennung	14, 84, 86, 97, 98
Gesprächsdaten	70
Globalisierung	103
Hacker	37, 46, 58, 59, 110
Info cubes	33
Informationelle Selbstbestimmung	8, 9, 12, 42
Initiativrecht	23
Internet	10, 11, 14, 26, 36, 37, 38, 39, 41, 43, 44, 45, 46, 47, 50, 51, 53, 57, 59, 68, 77, 79, 80, 84, 97, 99, 110
Intranet	31, 37, 51, 52, 53
Inventarisierung	64, 65, 66, 67
Iriserkennung	97
Kalender	12, 52, 53
Kamera	14, 17, 55, 56, 83, 84, 85, 97, 98, 110
Lizenzkontrolle	64, 65
Login	14, 31, 68, 87, 94, 95
Meilensteinverfahren	101
Mikrofon	55, 56
Missbrauchsregelung	40, 45
Mitarbeiterausweise	88, 96
Mobiltelefon	12, 78, 79, 80, 84
Mobiltelefonie	78
Netzwerksicherheit	41, 47, 57
Outsourcing	85
Pausendauer	91
Performance-Management	27
Personaldaten	19, 20, 25, 27, 31, 32, 33, 34, 99
Personalsystem	13, 21, 31, 32, 34
Persönliche Speicherbereiche	62
Positivkatalog	20
Power-Dialer	76
Private Nutzung	36, 37, 38, 43, 44, 70
Produktionsplanung	99, 100

Bezeichnung	Seite
Produktionssteuerung	99, 100, 101, 102
Protokolldaten	39, 40, 41, 44, 45, 52, 60, 66, 93
Provider	13, 30, 37, 38, 78, 79
Remote Control	62, 66, 68
Reporting	28, 32, 33, 46, 74, 76
Risikobewusstsein	61
Sachverständige	19, 107, 108
Safe-Harbor-Abkommen	105
SAP	13, 21, 26, 27, 28, 32, 33, 34, 103, 110
Self Service	27, 28, 30, 31
Shared Service	29, 103
Sicherheitsprogramme	37
Skill-Management	27
Social networking	14
Softwareverteilung	58, 66
Spamfilter	37, 48
Telekommunikationsanlage	69
Terminkalender	12, 53
Trouble-Ticket-System	102
Unlizensierte Software	66
User generated content	51
Verdachtsmomente	41
Verhältnismäßigkeitsgrundsatz	15, 16
Vertrauensperson	43
Vertreterregelung	43
Videoüberwachung	83, 84, 93, 109
Vier-Augen-Prinzip	62
Virenmuster	48
Vorratsspeicherung	38
Web 2.0	14, 51
Webcam	55
Webfilter	37, 39, 46
Webkonferenz	55, 56
Weblog	53
Wiki	51, 53, 54, 55
Windows	62, 67, 68
Workflow	27, 28, 30, 31, 103
Zeiterfassung	65, 87, 89, 90, 91, 93, 96
Zeitmanagement	13, 26, 27
Zentralisierung	103
Zutrittskontrolle	87, 92