KNUT HÜNEKE, BERND ZIMMERMANN

Gesucht: eine neue Datenschutzkultur

Es wurde schon angedeutet: Vielleicht kommt es ja gar nicht darauf an, jedes Detail jeder Vorschrift mit Macht und Mühe in die Realität umzusetzen. Wer Datenschutz als bürokratisches Zwangssystem organisiert, erweist ihm möglicherweise einen Bärendienst ...

In zunehmend vernetzten Systemen wird es immer schwieriger Datenschutz zu gewährleisten (CF 10/98 ab Seite 16 und CF 2/99 ab Seite 24). Die einzelnen Systeme werden ständig komplexer und die Grenzen zwischen den Systemen immer verschwommener.

Um solche Systeme – oder besser: System-›Landschaften‹ – datenschutzmäßig ›dicht‹ zu machen, brauchte es wahre Multitalente bei allen Beteiligten. Man nehme einfach mal die Anlage zu § 9 BDSG (die ›10 Gebote des Datenschutzes‹ – siehe Seite 11) und überlege, was in der Umsetzung dieser Vorgaben technisch und organisatorisch alles aufeinander abgestimmt werden müsste, um ein stimmiges sicheres System oder gar eine ebensolche ›System-Landschaft‹ zu erhalten ...

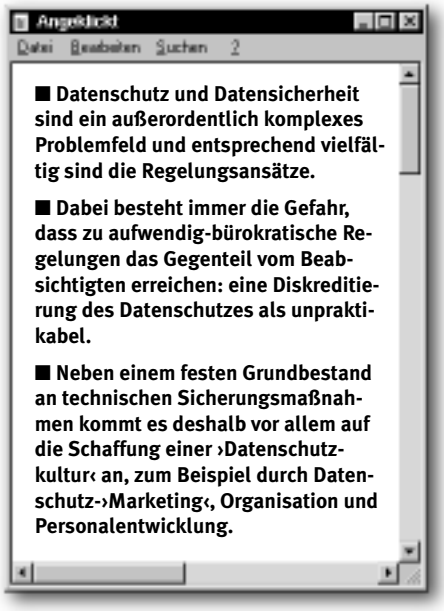
Die Vielfältigkeit dieser Anforderungen wollen wir beispielhaft am Thema Netzsicherheit verdeutlichen, denn die Sicherheit von Netzen ist Grundvoraussetzung des Datenschutzes für jede Software, die auf solchen Netzen läuft. So wie überhaupt die Datensicherheit die Voraussetzung für jeden wirksamen Datenschutz darstellt. Unter Datensicherheit (Datensicherung) werden nämlich alle die Maßnahmen verstanden, die den Schutz von Daten und Datenträgern vor Verlust, Beschädigung, Missbrauch und so weiter gewährleisten sollen. Datenschutz dagegen bezieht sich nur auf den Schutz *personenbezogener* Daten vor Missbrauch. Datensicherheit ist damit eine – wenn auch allein nicht hinreichende – Möglichkeit, den Datenschutz zu gewährleisten.

Beispiel Netzsicherheit

Die Sicherheit eines Computer-Netzwerks entsteht im Zusammenwirken unterschiedlichster Komponenten, sowohl bei der Hardware (den Geräten), wie bei der Software (den Programmen). Im Wesentlichen sind dies: Berechtigungssystem, Datenhaltung, Zugangskontrolle, Verschlüsselung, Verkabelungsart, Vermittlungstechnik, Übertragungsprotokolle, Netzaufbau/Netztechnik und das oder die verwendeten Betriebssysteme.

Bei einer Anbindung an das Internet kämen noch weitere Komponenten hinzu wie zum Beispiel die ›Firewall‹ (siehe CF 4/99 ab Seite 16).

Man kann sich nun ein solches Netzwerk wie aus Schichten aufgebaut vorstellen (= OSI-Referenzmodell – siehe Übersicht auf Seite 10). Die oberste Schicht ist die ›Anwendungsschicht‹. Hier finden sich die, sagen wir, Arbeitsergebnisse aus beliebigen ›Anwendungsprogrammen‹ wie zum Beispiel Textnachrichten, Bilder oder Datenbankauswertungen. Die nächste Schicht ist die ›Darstellungsschicht‹, in der sich die über das Netzwerk zu verbindenden Systeme auf eine gemeinsame ›Sprache‹ einigen, also die Voraussetzungen für einen funktionierenden Datenaustausch schaffen. Die Ebene darunter ist dann die ›Kommunikationsschicht‹, die alle Informationen (Absender- und Empfängeradressen usw.) enthält, die gebraucht werden, um eine Netzverbindung zwischen zwei Systemen herzustellen. Und so geht es dann durch verschiedene Schichten weiter bis zu untersten, wo sich alle die vielen Nullen und Einsen befinden, aus denen letztlich jede in einem Computer verarbeitete Information besteht.



Firewall = ›Brandschutzmauer‹ = System, das (Unternehmens-)Netzwerke vor unbefugten Zugriffen aus dem Internet schützen soll und das deshalb auch den gesamten Datenverkehr zwischen Innen und Außen kontrolliert.

Stellt man sich die Datenübertragung in Netzen so ›geschichtet‹ vor, wird auch klar, dass und wie Sicherheitsmaßnahmen hierarchisch greifen – denn: Findet eine Verschlüsselung nur auf der obersten Ebe-

info

Übersicht:

Die ›Sicherheitsschichten‹ (OSI-Referenzmodell)

Schicht	*Bereich*	*Name*
7	Arbeitsergebnisse aus beliebigen Anwendungsprogrammen (wie z.B. Textverarbeitung)	Anwendungsschicht
6	Festlegung, auf Grund welcher z.B. technischen Standards zwei Systeme Kontakt aufnehmen	Darstellungsschicht
5	Alle Informationen, die zum Aufbau einer Verbindung benötigt werden (z.B. Adressen)	Kommunikationsschicht
4	Aufbau und Struktur des Netzes über das die Datenübertragung läuft	Transportschicht
3	Auswahl des konkreten Übertragungsweges (von wo über welche Zwischen-Rechner wohin)	Netzwerkschicht
2	Sicherung gegen Übertragungsfehler	Sicherungsschicht
1	Die Übertragung der Bits und Bytes, also der nicht mehr weiter zu ›übersetzenden‹ Information	Physikalische Schicht

ne statt, ist auch nur diese geschützt. Wird eine dort verschlüsselte Datei über das Netz versandt, kann diese Datei zwar nicht ohne Weiteres ›gelesen‹ werden, aber weil alle Informationen aus den darunter liegenden Schichten frei vorliegen, ist man nicht davor gefeit, dass die verschlüsselten Datenpakete den falschen Empfänger im falschen System im falschen Netz erreichen (und dort müssten sie nur noch in aller Ruhe geknackt/entschlüsselt werden).

Je tiefer die Schicht, desto sicherer

Hinzu kommt, dass auch die Verbindungsinformationen (Netzadressen, Benutzerkennung, Passwörter usw.) abgefangen werden können, die sich dann auf unterschiedlichen Wegen dazu benutzen ließen, unberechtigt in ein Netz einzuschleichen.

Je ›tiefer‹ also die Schicht liegt, auf der eine Nachricht verschlüsselt wird, desto schwerer werden solche ›Angriffe‹. Außerdem sind die Kombinationsmöglichkeiten von Sicherheitsmaßnahmen um so größer, je mehr ›Schichten‹ einbezogen werden können…[1] !

Weiter kompliziert wird die ganze Sache noch durch die verschiedenen Arten personenbezogener Daten, die in einem Netzwerk anfallen können:

Da gibt es *Netz-Stammdaten* (also Daten, die von allen Benutzern des Netzwerks erfasst sind, wie z.B. Benutzernamen, Berechtigungen, Passwörter), es gibt *Verbindungsdaten* (die jedesmal anfallen, wenn über das Netz Verbindung irgendwohin aufgenommen wird, wie z.B. Adressdaten oder Anmelde-Informationen zu Abrechnungszwecken) und es gibt *Inhaltsdaten* (Daten von Arbeitnehmern oder Kunden, deren Verarbeitung der eigentliche Zweck eines Netzwerks ist, wie z.B. Bestellungen, Arbeitszeiten, Leistungsdaten oder Daten zur Materialentnahme). Diese Vielzahl unterschiedlicher Daten gilt es zu schützen, und zwar sowohl vor der unberechtigten Nutzung durch Personen, die ansonsten durchaus berechtigt sind, im Netzwerk zu arbeiten, und vor einer gänzlich unberechtigten Nutzung von Netzwerk und Daten (z.B. Hacker-›Angriff‹ von außen).

Dieses ›kurze‹ Beispiel für die Komplexität der Datenschutz-/Datensicherheitsproblematik ließe sich beliebig weiter ausbauen:

Haben Sie beispielsweise schon einmal darüber nachgedacht, was es unter Datenschutzgesichtspunkten bedeutet, wenn unter besonderen Bedingungen Ausschnitte aus Tabellen (z.B. die Leistungsübersicht der Montagegruppe X aus der Übersicht für alle Montagegruppen) in eine Textverarbeitung übertragen werden…[2]? Oder haben Sie schon einmal die Effekte der Schnellspeicherung in MS-Office-Dokumenten betrachtet, ehe Sie diese in irgendeiner Form (z.B. durch elektronische Post) der Öffentlichkeit zugänglich gemacht haben…[3]? Oder wie steht es mit den Ein-

1… Zur Vertiefung der Materie empfehlen wir die hervorragend einführende Broschüre ›Datenschutz in Netzen‹ aus der Reihe der Hamburger Datenschutzhefte, herausgegeben vom Hamburger Datenschutzbeauftragten; dort kostenlos zu bestellen (Baumwall 7, 20459 Hamburg oder im Internet herunterzuladen unter http://www.hamburg.de/Behoerden/HmbDSB/Material/netze.htm)

2… Wird dieses ›Embedding‹ (= Einbetten) mit einer aktiven Dateiverknüpfung vorgenommen und hat der Empfänger prinzipiell Zugriff zum Ablageort der verknüpften Datei (die er sonst eventuell gar nicht öffnen kann), so kann durch einen Doppelklick zum Bearbeiten des Tabellenausschnitts die gesamte Datei eingesehen werden, aus der der Ausschnitt stammt.

3… Dann ist es nämlich möglich mit einem Text-Editor einzusehen, was alles mal geschrieben, dann aber wieder gelöscht wurde. Das kann z.B. dann sehr spannend werden, wenn der Beschwerdebrief nach einer überschlafenen Nacht entschärft und von mehr oder weniger beleidigenden Äußerungen ›gereinigt‹ wurde.

schränkung der ›Download‹-Funktionen in SAP…[4]? Ein Feld ohne Ende …

Das Bürokratie-Problem

Die hier nur angedeutete Vielzahl technischer Sicherungsprobleme und -maßnahmen führt oder würde irgendwann dazu führen, dass bürokratische Hürden entstehen, die dem eigentlichen Sinn all dieser Schutz- und Sicherungsmaßnahmen zuwider laufen. Denn wenn Regelungen unpraktikabel sind, werden sie missachtet. Und wenn dann auch noch – was schnell geschehen kann – die Funktionsfähigkeit einzelner Programme eingeschränkt wird, kollidiert Datenschutz sogar mit Anforderungen aus dem Bereich der Software-Ergonomie (der menschen- und funktionsgerechten Gestaltung von Computer-Programmen). Die Folge ist oder wäre eine eigentlich von niemandem gewollte Diskreditierung des Datenschutzes an sich.

Technischer Datenschutz aber läuft ohne entsprechendes Bewusstsein ins Leere. Die Statistiken über Datenmissbrauch weisen die Mehrzahl der Verstöße (über 80 Prozent) in den Kategorien ›Irrtum‹ und ›Unwissenheit‹ aus – also Verstöße durch Personen, die auf Grund ihrer Tätigkeiten zwar einen berechtigten Zugriff auf schutzwürdige Personendaten haben, diese Möglichkeit aber unwissentlich, ohne Unrechtsbewusstsein oder auch als Befehlsempfänger vermeintlich von Verantwortung befreit, missbrauchen. Welcher Beschäftigte weigert sich schon, wenn ein Vorgesetzter eine datenschutzrechtlich bedenkliche oder gegen eine Betriebsvereinbarung verstoßende Auswertung von Arbeitnehmerdaten verlangt (wenn er das Ganze überhaupt als eine bedenkliche Auswertung begreift)? Jedenfalls: Nur ein sehr geringer Teil von Datenschutzverstößen ist auf kriminelle Energie zurückzuführen.

Da liegt die Vorstellung nahe, dass eine Sensibilisierung der Beschäftigten für den Datenschutz wesentlich stärker in den Vordergrund gerückt werden sollte. Deshalb möchten wir den Blick einmal (stärker) auf das letzte der berühmten ›10 Gebote des Datenschutzes‹ lenken. Dort heißt es (und in allen Landesdatenschutzgesetzen sieht es ähnlich aus):

»Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind, […] die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).«

Entgegen der landläufigen Praxis ist dabei mit der *Organisationskontrolle* nicht nur gemeint, die Organisation (z. B. das Unternehmen) und die Mitglieder der Organisation zu kontrollieren, sondern es wird der klare Auftrag zum *Aufbau*, zur *Gestaltung* einer den Datenschutz unterstützenden Organisation…[5] gegeben. Und genau hier liegt auch eine Möglichkeit für den zukünftigen Ausbau des betrieblichen Datenschutzes:

info

Anlage zu § 9 Bundesdatenschutzgesetz

Die zehn Gebote des Datenschutzes

Maßnahme	*Inhalt*	*Beispiel*
Zugangskontrolle	**Nur Berechtigte dürfen an die EDV-Anlage heran.**	**Zugangskontrollsystem, Schlüssel, ›Closed Shop‹-Betrieb**
Datenträger-kontrolle	**Nur Berechtigte dürfen einen Datenträger benutzen.**	**Datenträger werden in einem gesicherten Raum aufbewahrt.**
Speicherkontrolle	**Nur Berechtigte dürfen auf Daten im Hauptspeicher zugreifen.**	**Hauptspeicher-Ausdruck (›Dump‹) istnur für den Systemadministrator erlaubt.**
Benutzerkontrolle	**Nur Berechtigte dürfen die EDV nutzen.**	**Einrichtung von Benutzeridentifizierung und -authentisierung**
Zugriffskontrolle	**Nur Berechtigte dürfen auf Informationen zugreifen.**	**Einrichtung von Dateiberechtigungen und Benutzerrechten**
Übermittlungs-kontrolle	**Es wird kontroliert, an wen Personendaten gehen.**	**Protokollierung der Datenübermittlung**
Eingabekontrolle	**Es wird kontrolliert, wer welche Daten eingibt.**	**Protokollierung, wer welche Daten zu welchem Zeitpunkt eingibt.**
Auftragskontrolle	**Datenverarbeitung im Auftrag nur nach Weisungen**	**Sorgfältige Auswahl, eindeutige Vertragsgestaltung**
Transportkontrolle	**Nur Berechtigte dürfen Informationen transportieren.**	**Datenträger werden nur von Berechtigten transportiert (diese müssen auf das Datengeheimnis verpflichtet werden!)**
Organisations-kontrolle	**Organisation muss auf Datenschutz ausgerichtet sein.**	**Funktionstrennung, Arbeitsanweisungen, vier-Augen-Prinzip, Katastrophenplan**

Quelle: Jochen Konrad-Klein

4… Mühsam verständigt sich der Betriebs-/ Personalrat darauf, dass zwar die Jahres-/ Monats-Hitliste der Abwesenheiten als unerlaubte Auswertung verboten ist, kann sich aber dem Argument nicht entziehen, dass die tagtägliche Abwesenheit einsehbar sein muß. Und ganz fiese Menschen – die es in der Wirklichkeit natürlich nicht gibt – laden sich die Tageslisten dann in PC-Tabellenprogramme herunter und erstellen dort ungestört und unprotokolliert ihre Hitliste.

5… Man muss dem Datenschutzgesetz und insbesondere der Anlage zu § 9 BDSG die technische ›Schieflage‹ (neun von zehn Punkten sind eher technisch orientiert) entschuldigen. Es wurde in Zeiten erstellt, als noch niemand etwas von PC-Netzwerken, ›Client-Server‹-Umgebungen oder gar Internet ahnte.

Wir wollen nämlich dafür plädieren, dass sich der Betriebs- oder Personalrat dafür einsetzt, eine dem Datenschutz förderliche betriebliche ›Kultur‹ zu schaffen. Dies kann er tun, indem er immer dann, wenn es bei Verhandlungen mit dem Arbeitgeber um Datenschutzfragen geht, anbietet, für jeden wirksamen organisatorischen und/oder im Sinne einer ›Datenschutzkultur‹ wirkenden Schritt eine (möglicherweise) teure, aufwendige, bürokratische und arbeitsbehindernde technische Datenschutzmaßnahme zurück zu schrauben.

Nur um Irrtümern vorzubeugen: Eine *Grundsicherung* an technischen und organisatorischen Maßnahmen muss bleiben, daran führt kein Weg vorbei. Technische Sicherungssysteme, eng gefasste Berechtigungen, minimalste Datenerfassung und -auswertung…[6] und Zugriffsprotokollierung – das muss es auch bei ausgeprägter Datenschutzkultur in jedem Unternehmen geben.

Wir meinen aber (und haben die Erfahrung gemacht), dass die Unternehmenskultur im Umgang mit personenbezogenen Daten verändert werden kann und muss. Und die Kultur eines Unternehmens kann sehr wohl beeinflusst werden. Oder hat vor nur fünf Jahren schon jemand von Mobbing gesprochen und war nicht vor zehn Jahren noch jeder ›Grabscher‹ ein toller Hecht?

Wege zu einer neuen Datenschutzkultur

Eine Kulturänderung im Bereich Datenschutz (unter diesem Gesichtspunkt sollte auch das Gespräch mit einem Datenschutzbeauftragten ab Seite 30 besonders aufmerksam gelesen werden!) kann unseres Erachtens auf folgenden Gebieten vorangetrieben werden:

- Öffentlichkeitsarbeit;
- Umstrukturierung und Organisationsentwicklung;
- Personalentwicklung;
- Schaffung von materiellen und immateriellen Anreizen;
- Konkretisierung rechtlicher Vorgaben;
- Zertifizierung betrieblicher Schlüsselfunktionen (siehe dazu den Beitrag auf Seite 80);
- Aktivierung oder Neubestellung des betrieblichen Datenschutzbeauftragten (siehe den Beitrag ab Seite 68).

Öffentlichkeitsarbeit

Mit dem Datenschutz ist es wie mit der Datensicherung. Jahrelang passiert nichts, also wird das ›Ziehen‹ von Sicherungskopien (Backups) oder die automatische Zwischenspeicherung von Dokumenten großzügiger gehandhabt. Bis dann wieder einmal etwas passiert und dem Ganzen erneute Aufmerksamkeit geschenkt wird, bis dann …

Und genau hier liegt das Problem: Gibt es keine Auffälligkeiten, keinen Grund sich aufzuregen, dann wird auch kein Anlass gesehen, etwas zu hinterfragen und zu diskutieren – scheinbar gibt es ja nichts zu tun. Die Sensibilisierung für Datenschutzfragen darf aber nicht warten, bis ›etwas passiert‹ ist – denn *ein* Verstoß wäre bereits einer zu viel.

Öffentlichkeitsarbeit meint deshalb vor allem ein innerbetriebliches ›Marketing‹ für den Datenschutz. Was Datenschutz ist und welche Vorteile Datenschutzmaßnahmen bieten, hat im Mittelpunkt der Werbearbeit für den Datenschutz zu stehen. Wichtig ist dabei, dass immer wieder dieses deutlich wird: »Wir nehmen Datenschutz ernst! Wir wollen Datenschutz! Datenschutz auf allen Ebenen ist Teil unserer ›Unternehmenspolitik‹.«

Als einzelne Maßnahmen kommen in Betracht:

- Datenschutz wird regelmäßiger Tagesordnungspunkt auf Betriebs- und Abteilungsversammlungen (z. B. mit Berichten über Datenschutzprüfungen und durchgeführte Maßnahmen);
- Datenschutz wird regelmäßige Rubrik in der Betriebs-/Werkszeitung (z. B. mit ›Vorbildern‹, ›Missgeschicken‹ aus anderen Betrieben, Berichte über neu eingeführte Maßnahmen, Auszügen aus Fachzeitschriften);
- auf Betriebs- und Abteilungsversammlungen werden Vorträge und Referate gehalten (bevorzugt von Externen wie z. B. dem Landesbeauftragten für den Datenschutz, denn ›der Prophet gilt nichts im eigenen Land‹);
- Datenschutzgesetz(e) und die entsprechende Rechtsprechung sowie Datenschutz-Betriebsvereinbarungen werden selbstverständlicher Bestandteil betrieblicher Qualifizierungsmaßnahmen zum Thema EDV;
- Probleme und Unsicherheiten im Datenschutz werden offizieller und gewollter Bestandteil beispielsweise auf Abteilungsbesprechungen.

Umstrukturierung und Organisationsentwicklung

Hier kommt es vor allem darauf an, der im Sinne einer Stabsstelle definierten Position des betrieblichen Datenschutzbeauftragten eine Organisation beizustellen, die das Unternehmen durchdringt, dort mit Rat und Tat zur Seite steht, wo Probleme und Unsicherheiten entstehen, Handlungsanleitungen für die alltägliche Praxis vor Ort gewährleisten und für Fragen zur Verfügung stehen kann. Denkbar sind hier:

- Aufbau einer dem Datenschutzbeauftragten nachgeordneten dezentralen Struktur für den Datenschutz in sensiblen Bereichen (Personalabteilung; EDV-Abteilung; Zeitbeauftragte in den Bereichen Produktion und Projektarbeit und überall da, wo Leistungsrückmeldungen anfallen). Wir empfehlen, dass Referenten oder lokale Datenschutzexperten mit besonderer Qualifizierung, externe Vorträgen sowie regelmäßiger Austausch (›Workshops‹) unter Anleitung des betrieblichen Datenschutzbeauftragten eingerichtet werden;
- Aufbau eines Datenschutz-Qualitätszirkels (oder mehrerer davon);
- so weit vorhanden: Einbeziehung des Datenschutzes ins ›Total Quality Management‹ oder ISO 9000-Zertifizie-

6… Wir sprechen auch von ›Askesen‹: Datenaskese, Auswertungsaskese, Zugriffsaskese (Askese = Enthaltsamkeit).

rungen einschließlich regelmäßiger ›Datenschutz-Audits‹ mit externer Begutachtung;
- Festlegung von Einrichtungen und Personen als Verantwortliche für die Pflege von Dokumentationen und die Weiterentwicklung betrieblicher organisatorischer und technischer Datenschutzmaßnahmen;
- Aufnahme entsprechender Tätigkeiten in Stellenbeschreibungen und Qualifikationskataloge;
- bei Ausschreibungen von Stellen in datenschutzsensiblen Bereichen: offensive Darstellung der datenschutzrechtlichen Anforderungen und Hinzuziehung des betrieblichen Datenschutzbeauftragten bei der Entscheidung über eine Einstellung.

Personalentwicklung

Im Vordergrund stehen Bemühungen, den Personen, die Umgang mit personenbezogenen Daten haben oder haben werden und den Trägern des betrieblichen Datenschutzes Fach- und Anwendungswissen näherzubringen und einzuüben. Es geht also um:

- Etablierung des Datenschutzes als Bestandteil des betrieblichen Weiterbildungsprogramms;
- ›Trainee‹-Programme für Beschäftigte in der EDV- und der Personalabteilung mit Praktikum beim betrieblichen Datenschutzbeauftragten;
- Datenschutz muss (rechtlich, organisatorisch) Teil der Führungskräfte-Qualifikation werden;
- Aufnahme des betrieblichen Datenschutzbeauftragten in die Personalentwicklungs-Planung.

Materielle und immaterielle Anreize

Der Schaffung von materiellen und immateriellen Anreizen kommt eine ganz entscheidende Rolle zu, denn letztlich wird daran bewertet, welche Rolle der Datenschutz in der betrieblichen Realität wirklich einnimmt oder jedenfalls künftig einnehmen soll. Hier wäre zu überlegen:

- Ausdrückliche Aufnahme des Datenschutzes in das betriebliche Vorschlagswesen;
- Belobigung und/oder Prämien für Abteilungen oder Personen, die in definierten Zeiträumen ›sauber bleiben‹ und den betrieblichen Richtlinien entsprechend gehandelt haben (Verknüpfung mit Qualitätssicherung und Datenschutz-Audit);
- Aufnahme von datenschutzbedeutsamen Punkten in ›Mitarbeitergesprächen‹ und/oder Zielvereinbarungen auf allen Ebenen (einschließlich eines Anforderungskatalogs für Führungskräfte);
- ›Ahndung‹ von Verstößen mit Qualifizierungsmaßnahmen.

Konkretisierung rechtlicher Vorgaben

Hier geht es vor allem darum, betriebliche ›Pflichtübungen‹ zur Absicherung der Geschäftsleitungen gegenüber dem Gesetz (»Unterschreiben Sie hier doch bitte noch schnell, dass Sie vom Datenschutzgesetz Kenntnis erhalten haben!«) in eindeutige und klare Verpflichtungen zu wandeln. Hier sind geeignet:

- Besondere Verpflichtung von Systemverwaltern, Beschäftigten der Personalabteilung und so weiter auf Datenschutz und Verschwiegenheit (vergleichbar mit ärztlicher Schweigepflicht) mit möglichst feierlichem und verbindlichem Charakter (Unterschriftsleistung unter Urkunde, ›Gelöbnis‹);
- ›Vertraut machen mit dem Datenschutz‹ (Aufgabe des betrieblichen Datenschutzbeauftragten nach §37 Abs. 2 BDSG) einschließlich Ablegen einer Prüfung mit Zertifikat;
- Anwesenheit des betrieblichen Datenschutzbeauftragten bei Personalgesprächen (Einstellung, Versetzung);
- Erstellung eines Organisationshandbuchs ›Datenschutz‹.

Zertifizierung betrieblicher Schlüsselfunktionen

Damit soll insbesondere die Arbeit der System- und Netzwerkverwalter und der Beschäftigten in der Personalabteilung bezogen auf einen sensiblen Umgang mit personenbezogenen Daten professionalisiert werden. Grundvoraussetzung für einen effizienten Datenschutz ist nicht allein das Vorhandensein technischer Einrichtungen, sondern diese müssen auch entsprechend gewartet, eingestellt und durch ein entsprechendes Verhalten der Benutzer unterstützt werden. Was nützt beispielsweise das ausgefeilteste Berechtigungskonzept, wenn bei der Vergabe von Berechtigungen geschlampt wird? Deswegen sollen die betrieblich Verantwortlichen entsprechend qualifiziert und regelmäßig sensibilisiert werden. Nachweispflichten für eine entsprechende Zertifizierung könnten sein:

- Kenntnisse des Bundesdatenschutzgesetzes;
- Kenntnisse weiterer gesetzlicher Regelungen (je nach betrieblichen Besonderheiten);
- Kenntnisse der betrieblichen Regelungen zum Datenschutz und zur Leistungs- und Verhaltenskontrolle;
- Kenntnisse über die technischen Datenschutzmöglichkeiten des jeweiligen DV-Systems (Berechtigungskonzept, Protokolle, Verschlüsselungsmechanismen usw.) und ihr Zusammenwirken mit anderen technischen Maßnahmen.

Knut Hüneke und Bernd Zimmermann sind selbständige Organisationsberater und Gründer des NIM (Netzwerk Innovative Mitbestimmung), eMail: **info@nim-online.de**; Internet: **www.nim-online.de**;
Kontaktadressen: Knut Hüneke, Netzwerk Innovative Mitbestimmung, Büro München, Angerweg 6 a, 82140 Olching-Esting, eMail: **k.hueneke@link-m.de**; Bernd Zimmermann, Netzwerk Innovative Mitbestimmung, Büro Gelsenkirchen, Teichstraße 15, 45897 Gelsenkirchen; eMail: **zimmermann.b@cityweb.de**