DuD
Datenschutz und Datensicherheit

Betriebsvereinbarung E-Mail und Internet

Ein kommentierter Entwurf für die Praxis

Rainer W. Gerling

In viele Firmen halten E-Mail und Internet-Zugänge Einzug. Der Umgang mit diesem neuen Medium ist für Geschäftsleitungen und Beschäftigte gleichermaßen ungewohnt. Von seiten der Geschäftsführungen wird vielfach befürchtet, mit der Anwendung von E-Mail könnten Zuständigkeiten und Hierarchien umgangen werden und Internet-Zugänge führten zu wildem "Surfen". Betriebs- oder Personalräte thematisieren die Möglichkeiten der Kontrolle und Ausforschung der Beschäftigten durch dieses neue Medium. Daß diesen Befürchtungen mit klaren Regelungen zwischen Betriebsräten und Arbeitgeber entgegengetreten werden kann, zeigt der folgende Vorschlag für eine Betriebsvereinbarung, die in ähnlicher Form schon abgeschlossen wurde.

[FOTO]

Dr.
Rainer W. Gerling

Datenschutzbeauftragter einer Forschungseinrichtung, Lehrbeauftragter für Datensicherheit an der FH München. Studium der Physik an der Universität Dortmund. Promotion und Habilitation an der Universität Erlangen-Nürnberg
E-Mail: rgerling@gmx.de

Die X GmbH, vertreten durch den Geschäftsführer Herrn N.N. und der Betriebsrat der X GmbH, vertreten durch den Vorsitzenden, Herrn N.N., schließen folgende Betriebsvereinbarung (im folgenden BV):

§ 1 Gegenstand

Gegenstand dieser BV ist die Einführung von E-Mail und die Nutzung von Internet-Diensten durch die Beschäftigten der X GmbH.

§ 2 Geltungsbereich

(1) Diese BV gilt für alle Beschäftigten der X GmbH.

(2) Die X GmbH vereinbart bei Verträgen mit Dritten, daß diese BV auch im Rahmen der Dienstleistung des Dritten für die X GmbH eingehalten wird.

Erläuterung:
Damit die Arbeitgeberseite die BV nicht durch die Einschaltung von betriebsfremden Dritten aushebeln kann, wird die Geschäftsleitung verpflichtet, die Geltung dieser BV auch bei Dienstleistungen Dritter zu vereinbaren. Beispiele sind das Outsourcen von EDV-Dienstleistungen wie die Netzbetreuung oder die Fernwartungen von Firmeneinrichtungen.

§ 3 Zweckbestimmung

(1) E-Mail dient der Kommunikation der Beschäftigten untereinander sowie mit externen Stellen.

(2) Die Nutzung der Internet-Dienste dient dem Zugriff auf weltweit verfügbare Informationen und Daten und dem Angebot firmenbezogener Informationen.

(3) Eine ausschließlich private Nutzung von E-Mail und Internetdiensten während der Dienstzeiten ist untersagt.

(4) Die bei der Nutzung der E-Mail und der Internet-Dienste anfallenden personenbezogenen Daten (Protokoll- oder Verbindungsdaten) dürfen nicht zu einer Leistungs- und Verhaltenskontrolle verwendet werden. Personenbezogene Daten, die zur Sicherstellung eines ordnungsgemäßen Betriebs der E-Mail/Internet-Dienste erhoben und gespeichert werden, unterliegen der besonderen Zweckbindung nach § 31 Bundesdatenschutzgesetz (BDSG).

Erläuterung:

(1) Die Bedeutung der Zweckbestimmung liegt in der Regelung, daß die Beschäftigten E-Mail nicht nur firmenintern sondern auch für die Kommunikation mit externen Personen nutzen können.

(2) Zulässig ist weiterhin das Abrufen aller im WWW denkbaren Daten zur Erfüllung dienstlicher Aufgaben. Die BV regelt auch das Angebot firmenbezogener Informationen im Internet. Gemeint sind damit Informationen über und aus der X GmbH. Zulässig ist demnach auch die Bereitstellung von Beschäftigtendaten wie z.B. Telefonverzeichnisse, Organigramme etc. Werden jedoch Beschäftigten-Daten personenbezogen ins Internet eingestellt und damit „übermittelt“, ist eine Einwilligung gemäß § 4 BDSG erforderlich.

(3) E-Mail und Internet-Dienste sollen dienstlich genutzt werden. Eine minimale private Nutzung (z.B. während einer Pause) wird toleriert. Verursacht die private Nutzung Kosten, muß geregelt werden, wie diese dem Arbeitgeber erstattet werden.

(4) Protokoll-Daten, die bei der Nutzung von Diensten, die in dieser BV geregelt werden, anfallen, dürfen nicht zu einer Verhaltens- und Leistungskontrolle benutzt werden. Ausgeschlossen ist also eine personenbezogene Auswertung von Server Logdateien oder Nutzungsstatistiken, die beim Betrieb von WWW-Servern, Firewall-Systemen und anderen Servern anfallen.

Ausdrücklich hingewiesen wird auf die besondere Zweckbindung (§ 31 BDSG), wonach die personenbezogene Daten, die „ausschließlich zu Zwecken der Daten-

schutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden", nur für diese Zwecke verwendet werden dürfen.

§ 4 Begriffe

(1) Personenbezogene Daten (Personaldaten) sind Einzelangaben über persönliche und sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Beschäftigte der X GmbH).

(2) Im übrigen gelten die Begriffsbestimmungen des BDSG.

Erläuterung:

(1) Personenbezogene Daten im Sinne dieser BV sind nur Beschäftigten-Daten. Für die Handhabung anderer personenbezogener Daten (z.B. Kundendaten) ist der Betriebsrat nicht zuständig. Es gilt zwar das BDSG, aber Regelungen im Rahmen einer BV sind nicht zulässig. Anders sähe es aus, wenn die Beschäftigten in der Mehrzahl auch Kunden wären wie dies bei großen Dienstleistern (z.B. Telekom, Lufthansa etc.) durchaus der Fall sein kann.

(2) Die BV versucht die einschlägigen Begriffe jeweils in ihrem Regelungszusammenhang zu definieren. Neben § 4 enthalten daher auch die folgenden Paragraphen Begriffsbestimmungen.

§ 5 Netze

(1) Als Netz werden alle technischen Einrichtungen bezeichnet, die es ermöglichen, Daten zwischen zwei oder mehr Computern in Form von elektromagnetischen oder optischen Signalen zu senden, zu übertragen, zu vermitteln, zu empfangen, zu steuern oder zu kontrollieren.

(2) Die Einrichtungen des Netzes sind angemessen zu sichern, insbesondere Server, Router und ähnliche Netzeinrichtungen sind in Räumen aufzustellen, zu denen nur besonders Berechtigte Zugang haben. Die Verkabelung ist vor unberechtigten Zugriffen zu schützen. Angemessen ist die Sicherung (Satz 2), wenn der für die Schutzmaßnahmen zu erbringende technische und wirtschaftliche Aufwand im Verhältnis zur Bedeutung der zu schützenden Daten und der zu sichernden Anlagen und dem Risiko ihrer Verletzlichkeit verhältnismäßig ist.

Erläuterung:

(1) Die Definition des Netzes orientiert sich an dem funktionalen Begriff des Telekommunikationsnetzes in § 3 Nr. 16, 21 TKG. Da die verschiedenen elektronischen Kommunikationsformen mehr und mehr zusammen wachsen, ist es auf Dauer sinnvoll eine „Telekommunikations-BV" abzuschließen.

(2) Alle aktiven Komponenten des Netzes sind besonders zu schützen. Kabel sollten nicht offen verlegt werden, damit insbesondere der Einbau von Überwachungsgeräten (z.B. Sniffer) verhindert wird. Von der Netzverkabelung sollte in den Arbeitsräumen der Beschäftigten nur die Netzwerksteckdosen sichtbar sein. So weit Switches/Hubs technisch in der Lage sind sollten feste Bindungen zwischen der MAC-Adresse des Netzwerkadapters und dem entsprechenden Port des Switches/Hubs hergestellt werden. Auf diese Weise kann das unkontrollierte Anschließen privater EDV-Geräte durch nicht autorisierte Mitarbeiter verhindert werden.

Alle Schutzmaßnahmen müssen wirtschaftlich vertretbar sein. Maßstab ist die Schutzwürdigkeit der personenbezogenen Daten.

§ 6 E-Mail

(1) E-Mail-Server sind zentral aufgestellte Computer, die der Verteilung, Zwischenspeicherung und gegebenenfalls auch der Speicherung von E-Mail dienen. Klienten sind die Arbeitsplatzrechner der Beschäftigten, auf denen E-Mail erstellt, empfangen, gelesen und verarbeitet wird.

(2) E-Mail-Server sind so aufzustellen, daß Unberechtigte keinen Zugang haben. Auf den Servern sind E-Mails gegen unberechtigte Zugriffe besonders zu sichern.

(3) E-Mail darf nur auf den dafür vorgesehenen E-Mail-Servern zwischengespeichert und an die Empfänger verteilt und zugestellt werden.

(4) Eingehende E-Mail kann auf dem Arbeitsplatzcomputer des Empfängers, ausgehende auf dem des Absenders gespeichert werden.

(5) Die E-Mail-Server sind in Anlage 1 aufgeführt. Anlage 2 enthält die in der X GmbH eingesetzte E-Mail-Software für E-Mail Server und Klienten.

Erläuterung:

(1) Die BV unterscheidet in Hinblick auf die unterschiedlichen Schutzbedürfnisse zwischen E-Mail Servern (Satz 1) und Klienten (Satz 2).

(2) Der Arbeitgeber wird verpflichtet die E-Mail Server besonders geschützt aufzustellen, da auf ihnen regelmäßig zahlreiche E-Mails gespeichert sind, die dem Fernmeldegeheimnis nach § 85 TKG unterliegen.

Soweit möglich sollte auch der Zugriff der System- und Netzadministratoren auf die Inhalte der E-Mails technisch unterbunden werden. Hierfür eignet sich am besten die End-zu-End Verschlüsselung der E-Mail mit Verfahren wie PGP, PEM oder S/MIME.

(3) Die Klienten übermitteln die abgesandten Nachrichten an den E-Mail Server und rufen eingehende E-Mails dort ab. E-Mail, die auf die Zustellung wartet, befindet sich nur auf den E-Mail Servern. Mit einem solchen Verfahren wird sichergestellt, daß die gesamte Menge der E-Mails auf wenigen und damit überschaubaren Speichern befindet und entsprechend gut geschützt werden kann.

(4) Dieses Verfahren entspricht den Vorgaben der TCP/IP Welt mit den Protokollen SMTP und POP3. Die eingehenden E-Mail-Nachrichten werden auf dem Zielsystem gespeichert, typischerweise dem Arbeitsplatzcomputer der Beschäftigten. Um keine Technik auszuschliessen, regelt Abs. 4 eine Ausnahme von Abs. 3.

(5) Die Konfiguration der Hardware und die eingesetzte Software werden in Anlagen aufgezählt, die Bestandteil der BV sind und nicht einseitig geändert werden können. Bei ständig umfangreicher werdender Software ist es im Hinblick auf die Kontrollmöglichkeiten wichtig, daß über Versionsnummern und ihre Funktionalitäten Einigkeit besteht. Bei einer Änderung der eingesetzten Hard- oder Software ist keine Änderung der BV, sondern nur der jeweiligen Anlage erforderlich.

§ 7 Verwendung von E-Mail

(1) E-Mail wird zum Empfang und zur Versendung von elektronischer Post genutzt. Sie kann zur Weitergabe von Dateien und Vorgängen benutzt werden. Eine automatisierte Vorgangssteuerung mittels E-Mail wird hiermit nicht eingeführt. Eine derartige Vorgangsteuerung bedarf zur Einführung einer gesonderten Betriebsvereinbarung.

(2) Die X GmbH kann zur Information der Beschäftigten ein „Schwarzes Brett" im E-Mail-System einrichten oder E-Mail an alle Beschäftigten versenden. E-Mail mit identischem Inhalt an alle Beschäftigten muß nicht verschlüsselt werden. Solange nicht alle Beschäftigten einen Arbeitsplatz-

rechner mit Zugriff auf E-Mail haben, werden sie auf herkömmliche Art (z.B. durch Aushänge oder Rundschreiben) informiert.

(3) Der Betriebsrat der X GmbH erhält auf Wunsch die gleichen E-Mail-Möglichkeiten zur Information der Beschäftigten wie die Geschäftsleitung.

(4) Das Löschen von unerwünschter E-Mail (SPAM) geschieht nach vom Arbeitgeber zur Verfügung gestellten Regeln. Die Aktivierung dieser Regeln erfolgt durch den Beschäftigten

Erläuterung:
(1) Zur Arbeitsvereinfachung und Zeiteinsparung ist es zulässig, Vorgänge und Dateien per E-Mail weiter zu leiten. Diese Opton ist jedoch gegenüber einer automatisierten Vorgangssteuerung abzugrenzen. Bei einer Vorgangssteuerung laufen Bearbeitungschritte entweder zeitgesteuert oder ereignisgesteuert ab. Jederzeit ist der Stand des Vorgangs für die Beteiligten (auch die Vorgesetzten) abrufbar. Wegen des großen Potentials an Verhaltens- und Leistungskontrolle wird vorerst hierauf verzichtet.

(2) Hier wird die Absicht erklärt firmeninterne Informationen in Zukunft nur noch elektronisch zu verteilen. Solange es Beschäftigte ohne Arbeitsplatzcomputer oder ohne Zugriffsmöglichkeiten auf die E-Mail gibt, haben diese einen Anspruch auf Information auf Papier.

(3) Um „Waffengleichheit" zwischen Arbeitgeber und Betriebsrat in Hinblick auf die innerbetrieblichen Informationsmöglichkeiten herzustellen, kann der Betriebsrat auf Wunsch die gleichen Möglichkeiten zur Information der Beschäftigten wie der Arbeitgeber benutzen. Der Betriebsrat kann jedoch nichts einfordern, was über die Möglichkeiten des Arbeitgebers hinausgeht.

(4) § 354 StGB (bzw. der geplante § 206 StGB gemäß BegleitG-E-TKG) stellt das Unterdrücken von E-Mails unter Strafe. Im Interesse einer Ressourcen-schonenden Nutzung ist das Filtern der E-Mail sinnvoll, um beispielsweise die Übersendung unverlangter Werbung zu unterbinden. Das Aktivieren des Filtermechanismus erfolgt durch den Nutzer (=Empfänger der E-Mail). Die technischen Werkzeuge zum Filtern werden zentral zur Verfügung gestellt.

§ 8 Verschlüsselung

(1) E-Mail mit vertraulichem Inhalt oder mit personenbezogenen Daten Dritter darf innerhalb der X GmbH sowie an externe Stellen nur verschlüsselt versendet werden. Nachrichten mit Inhalten nach Satz 1 dürfen an externe Stellen nicht per E-Mail übermittelt werden, soweit diese nicht in der Lage sind, verschlüsselte E-Mail zu lesen.

(2) Das E-Mail-System muß ermöglichen, ausgehende E-Mail mit dem öffentlichen Schlüssel des Empfängers zu verschlüsseln. Das Format der ausgehenden verschlüsselten E-Mail soll einem offenen Standard für verschlüsselte E-Mail genügen.

(3) Zur Verschlüsselung der E-Mail stellt der Arbeitgeber ein Public-Key-Verschlüsselungsschema zur Verfügung. Jeder Beschäftigte erhält einen öffentlichen und einen privaten Schlüssel. Öffentliche Schlüssel werden allgemein zugänglich gemacht und in geeigneter Weise vor Manipulationen gesichert (zertifiziert). Der private Schlüssel eines Beschäftigten wird ihm geschützt übergeben, so daß Dritte von ihm keine Kenntnis erlangen können. Private Schlüssel dürfen nicht dupliziert und an keiner zentralen Stelle innerhalb der X GmbH gespeichert werden.

(4) Schlüsselpaare nach Abs. 3 werden nach allgemein anerkannten Regeln generiert. Die zur Generierung der Schlüssel erforderlichen Daten werden nach der Schlüsselgenerierung unverzüglich gelöscht. Die technischen Einrichtungen orientieren sich am § 16 SigV[1]; die privaten Schlüssel werden bevorzugt in Chipkarten gespeichert.

(5) Die X-GmbH ist berechtigt, die E-Mail-Adressen und die öffentlichen Schlüssel der Beschäftigten Dritten zugänglich zu machen. Die erforderliche Einwilligung im Sinne des BDSG wird auf den Anträgen zur Einrichtung eines E-Mail-Accounts eingeholt.

Erläuterung:
(1) Erklärte Absicht der BV ist es, zum Schutz von Betriebs- und Geschäftsgeheimnissen und zur Wahrung des Fernmeldegeheimnisses die Verschlüsselung von E-Mail zu ermöglichen. Die BV verpflichtet die Beschäftigten, firmeninterne E-Mail und E-Mail nach außen zu verschlüsseln. Welche Inhalte im Einzelfall vertraulich zu behandeln sind, wird durch die BV nicht geregelt, sondern ist Gegenstand von Geheimschutzanweisungen des Arbeitgebers. Derartige Inhalte können beispielsweise Betriebs- und Geschäftsgeheimnisse sein (Konstruktionszeichnungen, Angebote über Leistungen, Bilanzangaben etc.). Mit der Verpflichtung, personenbezogene Daten zu verschlüsseln, erfüllt die BV die Anforderung der Anlage nach § 9 BDSG.

Wenn Empfänger nicht über die erforderliche Ausstattung zum Empfang verschlüsselter E-Mail verfügen, dürfen die Nachrichten nicht per E-Mail übermittel werden.

(2) Der Arbeitgeber ist verpflichtet, ein E-Mail-System zu installieren, daß die Verschlüsselung ermöglicht. Es soll sich an einem offenen Standard orientieren, damit der Schutzmechanismus der Verschlüsselung möglichst vielfältig eingesetzt werden kann.

(3) Als Verschlüsselungsverfahren kommen nach dem derzeitigen Stand der Technik nur sogenannte Publik-Key Verfahren in Frage. Durch die explizite Erwähnung des öffentlichen und privaten Schlüssels bekennt sich die BV zu diesem Verfahren, das im übrigen auch zur Anwendung von elektronischen Signaturen nach dem Signaturgesetz geeignet ist.[2] Die öffentlichen Schlüssel werden geeignet zertifiziert und verteilt. Bewußt verzichtet die BV auf detaillierte Aussagen, um einer Anpassung an die weitere technische Entwicklungen nicht entgegenzustehen. Zur Zeit kann die Vorgabe des Abs. 1 durch die drei Verfahren PGP, PEM und S/MIME erfüllt werden.

Das Verbot der zentralen Schlüsselspeicherung richtet sich gegen Key-Recovery und andere Schüsselhinterlegungs-Verfahren. Sollte in Deutschland eine gesetzliche Kryptoregulierung kommen, muß die BV an die gesetzlichen Vorschriften angepaßt werden.

(4) Die Schlüsselpaare können nach beliebigen technischen Verfahren generiert werden, so lange sichergestellt ist, daß die privaten Schüssel der Beschäftigten nicht rekonstruiert werden können. Um jedweden Verdacht auf Hintertüren in einer zentralen Schlüsselerzeugung zu begegnen, sollen die Schüssel vorzugsweise dezentral auf den Arbeitsplatzrechnern der Beschäftigten erzeugt werden. Damit verläßt der private Schlüssel nie die Einflußsphäre des Beschäftigten.

(5) Damit Dritte mit der X-GmbH verschlüsselt kommunizieren können, ist es erforderlich , daß die E-Mail-Adressen und

[1] Verordnung zur digitalen Signatur (Signaturverordnung - SigV), Beschluß des Bundeskabinets vom 8. Oktober 1997; http://www.iukdg.de

[2] Art. 3 des IuKDG vom 22. Juli 1997, BGBl. I S. 1870: http://www.iukdg.de.

die öffentlichen Schlüssel der Beschäftigten allgemein abgerufen werden können (z.B. über X.500 oder LDAP Server). Derartige Server sind Teledienste nach dem Teledienstgesetz.[3] *Die Speicherung und Übermittlung von personenbezogenen Adressen auf dem Server ist nur mit Einwilligung des Betroffenen nach § 4 BDSG möglich. Beschäftigte mit Außenwirkung (Pressestelle, Geschäftsführer etc.) werden diese Einwilligung aus arbeitsrechtlichen Gründen nicht verweigern können. Die erforderliche Einwilligung kann bereits mit dem Einstellungsvertrag eingeholt werden.*

§ 9 Vertretungsregelung

(1) Das E-Mail-System muß über die Funktionen Auto-Forward und Auto-Reply verfügen.

(2) Jeder Beschäftigte erhält zwei E-Mail-Adressen: eine funktionsbezogene (dienstliche) und eine namensbezogene (persönliche) Adresse. Eine funktionsbezogene E-Mail-Adresse kann sich auch auf eine Gruppe von Beschäftigten beziehen (z.B. auf eine Abteilung oder ein Referat). Die E-Mail an beide Adressen landet in der selben Mailbox. Für normale Dienstgeschäfte wird die funktionsbezogene E-Mail Adresse benutzt.

a) Eine E-Mail an die *funktionsbezogene* Adresse wird bei Abwesenheit automatisch an den Stellvertreter weitergeleitet (Autoforward) oder der Absender wird automatisch über die Abwesenheit informiert (Auto-Reply). Vor vorhersehbarer Abwesenheit (z.B. Urlaub, Dienstreise) wird dieser Automatismus durch den Beschäftigten in Absprache mit dem Stellvertreter aktiviert. Bei unvorhersehbarer Abwesenheit (z.B. Krankheit) kann das Verfahren für diese funktionsbezogene Adresse durch den Postmaster (§ 11) auf Veranlassung des Vorgesetzten und in Absprache mit dem Stellvertreter aktiviert werden. Der Zeitpunkt ist schriftlich festzuhalten und dem Beschäftigten nach Rückkehr mitzuteilen.
b) Eine E-Mail an die *namensbezogene* Adresse wird grundsätzlich nicht weitergeleitet. Jeder Beschäftigte kann die Absender automatisch über seine Abwesenheit informieren (Autoreply).

Erläuterung:

(1) Ein Problem stellt der Umgang mit E-Mail im Abwesenheitsfall dar. Da Mitarbieter gegenseitig ihre Passworte nicht kennen (sollten), ist der Zugriff auf die E-Mail abwesender Kollegen nicht möglich. Die dienstliche E-Mail muß aber trotzdem weiter bearbeitet werden können. Es ist deshalb notwendig, entweder die dienstliche E-Mail an den Stellvertreter weiter zu leiten, oder den Absender der E-Mail über die Abwesenheit zu informieren. Die Weiterleitung ist zu bevorzugen, da andernfalls der Absender der E-Mail über die Vertretungsregeln innerhalb der X-GmbH informiert sein muß. Es ist aber möglich, in der automatischen Antwort auf den Vertreter hinzuweisen, vorausgesetzt er hat in diese Übermittlung eingewilligt.

(2) Jeder Beschäftigte erhält eine E-Mail-Adresse, die sich aus seiner Funktion ableitet. Zusätzlich erhält er auch eine Adresse mit seinem normalen Namen. Außerdem soll es möglich sein, Gruppenadressen einzurichten. E-Mail kann dann einfach an diese Gruppenadresse (z.B. Einkauf, Controlling etc.) gerichtet werden. In der Gruppe wird diese E-Mail dann an die zuständigen Gruppenmitglieder verteilt.

a) Wird auf Grund der funktionsbezogenen Adressierungsvariante die E-Mail als eindeutig dienstlich gekennzeichnet, wird sie bei Abwesenheit weiter geleitet, um keine Verzögerungen bei der Bearbeitung zu erzeugen. Weiß ein Beschäftigter, daß er abwesend sein wird, aktiviert er die Weiterleitung und informiert seinen Stellvertreter. Bei unvorhersehbarer Abwesenheit muß ein Dritter die Weiterleitung der E-Mail aktivieren. Die nötige formale Prozedur wird festgelegt, damit im nachhinein jederzeit feststeht, an wen eine E-Mail zugestellt wurde. Auch der abwesende Beschäftigte ist bei Rückkehr zu informieren.

b) Eine E-Mail an die namensbezogene E-Mail wird wie ein Brief mit dem Zusatz „persönlich" behandelt. Ist der Beschäftigte abwesend, wird die E-Mail nicht weiter geleitet. Niemand außer dem betreffenden Mitarbeiter kann diese E-Mail lesen. Der Arbeitgeber hat unter keinen Umständen Zugriff auf diese E-Mail, da der Inhalt persönlich sein kann. Der Beschäftigte kann bei Abwesenheit im eigenen Ermessen den Absender einer E-Mail über seine Abwesenheit informieren.

Eine vom Beschäftigten nachvollziehbare Transparenz des Verfahrens hilft bei der Akzeptanz des neuen Verfahrens.

§ 10 Posteingangsbuch

(1) Die X GmbH führt ein elektronisches Posteingangsbuch. Dabei werden alle von Außen eingehenden E-Mails an funktionsbezogene Adressen gemäß § 9 Abs. 2 mit Absender, Empfänger, E-Mail-ID, Datum und Uhrzeit in einer Log-Datei gespeichert.

(2) In E-Mail-Systemen kann man sich mittels der Optionen „die E-Mail ist auf dem Zielrechner angekommen" (Zustellungsbestätigung) oder "der Empfänger hat die E-Mail gelesen" (Lesebestätigung) davon überzeugen, ob eine Nachricht angekommen ist. Diese Optionen dürfen nicht zu Verhaltens- und Leistungskontrolle von Beschäftigten verwendet werden. Im E-Mail-System wird standardmäßig keine Lesebestätigung angegeben. Von Beschäftigten darf nicht verlangt werden, die Lesebestätigung zu aktivieren.

Erläuterung:

(1) Der Posteingang von außen muß nachvollziehbar bleiben. In Analogie zur guten alten Poststelle, die ein Posteingangsbuch auf Papier führt, wird jetzt ein elektronisches Posteingangsbuch in Form einer Logdatei geführt. In dieser Datei werden keine Inhalte und auch keine Betreffs gespeichert. Dies wäre auch ein Verstoß gegen das Fernmeldegeheimnis nach §85 TKG. E-Mails an die namensbezogene Adresse dürfen nicht protokolliert werden.

(2) Um zu verhindern, daß mittels E-Mail festgestellt wird, ob ein Beschäftigter am Arbeitsplatz sitzt und seine E-Mail zeitnah liest, wird die Lesebestätigung ausgeschaltet. Alle E-Mail-Klienten werden mit ausgeschalteter Lesebestätigung installiert. Ein Beschäftigter kann, wenn er will, die Lesebestätigung aktivieren. Das Aktivieren der Lesebestätigung darf weder von Vorgesetzten noch von Kollegen verlangt werden.

§ 11 Postmaster

Für die Verwaltung des E-Mail-Systems sind sog. Postmaster zuständig. Sie müssen mit den Bestimmungen des Fernmeldegeheimnisses im TKG und den Vorschriften des BDSG vertraut sein und sie sind auf das Datengeheimnis gemäß § 5 BDSG zu verpflichten. Über alle Informationen, die sie durch ihre Tätigkeit erhalten, haben sie Stillschweigen zu bewahren. Dies gilt insbesondere auch für die unbeabsichtigte Kenntnisnahme von E-Mails dienstlichen oder persönlichen Inhalts.

[3] Art. 1 des IuKDG (Fußn. 2).

Erläuterung:
Die Verwalter der E-Mail-Systeme (Postmaster) müssen besonders vertrauenswürdig und mit den entsprechenden gesetzlichen Regelungen und Vorschriften vertraut sein. Sie sollten zumindest das BDSG und das TKG in den relevanten Vorschriften kennen. Auch Kenntnisse des TDG, TDDG und des MeDStV wären sinnvoll. Bei Zustellfehlern erhalten sie im Allgemeinen Kopien der fehlerhaften E-Mail.

§ 12 Zugriffsrechte und Passworte

(1) Jeder Benutzer des E-Mail-Systems erhält eine Zugriffsberechtigung (Passwort) und einen eigenen Datenbereich (Mailbox).

(2) Passworte bestehen aus mindestens sechs Zeichen, davon mindestens ein Sonderzeichen; damit sind alle Wörter ausgeschlossen, die im Duden stehen. Benutzer müssen ihre Passworte sorgfältig auswählen und geheimhalten. Es ist untersagt, Passworte an andere weiterzugeben.

(3) Ohne Kenntnis und Zustimmung der Beschäftigten dürfen Dritte keine Einsicht in die E-Mail eines Beschäftigten nehmen. Kenntnis und Zustimmung werden unterstellt, wenn E-Mail in Bereiche weitergeleitet wird, die für Dritte zugänglich sind.

(4) Soweit die E-Mail dienstliche Inhalte betrifft, kann der Vorgesetzte verlangen, daß der Beschäftigte die E-Mail für ihn ausdruckt.

Erläuterung:
(1) Um seine E-Mail aus der Mailbox abzurufen benötigt jeder Beschäftigte ein eigenes Passwort. Außerdem wird die E-Mail auf dem E-Mail-Server so abgelegt, daß jeder nur auf seine E-Mail zugreifen kann.

(2) Benutzer neigen dazu einfache, leicht merkbare Passworte zu wählen. Hier wird ein Mindest-Standard vorgeschrieben. Außerdem wird es deutlich verboten, Passworte weiter zu geben. Damit wird zumindest verhindert, daß ein Vorgesetzter verlangen kann, daß man sein Passwort vor dem Urlaub einem Kollegen mitteilen muß.

(3) Der Arbeitgeber und Dritte dürfen ohne Wissen und Einverständnis des Beschäftigten nicht in dessen E-Mail lesen. Insoweit unterstreicht dieser Absatz das Fernmeldegeheimnis nach §85 TKG. Wer E-Mail in allgemein zugänglich Bereiche weiter leitet gibt damit indirekt die Zustimmung, daß andere die Information auch lesen.

(4) Allerdings kann der Arbeitgeber im Rahmen seines Direktionsrechts von dem Beschäftigten verlangen, ihm alle dienstlichen Vorgänge zugänglich zu machen. Um die Privatsphäre des Beschäftigten zu wahren, ist der Beschäftigte seinerseits verpflichtet, den Inhalt dienstlicher E-Mail zugänglich zu machen. Verweigert der Beschäftigte die Einsicht in dienstliche E-Mail muß er mit arbeitsrechtlichen Konsequenzen rechnen. Im übrigen gelten die folgenden Grundsätze der Archivierung.

§ 13 Archivierung

(1) Soweit zu Dokumentationszwecken erforderlich, werden ein- und ausgehende E-Mails ausgedruckt und wie Schriftstücke aufbewahrt. Die zugrundeliegenden Dateien werden im Rahmen der normalen Datensicherung gesichert (Anlage zu § 9 BDSG) und nicht archiviert.

(2) Dienstliche E-Mail, die verschlüsselt empfangen und zu Nachweiszwecken noch benötigt wird, ist auszudrucken und zu den Akten zu nehmen.

Erläuterung:
(1) Viele Informationen müssen langfristig aufbewahrt werden. Gegebenenfalls sollen sie einem klassischen Vorgang (d.h. auf Papier) zugefügt werden. Solange nicht ein ausgefeiltes elektronisches Archivsystem zur Verfügung steht, müssen E-Mails ausgedruckt werden. Die normale Datensicherung mit dem Ziel Datenverlusten bei technischen Störungen vorzubeugen, ersetzt keine Archivierung.

(2) Die Verschlüsselung wird nach dieser BV eingesetzt, um die Daten während der Übermittlung zu schützen. Damit auch verschlüsselte E-Mail zur Abwicklung der Dienstgeschäfte zur Verfügung steht, ist sie wie gewöhnliche Post auch zu den Akten zu nehmen.

§ 14 Internet-Dienste

(1) Alle Beschäftigten, die Zugang zum Internet haben, können die in der Anlage 3 aufgeführten Internet-Dienste dienstlich nutzen. Bei deren Nutzung sind die in Anlage 4 enthaltenen Vorschriften und Regeln zu beachten.

(2) Soweit zum effektiven Zugriff auf das Internet Proxy- oder Cache-Server installiert werden, werden die Log-Dateien nur anonymisiert geschrieben.

(3) Eine personenbezogene Kontrolle der Internet-Nutzung findet nur beim konkreten Verdacht der mißbräuchlichen Benutzung statt. Die anfallenden Protokolldaten werden nur zur Klärung des konkreten Verdachts ausgewertet. Der Betriebsrat ist zu beteiligen.

(4) Eine Auswertung der Nutzungsinformationen des WWW-Browsers auf der lokalen Festplatte eines Benutzer ist nur unter sinngemäßer Anwendung des Abs. 3 zulässig.

(5) Der Arbeitgeber ist berechtigt den Zugriff auf offensichtlich dienstlich nicht erforderliche Inhalte zu sperren.

Erläuterung:
(1) Den Arbeitnehmern wird die Nutzung der üblichen Internetdienste (WWW, ftp etc.) für dienstliche Zwecke erlaubt. Er wird aber auf die geltenden Rechtsvorschriften und Nutzungsregeln hingewiesen.

(2) Das TDDG und das TKG regeln den Schutz der Kommunikationsinhalte. Ein Proxy- oder Cache-Server ist „hervorragend geeignet“ die detaillierte Internetnutzung der Beschäftigten zu kontrollieren. Diese Kontrolle wird nur anonym erlaubt. Es kann also festgestellt werden, ob und welche unerlaubte Inhalte die Beschäftigten nutzen, nicht aber wer diese nutzt.

(3) Ergeben die anonyme Kontrolle oder andere Hinweise einen konkreten Verdacht einer hinreichend schweren mißbräuchlichen Nutzung durch einen Beschäftigten (z.B. Verrat von Werksgeheimnissen, Abruf strafbarer Inhalte), so kann unter Einschaltung des Betriebsrates eine personenbezogene Kontrolle durchgeführt werden. Es wird aber nur der konkrete Verdacht geklärt, und nicht unter Vorgabe des Verdachtes die komplette Belegschaft kontrolliert. Es liegt in der Art der anfallenden Protokolldaten, daß diese das Nutzungsverhalten der kompletten Belegschaft offen legen. Die Auswertung muß eventuell durch eine neutrale Instanz (z.B. den Datenschutzbeauftragten) durchgeführt werden.

(4) Moderne Browser hinterlassen auf der lokalen Festplatte vielfältige Spuren. Diese Daten dürfen auch nur in Analogie zum Abs. 3 ausgewertet werden.

(5) Der Arbeitgeber kann den Zugriff auf nur privat-nutzbare Inhalte sperren. Dieser Absatz stellt ein Regulativ zur Eindämmung einer übermäßigen privaten Nutzung dar. Fall erforderlich kann der Zugriff auf z.B. Porno-Server unterbunden werden.

§15 Information der Beschäftigten

Die Beschäftigten sind über die besonderen Probleme der E-Mail und der Internet-Dienste zu unterrichten. Insbesondere ist auf folgendes hinzuweisen:

a) gesetzliche Regelungen zum Fernmeldegeheimnis,
b) Anwendung der Datenschutzvorschriften (BDSG),
c) Zugänglichkeit unverschlüsselter E-Mail bei Transport im Netz,
d) Probleme der Archivierung,
e) dienstliche (arbeitsrechtliche), gesetzliche und ethische Grundsätze und Vorschriften bei der Nutzung von Internet-Diensten.

Erläuterung:
Die Beschäftigten müssen über die rechtlichen Rahmenbedingungen der E-Mail und Internet-Nutzung aufgeklärt werden. Im Rahmen der Schulungen über die Nutzung der Software ist dieses problemlos möglich.

§ 16 Kontrolle der BV

(1) Der Betriebsrat hat das Recht, die Einhaltung dieser BV zu überprüfen.

(2) Der Betriebsrat kann zur Durchführung seiner aus dieser BV resultierenden Aufgaben nach Abstimmung mit der X GmbH Sachverständige seiner Wahl hinzuziehen; die notwendigen Kosten trägt die X GmbH.

Erläuterung:
(1) Die Kontrolle der BV erfordert unter Umständen einen detaillierten Einstieg in die Kommunikationssysteme. Da der Betriebsrat nachprüfen darf, kann ihm der Arbeitgeber den Zugriff auf die entsprechenden Systeme nicht verweigern.

(2) Falls der Betriebsrat mit den technischen Fragen überfordert ist, (was wohl im Allgemeinen der Fall ist) darf er technischen Sachverstand zuziehen. Der Arbeitgeber muß dann die Kosten tragen.

§ 14 Verstöße

(1) Der Datenschutzbeauftragte, der Arbeitgeber und der Betriebsrat sind unverzüglich über Mißbrauch und Mißbrauchsversuche des E-Mail-Systems zu informieren. Alle Beschäftigten haben das Recht, vermutete oder tatsächliche Verstöße den Genannten vorzutragen. Das Beschwerderecht der Beschäftigten gem. der §§ 84 und 85 BetrVG bleibt hiervon unberührt.

(2) Personenbezogene Daten, die entgegen dieser BV erfaßt oder gespeichert werden, dürfen nicht verwendet werden. Personelle Maßnahmen, die auf Informationen beruhen, die unter Verstoß gegen die Zweckbestimmung gem. §3 gewonnen wurden, sind unwirksam. Der unberechtigte Zugriff auf personenbezogene Daten hat arbeitsrechtliche Konsequenzen.

Erläuterung:
(1) Das Informationsrecht dient zur Fortentwicklung der BV, um Schwachstellen aufzudecken und Lösungen zu entwickeln.

(2) Wird gegen die vorliegende BV verstoßen, dürfen die dabei gewonnenen Erkenntnisse nicht verwertet werden. Außerdem wird der unberechtigte Zugriff auf personenbezogene Daten mit arbeitsrechtlichen Konsequenzen bedroht. Denkbar wäre auch bereits den Versuch des Zugriffs zu sanktionieren.

§ 15 Inkrafttreten und Kündigung

Diese BV tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist von drei Monaten zum Ende eines Kalenderjahres gekündigt werden. Bis zum Abschluß einer neuen BV gilt die vorliegende Vereinbarung weiter.

Erläuterung:
Eine Nachwirkungs Klausel verhindert, daß nach Kündigung der BV durch eine Seite der E-Mail-Betrieb eingestellt wird.

Anlagen 1-3

Auf den Abdruck der Anlagen 1 bis 3 wurde verzichtet, da diese individuell erstellt werden müssen. Sie enthalten technische Informationen über die eingesetzte Hard- und Software sowie die genutzten Internet-Dienste.

Anlage 4: Code of Conduct

Unzulässig ist jede Internetnutzung, die geeignet erscheint den Interessen der X GmbH oder deren Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Gesetze oder Verordnungen verstößt. z.B.

- das Abrufen oder Anbieten von Texten die gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- das Abrufen oder Anbieten von weltanschaulicher, politischer oder kommerzieller Werbung,.
- das Abrufen oder Anbieten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen oder pornographischen Äußerungen oder Abbildungen.

Anbieten heißt verbreiten über das WWW oder das Einstellen in Newsgruppen oder Diskussionsforen in einer Art, daß die Firmenzugehörigkeit erkennbar ist (z.B. durch die E-Mail-Adresse des Absenders) oder unter Verwendung von EDV-Anlagen der X GmbH. Abrufen heißt auf im Netz vorhandene Informationen mit EDV-Anlagen der X GmbH zugreifen.

Literatur

Gesetzentwurf der Bundesregierung für ein Begleitgesetz zum Telekommunikationsgesetz (BegleitG), Bundestagsdrucksache 13/8016 vom 23.06.1997. Siehe auch http://www.gwdg.de/~rgerlin/stgbaus.htm

Privacy Enhanced Mail, RFC 1421 bis RFC 1424; ftp://ftp.nic.de/pub/doc/rfc

Pretty Good Privacy, http://www.pgp.com und http://www.ifi.uio.no/pgp

S/MIME: siehe auch http://www.rsa.com/rsa/S-MIME/home.html

LDAP, Lightweight Directory Access Protocol, RFC 1777; ftp://ftp.nic.de/pub/doc/rfc

X.500: The Directory: Overview of Concepts, Models and Service. CCITT Recommendation X.500, 1988; Information Processing Systems - Open Systems Interconnection - The Directory: Overview of Concepts, Models and Service. ISO/IEC JTC 1/SC21; International Standard 9594-1, 1988

Ich danke J. Bizer für klärende Diskussionen und hilfreiche Vorschläge.

Stichwörter

Arbeitnehmer, Betriebsrat, Betriebsvereinbarung, E-Mail, Fernmeldegeheimnis, Internet, Log-Dateien, E-Mailfilter, E-Mail-Server, Passworte, Telekommunikation, Verschlüsselung.