IT-Rechtsleitfaden

Autor

- Rechtsanwalt, Kanzlei esb in Stuttgart, spezialisiert auf IT-Recht
- Seminarleiter Internet-Recht, IT-Sicherheit, Datenschutz
- Ausbilder für Datenschutzbeauftragte
- Fachbuchautor „IT-Recht in der Praxis“, Vieweg, 2. Auflage, Dez. 2006
- Lehrbeauftragter der Universität Stuttgart für Medienrecht
- E-Mail: horst@speichert.de
- Internet: www.kanzlei.de, www.speichert.de

Vorwort

Das vorliegende Dokument ist ein genereller Leitfaden. Es kann nicht die verbindliche Rechtsauskunft durch einen Fachanwalt ersetzen. Websense bittet Sie um Ihr Verständnis, dass trotz sorgfältiger Recherche keine Garantie oder Gewährleistung übernommen werden kann für die Richtigkeit oder Eignung der enthaltenen Richtlinien. Grundsätzlich sollte sich ein Unternehmen vor einer Implementierung von Richtlinien individuell rechtlich von einem Spezialisten beraten lassen.

Websense Firmenprofil

Websense (Nasdaq: WBSN), eines des führenden Unternehmen im Bereich integrierter Web-, Messaging- und Data-Protection-Technologien, schützt weltweit mehr als 42 Millionen Mitarbeiter in über 50.000 Unternehmen, Behörden und öffentlichen Organisationen vor externen Angriffen und internen Sicherheitslücken. Distribuiert über ein globales Netz von Channelpartnern helfen Websense-Software und gehostete Security-Lösungen Unternehmen dabei, sich vor bösartigem Programmcode jeder Art zu schützen, den Verlust vertraulicher Daten zu verhindern und für die Einhaltung verbindlicher Regeln bei der Internetnutzung zu sorgen. Weitere Informationen: www.websense.de.

Inhalt:

Mit Sicherheit Recht behalten !

IT-Sicherheit ist eine von Haus aus technisch dominierte Disziplin, die jedoch in starkem Umfange organisatorische Maßnahmen erfordert und zwingend die rechtlichen Rahmenbedingungen einhalten muss. Es handelt sich um eine ganzheitliche Aufgabe, deren technische, organisatorische und rechtliche Komponenten in enger Wechselbeziehung miteinander verzahnt sind. Die technische Sicherheit etwa durch Firewalls wird flankiert von organisatorischen Maßnahmen wie Policies, Nutzungsrichtlinien oder Zertifizierungen. Technik und Organisation wiederum werden in Verträgen oder Betriebsvereinbarungen rechtlich gestaltet und umgesetzt. Überdacht wird das System von einem verbindlichen Risikomanagement, dass durch die Leitungsebene des Unternehmens umzusetzen ist. Insgesamt ergibt sich eine vielschichtige Pflichtenstruktur, die sich aus einer breiten Palette von Maßnahmen zusammensetzt.

Daraus ergibt sich eine ausgeprägte Ganzheitlichkeit der Informationssicherheit. Filtersysteme, Firewall, Hard- und Software für die IT-Sicherheit unterfallen der Mitbestimmung des Betriebsrates, sofern sie auch zur Mitarbeiterkontrolle geeignet sind. Spätestens wenn der Betriebsrat den Einsatz der Sicherheitstechnik sperrt, wird erkennbar, dass die technische Komponente nicht alleine steht, sondern in ein juristisches Regelwerk eingebunden ist. Die Beispiele lassen sich fortsetzen. Zur Vermeidung von Haftung und Schadensersatz etwa ist nicht allein der Einsatz von Technik, sondern sind insbesondere auch organisatorische Maßnahmen wie Nutzungsrichtlinien, Schulung und Beaufsichtigung von Mitarbeitern sowie rechtliche Gestaltung in IT-Verträgen und Betriebsvereinbarungen erforderlich. Auch hier zeigt sich die enge Verzahnung von Technik, Organisation und Recht.

Wer diesen Strukturen gerecht wird und das Thema ganzheitlich umsetzt, hebt die IT-Sicherheit auf die höhere Qualitätsstufe der Informationssicherheit im Sinne der Standards nach BSI-Grundschutz oder ISO 27001.

.

Bedrohungsszenario

- In einer Aktiengesellschaft mit 5.000 Mitarbeitern arbeitet seit langen Jahren ein qualifizierter Mitarbeiter an einer neuen Technologie zur Produktion von Sonnenkollektoren, die dem Unternehmen einen erheblichen Wettbewerbsvorsprung sichern wird. Durch den Bau eines Eigenheims gerät der Mitarbeiter in finanzielle Schwierigkeiten, als ein Unbekannter an ihn herantritt und ihm größere Geldbeträge für die Herausgabe wichtiger Unterlagen betreffend die neue Technologie bietet. Der Mitarbeiter erbittet Bedenkzeit und prüft die Möglichkeiten, durch eine heimliche „Datensicherung“ über das WAN des Unternehmens an die geforderten Unterlagen zu gelangen.
- Aus einem Bericht in den Medien: „Staatsanwaltschaft Köln ermittelt gegen ca. 3.500 P2P-Nutzer. Rund 130 Durchsuchungen wurden im Rahmen einer koordinierten Aktion gegen Tauschbörsennutzer heute zeitgleich im gesamten Bundesgebiet durchgeführt. Zahlreiche PC`s und andere Beweismittel wurden beschlagnahmt. Bei den Ermittlungen kam eine speziell zu diesem Zweck entwickelte Software zum Einsatz, die innerhalb von zwei Monaten über 800.000 Datensätze und mehr als 14 Gigabyte Log-Dateien zusammenstellte. Mit diesen Daten ist es gelungen, die Nutzer zu identifizieren.“
- Der Mittelstand zeichnet sich durch ein hohes Maß an Innovationskraft aus und ist deshalb der größte Know-how-Träger der deutschen Wirtschaft. „Keine Kleinstadt ohne Weltmarktführer“. Die notwendige Effizienz, um im globalen Wettbewerb zu bestehen, ist gewaltig. Der enorme Leistungsdruck führt oftmals zur Vernachlässigung notwendiger Sicherheitsbedürfnisse. Gerade der deutsche Mittelstand mit seinen Sicherheitslücken gehört deshalb zu den leichten Zielen weltweiter Wirtschaftsspionage. Wenn man so will, optimale Voraussetzungen für den Abfluss von Hochtechnologie.
- Ein langjähriger Abteilungsleiter ahnt, dass er zum Quartalsende aus betrieblichen Gründen die Kündigung erhalten wird. Seine Verärgerung hierüber ist verständlicherweise groß. Als „Abschiedsgeschenk“ möchte er deshalb seinem treulosen Arbeitgeber einen Trojaner hinterlassen, welcher zeitgesteuert einen Monat nach seinem letzten Arbeitstag die Server lahm legen soll.

Haftungsfragen – Alles was Recht ist!

Die IT-Verantwortlichen in Unternehmen und Behörden fragen sich immer häufiger und dringlicher, inwieweit illegale Vorgänge und Inhalte zur Mitverantwortung des Arbeitgebers bzw. der Mitarbeiter und Geschäftsleitung führen.

Ermittlungsverfahren und Auskunftspflichten

Seit Anfang 2005 wurden allein ca. 30.000 Strafverfahren wegen illegaler Downloads aus P2P- Netzwerken eingeleitet. Es stellt sich die Frage nach einer möglichen Mitverantwortlichkeit

- des Unternehmens
- der Geschäftsleitung
- der IT-Verantwortlichen, Mitarbeiter

für solch illegale und strafbare Inhalte und Vorgänge.

Bei strafbarem Verhalten (→ z.B. illegale Pornografie, raubkopierte Inhalte) erstatten die Geschädigten verstärkt Strafanzeige. Die Behörden versuchen daraufhin die zur Strafverfolgung notwendigen Daten zu ermitteln. Nach der Rechtsprechung werden Auskunftsansprüche der TK-Anbieter (Provider) nach § 113 TKG anerkannt. Auch der Arbeitgeber wird bei erlaubter Privatnutzung zum TK-Anbieter. Demnach müssen

- die öffentlichen Provider → die IP-Adresse herausgeben
- die Arbeitgeber → anhand der IP-Adresse die persönliche Zuordnung zum konkreten Mitarbeiter vornehmen.

Solche Ermittlungen der Behörden bringen die Verantwortlichen in den Unternehmen nicht selten in schwierige Situationen, insbesondere wenn die Passwort- bzw. Identitätsverwaltung beim Arbeitgeber so unzureichend ist, dass die persönliche Zuordnung der IP-Adresse auch den Falschen treffen kann. Je sensibler der verfolgte Straftatbestand ist, desto empfindlicher wird ein zu Unrecht beschuldigter Mitarbeiter reagieren. Denn die persönliche Zuordnung der IP-Adresse und Herausgabe der Daten führt zu unmittelbaren Ermittlungsmaßnahmen gegen den Mitarbeiter.

Vorratsdatenspeicherung

- neues Gesetz seit 01.01.2008 zur Regelung der TK-Überwachung und anderer verdeckter Ermittlungsmaßnahmen und zur Umsetzung der EU-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung
- Zweck: Strafverfolgung, Terrorismusbekämpfung
- betroffen ist die gesamte Telekommunikation: E-Mail, Internet, Mobiltelefonie, SMS, Telefonie, VoIP
- TK-Anbieter sind nach dem neuen § 113a TKG verpflichtet, Verbindungs- und Standortdaten 6 Monate vorzuhalten

Gegen die Neuregelung bestehen verfassungsrechtliche Bedenken, die jedoch laut Bundesregierung nicht zur Aussetzung des Gesetzesvollzugs bis zu einer Entscheidung des BVG führen wird. Entscheidende Frage ist daher, wer zur Vorratsdatenspeicherung gemäß §§ 113a, 113b TKG verpflichtet ist.

- Persönlicher Anwendungsbereich, Adressatenkreis
    - nach § 113a TKG jeder öffentlich zugängliche TK-Dienst für Endnutzer
    - Begründung Gesetzentwurf: „für den nicht-öffentlichen Bereich (z. B. unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server von Universitäten) besteht keine Speicherungspflicht“ → demnach wären geschlossene Benutzergruppen (Arbeitsplatz, Hotel, Krankenhaus etc.) ausgeschlossen
    - nach der Literatur jedoch sind geschlossene Benutzergruppen mit Außenkontakt als öffentliche TK anzusehen, so dass nur die interne Kommunikation ausgenommen wäre
    - Fazit: es besteht ein erhebliches Maß an Rechtsunsicherheit

- nach der Begründung des Gesetzentwurfs sollen auch Anonymisierungsdienste zur Vorratsspeicherung verpflichtet sein
- Gastzugang: Unternehmen sind zur Vorratsspeicherung verpflichtet, wenn sie kostenlos einen öffentlichen W-LAN-Zugang anbieten. Es müssen also auch für den Gastzugang Passwörter vergeben und Richtlinien gestaltet werden, um die Vorratsdatenspeicherpflicht zu vermeiden.

Verkehrssicherungspflichten

Zum besseren Verständnis der Haftungssystematik ist die obergerichtliche Rechtsprechung des Bundesgerichtshofes (BGH) zu den Verkehrssicherungspflichten sowie die Vorgaben des KonTraG für ein verbindliches Risikomanagement zu betrachten. Der BGH spricht im Rahmen der Haftungssystematik von Verkehrssicherungspflichten:

> *„wer eine Gefahrenquelle eröffnet oder sich an ihr beteiligt, muss Dritte schützen und hierfür geeignete Schutzmaßnahmen ergreifen“*

- die Kommunikationsvorgänge in Intranet und Internet eröffnen vielfältige Gefahren, sind also Gefahrenquellen im Sinne der Verkehrssicherungspflichten
- die Verkehrssicherungspflichten bestehen im Wesentlichen aus:
    - Organisationspflichten bezüglich betrieblicher (technischer) Abläufe
    - Aufsichtspflichten des Arbeitgebers gegenüber seinen Mitarbeitern
- 100%ige Sicherheit kann im Rahmen der Verkehrssicherungspflichten nicht verlangt werden, aber Maßnahmen nach der Verkehrserwartung, die wirtschaftlich zumutbar sind
- auch die vertraglichen Schutzpflichten orientieren sich an den Verkehrssicherungspflichten

Die Verkehrssicherungspflichten ergeben sich aus einer Vielzahl gesetzlicher und vertraglicher Bestimmungen sowie der Rechtsprechung. Nachfolgend einige Beispiele.

- besondere Verschwiegenheitsverpflichtung und eine strafbewehrte Garantenstellung für besonders sensible Daten
    - bei Amts-, Berufs- und Privatgeheimnissen, § 203 StGB
    - bei Geschäfts- und Betriebsgeheimnissen, § 17 UWG
    - Garantenstellung nach § 13 StGB
    - begehbar auch durch Unterlassen von Sicherungsmaßnahmen, Verletzung von Sorgfaltspflichten
- § 25a Abs. 1 Nr. 2 KWG: Kredit- und Finanzinstitute müssen über angemessene Sicherheitsvorkehrungen für die Datenverarbeitung verfügen, diese werden konkretisiert durch Richtlinien des BaFin (MaRisk), welche ein Risikomanagement für Banken und Finanzdienstleister verlangen
- Vorgaben der Finanzbehörden nach der GoBS oder GDPdU: Risiken für die steuerlich relevanten Datenbestände sind zu vermeiden
- § 9 BDSG plus Anlage → Die Vorschrift enthält die Grundsätze ordnungsgemäßer Datenverarbeitung, also Vorgaben für die technisch-organisatorische Datensicherheit. Es ist ein technisches Sicherheitskonzept zu entwickeln, dass unbefugten Zugriff auf personenbezogene Daten verhindert. Im Einzelnen bedeuted dies:
    - Zutrittskontrolle → räumliche, physische Sicherung, Authentifizierung
    - Zugangskontrolle → Paßwort, Firewall, Festplattenverschlüsselung
    - Zugriffskontrolle → effektive, rollenbasierte Rechteverwaltung
    - Weitergabekontrolle → Datensicherung, Verschlüsselung
    - Verfügbarkeitskontrolle → Virenschutz, Backup, sichere Archivierung

Die konkretisierenden Normen werden von der Rechtsprechung als Maßstab für die angemessenen Sicherungserwartungen herangezogen. Der Umfang der Verkehrssicherungspflichten bestimmt sich insbesondere nach…

- den Sicherheitserwartungen der beteiligten Verkehrskreise
- der Marktüblichkeit der Sicherheits-Hardware und –Software, z. B. hinsichtlich der notwendigen Update-Intervalle eines Virenscanners
- der Quantität der Datenverarbeitung
- der Gefährlichkeit des Tuns
- dem Prinzip der Verhältnismäßigkeit, also der Erforderlichkeit und Angemessenheit von Maßnahmen
- der wirtschaftlichen Zumutbarkeit, also der Größe und Leistungsfähigkeit eines Unternehmens

Nach der Rechtsprechung ist im gewerblichen Bereich eine zuverlässige, zeitnahe und umfassende Sicherung der IT-Systeme erforderlich. Ansonsten können betriebliche Brandherde - wie etwa raubkopierte Software oder der strafbare Download von mp3-Files aus P2P-Netzwerken zur Mitverantwortlichkeit in Unternehmen und Behörden führen. Umgesetzt werden die Pflichten zur Haftungsprävention durch ein Bündel von Maßnahmen, bestehend aus Technik, Nutzungsrichtlinien und rechtlicher Gestaltung:

- Ganzheitlichkeit: abgestimmter Mix aus technischen, organisatorischen und rechtlichen Maßnahmen
- technisch: upgedateter Virenschutz, Archivierung, URL-Filter, Content-, Spam-Filter etc.
- organisatorisch: Zuständigkeits-, Verantwortlichkeitsverteilung, Policy, Nutzungsrichtlinien, Kontrolle der Beschäftigten etc.
- rechtliche Gestaltung: Betriebs-/Dienstvereinbarung, Steuerung durch Verträge, SLA, AGB etc.
- Transparenz der Regeln: erzeugt Vertrauen + Warnfunktion mit Lenkungswirkung

Störerhaftung im Netzwerk, offene W-LAN

Das Landgericht Frankfurt hat am 22.02.2007 entschieden, dass der Betreiber eines offenen W-LAN für urheberrechtswidrige, strafbare Down- bzw. Uploads aus P2P zumindest im Rahmen der Störerhaftung verantwortlich ist. Bei einem offenen W-LAN ohne Passwortschutz ist die Datenübertragung nicht gesichert. So können z.B. strafbare mp3-Files missbräuchlich über das offene W-LAN durch externe Dritte heruntergeladen werden. Im Rechtssinne handelt es sich dabei um ein öffentliches Zugänglichmachen von Musikfiles über P2P. Dem Betreiber eines W-LAN obliegen umfangreiche Verkehrssicherungspflichten. Wer seine Internetverbindung drahtlos betreibt, muss für die Sicherung des Netzwerkes sorgen, andernfalls verstößt er gegen zumutbare Prüfungspflichten.

Das Urteil reiht sich in eine mittlerweile Vielzahl von Entscheidungen ein, welche die Störerhaftung für unsichere Netzwerke oder Plattformen bejahen. So haben etwa auch der BGH oder verschiedene OLG jüngst entschieden, dass für Markenpiraterie zu Schleuderpreisen auf Internetverkaufsplattformen das Auktionshaus haftet.

- es besteht eine Vorsorgepflicht gegen bekannte Missstände
- der Einsatz von präventiver Filtersoftware ist laut BGH zumutbare Prüfungspflicht
- bei eindeutigen Hinweisen (bedingter Vorsatz) → Schadensersatzpflicht

Die dargestellte Rechtsprechung ist auf unsichere Netzwerke, Systeme oder Plattformen gleichermaßen anzuwenden. So wird man in Zukunft auch bei offenen Mail-Relays, über die Spamattacken oder Hackerangriffe erfolgen, eine Haftung des Betreibers bejahen müssen.

Überträgt man die dargestellten Haftungssysteme auf die spezielle Situation in der IT, so ergibt sich das nachfolgende Haftungsszenario.

Szenario und Rechtsfolgen

- Rechtswidrige E-Mail-Anhänge oder Download von Mitarbeitern, z. B. Raupkopien, illegale mp3-Files, führen zu Strafverfolgungsmaßnahmen im Unternehmen (Durchsuchung der Geschäftsräume, Beschlagnahme von Firmenrechnern etc.)
- Eintragungen von außen im eigenen System, z. B. in Blogs, Gästebücher oder Foren → Gefahr illegaler Inhalte wie Beleidigungen, Obszönitäten, Persönlichkeits-, Marken- oder Urheberrechtsverletzungen etc.
- Fremdinhalte von Dritten (z.B. Kundendaten oder Webspace für Dritte)
  → ebenfalls Gefahr, dass die gehosteten Inhalte illegal sind
- Jugendschutz bei Minderjährigen, z.B. Azubis oder Praktikanten
  → Verstoß gegen Jugendschutz, der Arbeitgeber hat hier eine Garantenstellung
- Schutz des Persönlichkeitsrechts am Arbeitsplatz vor Belästigung, Beleidigung etwa durch Spam oder E-Mail-Anhänge, konkretisiert z. B. im Beschäftigtenschutzgesetz (BeschSG)
- Viren und Spam in Kombination mit Hackerangriffen: Verletzung von…
  - Eigentum und Gewerbebetrieb durch Datenbeschädigung oder –verlust
  - Persönlichkeitsrecht, etwa wenn ein Virus personenbezogene Daten ausspioniert und versendet
- Verlust von Arbeitszeit, Performance, Bandbreite, Verfügbarkeit

- bei Verstoß gegen die Pflichten:
    - mit Verschulden → Schadensersatz und möglicherweise Strafbarkeit des Unternehmens, der Geschäftsleitung und der Mitarbeiter
    - ohne Verschulden → Störerhaftung, Unterlassung, Abmahnung, Vertragsstrafe

- bei Erfüllung der dargestellten Pflichten: präventive Haftungsfreizeichnung, denn für Schäden, die trotz Pflichterfüllung eintreten (=Restrisiko), wird nicht gehaftet

Eigenhaftung der IT-Verantwortlichen

Die Vermeidung persönlicher Eigenhaftung ist für die handelnden Mitarbeiter, wie etwa IT-Leiter, Sicherheitsbeauftragte, Administratoren, sonstige IT-Verantwortliche, ein entscheidender Faktor. Hierbei ist zwischen der

- zivilrechtlichen (→ Schadensersatz),
- arbeitsrechtlichen (→ Abmahnung, Kündigung)
- und strafrechtlichen (→ Geld- oder Freiheitsstrafe)

Haftung zu unterscheiden.

Aus dem Arbeitsverhältnis treffen grundsätzlich jeden Mitarbeiter sog. arbeitsvertragliche Nebenpflichten

- Schutz-, Mitwirkungs-, Geheimhaltungs- und Aufklärungspflichten
- als Sorgfaltsmaßstab gilt ein besonnener Mensch mit durchschnittlichen Fähigkeiten in der Situation des Arbeitnehmers
- also individuell unterschiedlich: höhere Sorgfaltsanforderungen an leitende Mitarbeiter
- Beweislast des Arbeitgebers, § 619a BGB

Schadensersatzansprüche des Arbeitgebers wegen Verletzung der arbeitsvertraglichen Nebenpflichten sind in der Praxis nicht häufig, aber möglich.

Aufgrund der Fremdbestimmtheit der Arbeitsleistung trägt der Arbeitgeber das Unternehmensrisiko. Für Tätigkeiten mit erhöhtem Risiko gelten deshalb nach der Rechtsprechung des BAG die Grundsätze zur schadensgeneigten Tätigkeit:

- für vorsätzliches/grobfahrlässiges Verhalten → volle Haftung des Mitarbeiters
- mittlere Fahrlässigkeit → Schadensteilung zwischen Arbeitgeber und Mitarbeiter
- leichte Fahrlässigkeit → keine Haftung des Mitarbeiters

Diese Haftungserleichterung für den Mitarbeiter gilt grundsätzlich nur im Verhältnis zum Arbeitgeber. Im Verhältnis zu geschädigten Dritten besteht ein Freistellungsanspruch des Arbeitnehmers gegen den Arbeitgeber.

Für eine mögliche Strafbarkeit gilt dagegen der Grundsatz der vollständigen Eigenverantwortung. Ein Arbeitnehmer macht sich also selbst strafbar, die
arbeitsvertragliche Haftungserleichterung ist nicht anwendbar. Auch gilt kein Befehlsnotstand, so dass ein Mitarbeiter, der auf Anweisung seines Vorgesetzten handelt deswegen nicht gerechtfertigt ist.

Strafbarkeit ist möglich, etwa nach § 206 StGB oder nach BDSG:
- fahrlässige Verletzung: Ordnungswidrigkeit, bis 250.000 € Bußgeld
- bei Übermitteln/Abrufen gegen Entgelt oder Bereicherungs-/Schädigungsabsicht liegt eine Straftat vor

Nicht von der Haftungserleichterung erfasst sind auch die Sanktionen der Abmahnung oder Kündigung, welche bei Pflichtverstößen des Mitarbeiters stets eintreten können.

Zur Vermeidung von Eigenhaftung kann ein verantwortlicher Mitarbeiter nachfolgende Eigenschutzmaßnahmen ergreifen

- gewissenhafte Aufgabenerfüllung
- regelmäßige Information der Geschäftsleitung über mögliche Risiken
- Lösungsvorschläge für Sicherheitsmängel erarbeiten, Projekte vorschlagen, angemessenes Budget beantragen
- Hinzuziehung externer Berater

Reaktion der IT-Verantwortlichen bei Ablehnung der vorgeschlagenen Maßnahmen durch die Geschäftleitung

- Risiken erneut aufzeigen
- Ablehnung und eigenes Verhalten protokollieren und dokumentieren, etwa durch Besprechungsprotokolle oder schriftliche Fixierung in Briefen
- „Mitwisser schaffen oder E-Mail mit Cc
- schriftliche Bestätigung einfordern

Konsequenz → Verlagerung der Verantwortlichkeit auf die vorgesetzte Ebene

---

TMG-Haftung

Der Gesetzgeber unterscheidet im Telemediengesetz (TMG) zwischen eigenen und Fremdinhalten. Die gesetzliche Haftungssystematik bleibt allgemein und schablonenhaft, so dass sich die praktischen Fälle mit dem TMG allein nicht befriedigend lösen lassen. Eindeutig ist aber, dass ein Anbieter – wie z. B. ein Provider - für fremde Inhalte jedenfalls dann haftet, wenn er trotz Kenntnis bzw. trotz eindeutiger Hinweise nichts unternimmt. Im übrigen arbeitet die Rechtsprechung mit den geschilderten Verkehrssicherungspflichten. Diese lassen sich wie gesehen aus einer Vielzahl von gesetzlichen und vertraglichen Bestimmungen entnehmen.

Mobile Security

Szenario

Mobile Datenträger mit gewaltiger Kapazität, wie Laptop, USB-Sticks etc., gefährden durch Verlust oder Diebstahl die gespeicherten Daten. USB-Sticks sind aufgrund der U3-Technologie zu mobilen Micro-Plattformen geworden, die das Booten, die Installation von Software, Schnittstellen ins Internet oder den Betrieb von Webplattformen ermöglichen. Spezielle Anwendungen für USB-Sticks (Browser, E-Mail-Client, Webserver Apache) komplettieren die Gefährdungslage. Der Betrieb eines ebay-Shops aus der Hosentasche ist keine Utopie, sondern machbar. Mit dem Auslesen von Daten oder Einschleusen von Schadsoftware vom oder auf den USB-Stick muss jederzeit gerechnet werden. Somit ist das Potential für die Umgehung von Sicherheitspolicies durch mobile Datenträger enorm.

Ebenso gefährden unsichere Webportale oder alte Festplatten auf dem Müll, die nicht ordnungsgemäß entsorgt oder überschrieben wurden (DIN 32757), die gespeicherten Daten.

Abhilfe versprechen vor allem ganzheitliche Maßnahmen, bestehend aus einer Kombination aus Technik und juristisch-organisatorischen Lösungen.

Technische Schutzmaßnahmen

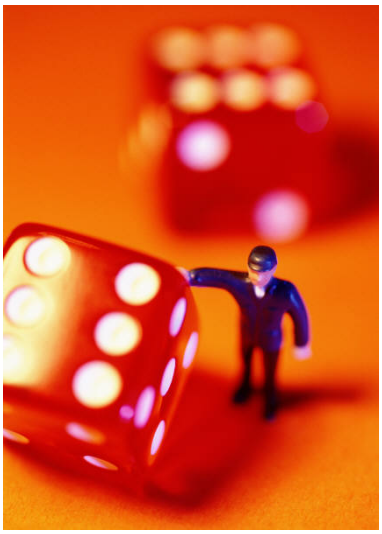
- device controle
- Verschlüsselung der Daten (oder integrierte Fingerabdruck-Scanner für USB-Sticks)
- zu beachten ist, dass Schnittstellenkontrollen als eine besondere Art der Protokollierung dem Datenschutz und der Mitbestimmung unterliegen

Nutzungsrichtlinien (Policy, Betriebsvereinbarung)

- keine Nutzung privater Datenträger (USB-Sticks) im Unternehmen
- keine Installation und Nutzung privater Software von externen Datenträgern
- Dienstliche Datenträger mit sensitiven (personenbezogenen) Daten
- sind im Unternehmen wegzuschließen
- bei Transport zu verschlüsseln
- dürfen nicht an externe Rechner angeschlossen werden
- Anschluss Datenträger (USB-Stick) nur an vorgesehene Rechner (z.B. Vortrags-Laptop)
- separater Datenträger (USB-Stick) für Anschluss an externe Rechner
- verantwortlich für die Einhaltung der Regeln ist der Mitarbeiter, dem der Datenträger überlassen wurde
- Androhung arbeitsrechtlicher Konsequenzen bei Verstoß
- die Regeln werden mit dem Datenträger (USB-Stick) ausgehändigt und gegebenenfalls abgezeichnet

Risikomanagement und IT-Compliance

Compliance, also die Einhaltung fremdgesetzter (gesetzlicher) und selbstgesetzter Standards (z.B. in der Policy), ist nicht nur ein Marketing-Schlagwort, sondern erfordert konkrete Maßnahmen.



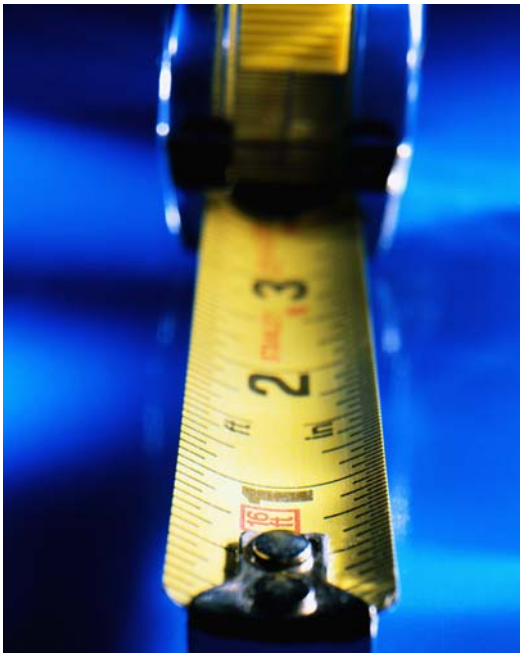
KonTraG - Haftung der Geschäftsleitung

Die Unternehmensleitung von Kapitalgesellschaften (AG, GmbH) hat für ein wirksames Risikomanagement-System zu sorgen. Im KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) schreibt der Gesetzgeber Sicherungsmaßnahmen vor, nach denen ein Überwachungssystem einzurichten ist, das bestandsgefährdende Entwicklungen frühzeitig erkennt. Dieses Frühwarnsystem erfordert u.a. eine präventive Überwachung und Erkennung von Fehlentwicklungen in der IT-Sicherheit. Auch das BSI verweist in seinen Standards ausdrücklich auf die Vorgaben des KonTraG (etwa im „Leitfaden IT-Sicherheit“).

- Eingriff des Gesetzgebers in die „Corporate Governance“ (=Führung und Überwachung) des Unternehmens
- Anwendungsbereich: mittlere und große AG, entsprechende Anwendung auf vergleichbar große GmbHs und Kapitalgesellschaften
- Zweck des KonTraG
    - Verpflichtung des Vorstands zu Risikomanagement
        - Risikomanagement = Risiko-Klassifizierung und -Controlling
    - Früherkennung von gefährlichen Schieflagen = Frühwarnsystem
        - präventive Überwachung und Erkennung von Fehlentwicklungen, z.B. Viren, illegale Inhalte, IT-Sicherheit
    - soll die Prüfung von Unternehmen erleichtern für Anleger und Wirtschaftsprüfer
- Organisations- und Sorgfaltspflichten des Vorstands nach § 91 Abs. 2 AktG →„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“
- nachteilige Folgen bei Verstößen:
    - Persönliche Haftung des Vorstands mit dem eigenen Vermögen
    - keine Entlastung des Vorstands: das LG München hat am 05.04.2007 entschieden, dass der Vorstand bei Verstößen gegen das Risikofrüherkennungssystem nicht entlastet werden darf

Anerkannte Standards und Zertifizierung

- Effektivster Schutz vor persönlicher Haftung und Organisationsverschulden
- Nachweis der geprüften Sicherheit nach außen, etwa für Anforderungen von externen Dritten:
    - Wirtschaftsprüfer (KonTraG)
    - Kreditgeber (Basel II), denn IT-Sicherheit ist Rating-Faktor im Rahmen von Basel II
    - Interne Revision
- Erwerb durch Audit eines zertifizierten Auditors



anerkannte Standards

- ISO/IEC 13335
    - allgemeine Leitlinie für die Initiierung und Umsetzung des IT-Sicherheitsmanagementprozesses
- ISO/IEC 17799
    - Rahmenwerk für das IT-Sicherheitsmanagement, kaum konkrete technische Hinweise, eine von mehreren Möglichkeiten, die Anforderungen des ISO-Standards 27001 zu erfüllen
- ISO/IEC 27001
    - der erste internationale Standard zum IT-Sicherheitsmanagement, der auch eine Zertifizierung ermöglicht, aber keine Hilfe für die praktische Umsetzung
- BSI-Standards zur IT-Sicherheit, IT-Sicherheitsmanagement
    - 100-1 Managementsystem für Informationssicherheit (ISMS)
    - 100-2 IT-Grundschutz-Vorgehensweise
    - 100-3 Risikoanalyse auf der Basis von IT-Grundschutz
    - 100-4 Notfallmanagement
    - ISO 27001 Zertifizierung auf der Basis von IT-Grunschutz

Basel II und die Rechtsfolgen

Am 26. Juni 2004 wurden die neuen Eigenkapitalanforderungen für Banken, kurz Basel II, am Sitz der Bank für internationalen Zahlungsausgleich unter dem Namen "International Convergence of Capital Measurement and Capital Standards: a Revised Framework" verabschiedet. Am 14. Juli 2004 hat die Europäische Kommission einen Richtlinienentwurf veröffentlicht, mit dem Basel II in Europa Gesetz wurde. Voraussichtlich Ende 2006/2007 treten die neuen Bestimmungen auch bei uns in Kraft.

- Basel II regelt die Kreditvergabe und die Kreditbedingungen
- gesetzlich noch nicht verbindlich, wird aber im Hinblick auf die baldige gesetzliche Umsetzung bereits heute allgemein beachtet und angewendet

Beherrschung der IT-Risiken gilt als wichtiger Rating-Faktor des Unternehmens im Rahmen der Kreditvergabe nach Basel II. Das BSI ausdrücklich in seinem Leitfaden IT-Sicherheit:

> *„Auch Banken sind inzwischen gezwungen, bei der Kreditvergabe IT-Risiken des Kreditnehmers zu berücksichtigen, was sich unmittelbar auf die angebotenen Konditionen auswirken wird (Stichwort: Basel II)“*

Ein hohes Sicherheitsniveau sowie ein effizientes Risiko- bzw. Sicherheitsmanagement-System, dass die Messung der verbleibenden Rest-Risiken erleichtert, führt zu einer reduzierten Eigenkapitalunterlegung bei den Kreditgebern (→ Banken müssen ihre vergebenen Kredite mit Eigenkapital als Sicherheit unterlegen)

- das vorhandene Sicherheitsniveau kann z. B. durch Zertifizierungen (etwa BSI-Grundschutz oder ISO 27001) dokumentiert werden
- allgemein anerkannt, dass im Rahmen der Ratingfaktoren „Risiko-Management, -Bewertung und –Controlling“ die IT-Riskien berücksichtigt werden
- insbesondere im Rahmen der operationellen Risiken von Unternehmen, welche die Eigenkapitalquote der Bank für die Kreditsicherung erhöhen
- was sich in einem erhöhten Zinssatz für den Kreditnehmer auswirkt

Aus der Sicht des Kreditgebers (Banken und Finanzdienstleister) hat Basel II noch weitreichendere Auswirkungen, umgesetzt in den sogenannten MaRisk
(= Mindestanforderungen an das Risikomanagement des BaFin vom 30.10.2007)
Die MaRisk schreiben verbindlich vor:

- IT-Sicherheit gehört zu den Adressausfallrisiken
- Gesamtverantwortung der Geschäftsleitung für Risikomanagement
- Internes Kontrollsystem (IKS)
    - Regelungen zur Aufbau- und Ablauforganisation
    - Einrichtung von Risikosteuerungs- und –controllingprozessen
- Organisationsrichtlinien
- Dokumentation
- technisch-organisatorische IT-Sicherheit
- gängige Standards wie BSI oder ISO sind zu beachten
- Test und Abnahme durch Verantwortliche
- Notfallkonzept
- Regelungen für Outsourcing

SOX-Compliance

In den letzten Jahren erfolgten weitreichende Eingriffe in die Corporate Governance von Kapitalgesellschaften durch amerikanische Gesetze, die zum Teil auch bei uns Auswirkungen haben.

- Sarbanes Oxley Act (SOX), US-Gesetz von 2002
- regelt persönliche Verantwortlichkeit und Haftung des Managements (insbes. CEO, CFO)

Anwendungsbereich – SOX gilt für…

- US-börsennotierte Unternehmen
- ausländische (also z.B. deutsche) Unternehmen, die an US-Börsen oder der NASDAQ gelistet sind
- ausländische (also z.B. deutsche) Töchter von US-Gesellschaften

Zweck von SOX:

- Verschärfung der Rechnungslegungsvorschriften in Folge gravierender Bilanzskandale (z.B. Enron oder Worldcom)
- Wiederherstellung des Vertrauens der Anleger
- Section 404 des SOX: Unternehmensprozesse und Kontrollverfahren müssen definiert und festgelegt werden, um das Risiko einer falschen Bilanz zu minimieren
- u.a. weitreichende Archivierungspflichten für E-Mail und elektronische Kommunikation

Section 404 fordert

- wirksames internes Kontrollsystem (IKS)
- IT hat im IKS über die Finanzberichterstattung hohen Stellenwert
- Datensicherheit und Backup
- Erfüllung der Compliance-Anforderungen
- Integration in operative Abläufe
- SOX bedeuted Regelbetrieb, also jährlich wiederkehrende Prüfung
- jährliche Bewertung durch eidesstattliche Versicherung (certification) des CEO und CFO
- Abschlussprüfer
- bewertet Vorgehen des Management
- eigene Stellungnahme zu IKS
- Offenlegungspflicht von Abschlussprüfer und Management bezüglich Fehler im IKS
- Dokumentationspflicht
- Berechtigungsvergabe und Transaktionsmonitoring
- Funktionstrennung, Schnittstellenüberwachung, allgemeine IT-Kontrollen
- Auswertungs- und Berichtsfunktionalitäten zwingend

Überwachung durch US-Behörden

- SEC = Securities and Exchange Commission = Börsenaufsicht in den USA
- PCAOB = Public Company Accounting Oversight Board = US-Aufsichtsbehörde für Wirtschaftsprüfer
- SEC und PCAOB veröffentlichen Leitfäden und Richtlinien für die Umsetzung von SOX

Euro-SOX

Als Reaktion auf Finanzskandale wie Parmalat oder Ahold hat die EU Regelungen ähnlich dem SOA in adaptierter Form eingeführt

- Richtlinie 2006/43/EG vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Anpassung der 8. EU-Prüferrichtlinie (umgesetzt durch Bilanzrechtsmodernisierungsgesetz, BilMoG)
- angestrebtes Ziel: Wirtschaftsprüfer werden verstärkt die Anforderungen an die IT-Sicherheit in den Unternehmen prüfen, weil sie selbst strengeren Kontrollen der Aufsichtsbehörden unterliegen
- Anwendungsbereich: Unternehmen des öffentlichen Interesses
    - börsennotierte Unternehmen
    - Banken, Versicherungen
    - Monopolunternehmen → Energieversorger, Post, Bahn etc.
- künftig höhere Anforderungen an das Interne Kontrollsystem (IKS)
- Prüfungsausschuss (Audit Committee)
    - dient der Zusammenarbeit zwischen Audit Committee und Wirtschaftsprüfer
    - Abschlussprüfer muss das Audit Committee insbesondere über wesentliche Schwachstellen im IKS informieren

NPSI - Nationaler Plan Schutz der Informationsinfrastrukturen

- Wirtschaft, Verwaltung und Gesellschaft sind auf ausfallsichere Informationstechnik angewiesen. Im Hinblick auf die deutliche Verschärfung der Gefährdungssituation aller IT-Infrastrukturen ist Informationssicherheit eine nationale Aufgabe. Dies erkannte bereits Ex-Innenminister Otto Schily und veranlasste deshalb einen „Nationalen Plan zum Schutz der Informationsinfrastrukturen".
- Das BSI in seinem „Bericht zur Lage der IT-Sicherheit":
    - Die Gefährdung von nationalen Informationsinfrastrukturen hat erheblich zugenommen
    - steigende Zahl von
        - Computerviren
        - Phishing- und Hacker-Angriffen
        - sowie die Zunahme IT-basierter Wirtschaftsspionage
    - Immer öfter nutzen kriminelle Banden und Täter aus dem Bereich der organisierten Kriminalität Nutznießer von Viren, Würmern oder Trojanischen Pferden für ihre kriminellen Aktivitäten/Straftaten.
- Der NPSI verfolgt drei strategische Ziele:
    - Prävention: Informationsinfrastrukturen in Deutschland angemessen schützen
    - Reaktion: Wirkungsvoll bei IT-Sicherheitsvorfällen handeln
    - Nachhaltigkeit: Deutsche IT-Sicherheitskompetenz stärken – international Standards setzen

Rechtskonformes SSL-Decryption

Die gleichzeitige gesetzliche Forderung nach Verschlüsselung auf der einen und Virenschutz auf der anderen Seite, etwa in Anlage zu § 9 BDSG, erzeugt einen technischen Widerspruch, da verschlüsselte Verbindungen nicht ohne weiteres auf Viren oder Malware untersucht werden können.

- Spannungsfeld zwischen Datenschutz und Systemschutz
- beides wesentliche Eckpfeiler zur Umsetzung der datenschutzrechtlichen Anforderungen
- https gewährleistet die Vertraulichkeit der übertragenen Daten
- Scannen der Verschlüsselung steht der Vertraulichkeit scheinbar entgegen, gewährleistet aber den vergleichbar wichtigen Virenschutz

Immer mehr Missbrauch und Malware erfolgt über https und erzeugt so ein Sicherheitsvakuum. Das technisch unbestritten notwendige https-Scanning muss datenschutzkonform betrieben werden.

Dies erfordert zunächst die Vermeidung von möglichen Straftatbeständen

- § 202a StGB Ausspähen von Daten
- § 206 StGB Bruch des Fernmelde-/Telekommunikationsgeheimnisses
- Ordnungswidrigkeit nach § 43 BDSG

Insbesondere darf der Scanvorgang nicht zur Kenntnisnahme der Inhalte führen, muss also in einer Blackbox ablaufen

Zulässigkeitsvoraussetzungen

- Anlass für das Scannen ist ein konkretes Gefährdungspotential, worunter in erster Linie der Virenschutz fällt, sowie Abwehr vergleichbarer Malware, sonstige Filtermaßnahmen sind kein ausreichender Anlass
- die Maßnahme muss erforderlich zur Gefahrenabwehr sein, z.B. um das Eindringen von Viren zu verhindern
- Möglichkeit zu optionalen Ausnahmen, besonders sensible https-Verbindungen, etwa Online-Banking, können vom Scanvorgang ausgenommen werden
- der Scanvorgang der Verschlüsselung, die Virenfilterung und das erneute Verschlüsseln müssen in einem geschlossenen System ablaufen
- Scanvorgang und Anti-Viren-Software arbeiten in einer Blackbox, führen also nicht zur Kenntnisnahme von Inhalten durch Administratoren oder sonstige Dritte

zusätzliche optionale Maßnahmen, welche die juristische Sicherheit erhöhen

- deutliche Hinweise gegenüber dem Nutzer vor dem Scanvorgang
- Einwilligung des Nutzers
  - schriftlich nach § 4a BDSG in Nutzungs- oder Betriebsvereinbarung
  - in elektronischer Form nach § 4 Abs. 2, 3 TDDSG, etwa durch Popup-Fenster

Best Practice-Beispiel

- Schutz des Berliner Landesnetzes vor Viren
- datenschutzrechtliche Abwägung des Landesdatenschutzbeauftragten (LDSB) Berlin fiel zugunsten des Virenschutzes und https-Scannings aus
- unter den dargestellten Voraussetzungen hatte der LDSB Berlin keine rechtlichen Bedenken geäußert und empfohlen, das https-Scan-Verfahren wieder einzusetzen

Mitarbeiterkontrolle versus Datenschutz – mit einem Bein im Gefängnis ?

Der Arbeitgeber hat ein vitales Interesse daran, dass private Surfen, Chatten oder Mailen am Arbeitsplatz sinnvoll zu begrenzen. Neben dem Verlust von Arbeitszeit und Bandbreite lauern hier vielfältige Haftungsrisiken. Die legale Kontrolle der Mitarbeiter, um Missbräuche einzuschränken, ist deshalb überall in den Unternehmen und Behörden ein Thema mit hoher Priorität.

Private Nutzung, Fernmeldegeheimnis

Bei Kontrollmaßnahmen stellt sich zunächst die Ausgangsfrage, ob der Arbeitgeber die private Nutzung erlaubt oder verboten hat. Bei erlaubter Privatnutzung wird der Arbeitgeber zum Telekommunikationsanbieter, da die Möglichkeit des Arbeitnehmers zur Privatnutzung von E-Mail und Internet als Dienstleistung ihm gegenüber einzustufen ist. Daraus resultiert die Geltung des Fernmeldegeheimnisses, da sich der Arbeitnehmer auf die Vertraulichkeit der privaten Kommunikation verlassen darf. Kontrollmaßnahmen unter dem Regime des Fernmeldegeheimnisses sind weitgehend unzulässig. Die reine „Erhebung“ von Daten zur technischen Datensicherheit, Notfallprävention, Störungsbeseitigung, Datenschutzkontrolle ist möglich. Die Auswertung dieser Daten ist dagegen nur ausnahmsweise nach § 88 TKG möglich…..

- zur Abrechnung, etwa der privaten Nutzung
- bei Gefahr im Verzug → z.B. akuter Virus
- bei Vorliegen einer Einwilligung aufgrund einer rechtfertigenden Nutzungsvereinbarung

Dienstliche Nutzung, unerlaubte Privatnutzung

Ist dagegen die Privatnutzung verboten und nur eine dienstliche Nutzung möglich, kommt das Fernmeldegeheimnis nicht zur Anwendung. Die dienstliche Nutzung steht dann jedoch unter dem Schutz des Bundesdatenschutzgesetzes (BDSG). Zwar sind hier weitergehende Kontrollen als unter dem Fernmeldegeheimnis möglich, trotzdem besteht kein schrankenloser Freibrief zur Einsicht in E-Mails oder Webinhalte. Eine Kontrolle der dienstlichen Nutzung ist nach den Vorgaben des BDSG nur zulässig, wenn aufgrund einer Güterabwägung nach dem Verhältnismäßigkeitsprinzip die Kontrollmaßnahme erforderlich und angemessen ist. In diese Gesamtabwägung der relevanten Belange sind alle beteiligten Interessen mit einzubeziehen. Daraus ergibt sich die grobe Faustformel, dass ….

- äußere Verbindungsdaten wie URL, Empfänger- oder Absenderadresse eingesehen werden dürfen,
- Inhaltskontrollen, wie das Mitlesen von E-Mails oder den Eintragungen des Arbeitnehmers auf den Webseiten, aber unzulässig sind.

Unterscheidet man nach den Hauptnutzungsarten, so ergibt sich für die dienstliche Nutzung im Überblick die nachfolgende Kontrollsituation…

Surfen im Internet

1. trotz Verbot der Privatnutzung keine unbeschränkte Kontrolle möglich
2. betroffen ist in erster Linie die Überwachung der Logfiles
3. Faustformel: kontrolliert werden können die besuchten URLs, Dauer des Surfens, Umfang der Downloads, nicht aber die auf den Seiten vorgenommene Eintragungen

Versendung von E-Mails

- vollständiges Verbot privater E-Mails von Arbeitnehmern anders als bei der Telefonnutzung möglich
- aber: private E-Mails können trotz Privatnutzungsverbot nicht vollständig verhindert werden, da auch ein Eingang von außen möglich, der vom Arbeitnehmer nicht beherrscht wird
- Faustformel: nur Kontrolle der Adressdaten zulässig, das ständige Mitlesen der E-Mails - wie in den USA üblich – ist nicht erlaubt
- denn es existiert ein gegenüber der Inhaltskontrolle milderes Mittel: die Herausgabe der geschäftlichen E-Mails durch den Arbeitnehmer an den Arbeitgeber

Interessensausgleich durch rechtliche Gestaltung

Unabhängig davon, ob Fernmeldegeheimnis oder Bundesdatenschutzgesetz gelten, bedeuten ungeregelte Zustände hinsichtlich der Mitarbeiterkontrolle einen ständigen rechtlichen Graubereich und Unsicherheit, da die Bestimmungen in TKG und BDSG unklar sind. Es herrscht große Verunsicherung bei Arbeitgeber, Administrator und Arbeitnehmer, da die notwendige Güterabwägung der beteiligten Interessen im Einzelfall alle Betroffenen überfordert. Das Datenschutzrecht eröffnet jedoch nach dem Grundsatz „präventives Verbot mit Erlaubnisvorbehalt“ einen Gestaltungsspielraum, um durch Vereinbarungen legale Handlungsgrundlagen zu schaffen. Nach dem Gesetzeswortlaut besteht zwar zunächst ein generelles Verbot, dass aber durch Vereinbarungen, die als Erlaubnisvorbehalt wirken, in Grenzen modifiziert werden kann. Solche Vereinbarungen bringen Vorteile für alle Beteiligten.

Im Überblick stellt sich die Situation bei der Mitarbeiterkontrolle wie folgt dar:

- präventives Verbot mit Erlaubnisvorbehalt → eröffnet Gestaltungsspielraum
- Vereinbarungen als legale Handlungsgrundlage entsprechen dem Wunsch des Gesetzgebers, solange ein klärendes Arbeitnehmerdatenschutzgesetz nicht exisitert
- klare Verhältnisse für Admin: keine illegale Kontrolle/keine Strafbarkeit wegen Verstoß gegen das Fernmeldegeheimnis
- Transparenz für Arbeitnehmer: schafft Vertrauen, hat aber auch Warnfunktion und damit Lenkungswirkung
- Haftungsprävention für den Arbeitgeber durch legale Kontrolle, da die Beaufsichtigung der Arbeitnehmer zur Erfüllung der Verkehrssicherungspflichten gehört

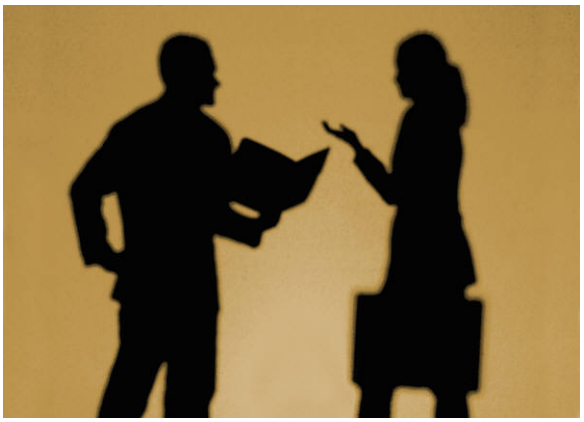
Mitbestimmung der Betriebs- und Personalräte

Da die Fragen der Mitarbeiterkontrolle der Mitbestimmungspflicht im Sinne des Betriebsverfassungsgesetzes unterliegen, müssen Betriebs-/Personalräte am Entscheidungsprozess in Form von Vereinbarungen beteiligt werden. Hier kommen insbesondere die Anpassung der Arbeitsverträge und der Abschluss von Betriebs-/Dienstvereinbarungen mit entsprechenden Nutzungs- und Kontrollregelungen für die E-Mail- und Internet-Nutzung in Betracht. Im Bereich Fernmeldegeheimnis, das auf ein Grundrecht zurückgeht, ist neben Kollektivvereinbarungen die individuelle Zustimmung der beteiligten Arbeitnehmer von Vorteil. Ergänzend zu entsprechenden Betriebs-/Dienstvereinbarung kann deshalb eine zusätzliche Legitimation und Information durch eine persönliche Zustimmung des betroffenen Arbeitnehmers erfolgen. Im Einzelnen ist die Situation wie folgt:

- Mitbestimmungsrechte des Betriebs-/Personalrates
- Anpassung der Arbeitsverträge
- Betriebs-/Dienstvereinbarung mit Nutzungsrichtlinien
- ergänzend: individuelle Zustimmung: dadurch zusätzliche Legitimation und Information (z.B. durch Verwendung als Info-Broschüre)

Betriebs- oder Dienstvereinbarungen

Bei der Betriebs-/Dienstvereinbarung handelt es sich um einen schriftlichen Vertrag zwischen Arbeitgeber und Mitarbeitervertretung, der zur Lösung des Kontroll- und Nutzungsproblems geschlossen wird. In Betrieben ab einer Größe von fünf Mitarbeitern sind Betriebsräte und damit Betriebsvereinbarungen möglich. Während der Arbeitgeber den Missbrauch einschränken will, befürchtet der Betriebsrat die Ausforschung der Arbeitnehmer. Die Betriebs-/Dienstvereinbarung hat rechtssetzenden Charakter und wirkt modifizierend auf die Inhalte der Arbeitsverträge ein.



Im Überblick gilt für die Betriebsvereinbarung:

- Zweck: Lösung gemeinsamer Probleme
- Internet/E-Mail-Nutzung durch Arbeitnehmer:
    - Arbeitgeber befürchtet Missbrauch
    - Mitarbeitervertretung befürchtet Ausforschung
- Mitbestimmungsrecht der Mitarbeitervertretung/ des Betriebsrates gemäß §87 Abs. 1 Nr. 1 und 6 BetrVG für die Bereiche:
    - Ordnung des Betriebes, Arbeitnehmer-Verhalten
    - technische Kontrolleinrichtungen
- schriftlicher Vertrag zwischen Arbeitgeber und Mitarbeitervertretung
- in Betrieben ab fünf Mitarbeitern, §1 BetrVG
- rechtssetzender Charakter, der den Arbeitsvertrag abändert
- endet durch Kündigung oder Fristablauf

Insbesondere die Missbrauchskontrolle und Abwesenheitsproblematik bedarf einer detaillierten Regelung. Zur inhaltlichen Gestaltung von Betriebs-/Dienstvereinbarung der nachfolgende Gesamtüberblick, wonach Regelungen zu folgenden Punkten enthalten sein sollten:

- Umfang einer erlaubten Privatnutzung, beispielsweise Beschränkungen nach Umgang, Dauer oder Art und Weise der E-Mail- und Internet-Nutzung
- verbotene Nutzungen, Aufzählung im Einzelnen, z.B. sexistisch, rechtsradikal, gewaltverherrlichend etc.
- welche Daten werden zur Kontrolle erfasst:
    - Protokollierung von E-Mail- und Internetaktivitäten
    - Gesamtdatenvolumen, etc.
- technische Einrichtungen, die optional der Kontrolle dienen:
    - Firewall, Proxy, Spamfilter etc.
    - Reporting-Tool URL-Filter
    - https-Scanning
- Monitoring-Funktionen, etc.
- Abwesenheitsregelung: Umgang mit der Mailbox im Falle von Urlaub, Krankheit, Kündigung etc.
- Kontrollprozedere: aus Gründen der Verhältnismäßigkeit, welche ständige personenbezogene Inhaltskontrollen verbietet, ist ein abgestuftes Kontrollverfahren erforderlich:
    - zunächst nur anonymisierte Stichprobenkontrolle
    - nur bei grobem Missbrauch oder Straftat: personenbezogene Kontrolle, möglichst unter Beteiligung des Betriebsrates/ Datenschutzbeauftragten nach dem Vier-Augen-Prinzip
- Regelung der Beteiligung von Betriebsrat, Datenschutzbeauftragter
- Löschungspflichten
- Konsequenzen bei Nichteinhaltung
- Kündigung, Evaluierung

Anhang

Checkliste

- Existiert ein Notfallszenario/Zuständigkeitsverteilung in Fällen wie Virenbefall, Plattencrash, Systemzusammenbruch?
- Haben die Anwender einen definierten Ansprechpartner beim Auftauchen gefährlicher oder illegaler Inhalte (Viren, Trojaner, mp3s etc.)?
- Haben sie eine datenschutzkonforme Abwesenheitsregelung (Krankheit, Urlaub, Kündigung) für den Fortbetrieb der Mailboxen?
- Haben Sie Spam/URL/Contentfilter im Einsatz?
- Haben Sie einen Spamfilter mit einer niedrigen false-positive-Rate?
- Hat der Enduser Zugriff auf die ausgefilterten Spam-Mails?
- Haben Sie eine rechtliche Gestaltung (Betriebsvereinbarung, Arbeitsvertrag), die den rechtssicheren Einsatz der Filtersysteme gewährleistet?
- Betreiben Sie ein datenschutzkonformes Lizenzmanagement?
- Haben Sie eine datenschutzkonforme Regelung zur Missbrauchskontrolle der Mitarbeiter getroffen?
- Sind die Passwörter am Monitor gepostet oder im Kollegenkreis bekanntgemacht?
- Kann jeder Mitarbeiter beliebige Software auf seinem PC installieren?
- Kann die Geschäftssoftware für den privaten Gebrauch kopiert werden?
- Gibt es Richtlinien zur Wahrung der Vertraulichkeit von Daten/E-Mails?
- Kann jeder Mitarbeiter auf alle vorhandenen Daten zugreifen?
- Wird die Virenschutzsoftware ständig und automatisiert upgedatet ?
- Wird ein brandschutzsicheres Backup-System betrieben?
- Sind die Firmen-Laptops in das Sicherheitskonzept integriert?
- Werden als Passwörter die Namen enger Angehöriger oder allgemeine Begriffe verwendet?
- Sind gefährliche Dateianhänge wie .exe, .bat, .vbs, etc. verboten?
- Wurden die Mitarbeiter/Innen durch Schulung in die Internet-Nutzung eingewiesen?
- Kommt eine Firewall zum Einsatz?
- Existiert eine Regelung zur Archivierung von E-Mails?
- Kann sichere Verschlüsselungstechnik für die externe und interne Kommunikation eingesetzt werden?
- Ist das Patchmanangement auf dem letzten Stand der Dinge?