

Juristische Information für

- *IT Administratoren,*
- *IT Verantwortliche,*
- *Personal- und Datenschutzbeauftragte*



Eine Informationsbroschüre mit praktischen Tipps zum richtigen Umgang mit dem vielschichtigen Thema IT-Sicherheit in Unternehmen

In Zusammenarbeit mit Rechtsanwalt Horst Speichert.

Inhaltsübersicht

Der Autor	3
Synopsis	4
Einleitung	6
Ganzheitliche Sicherheit – juristische Sicherheit	7
Mitarbeiterkontrolle versus Datenschutz – mit einem Bein im Gefängnis ?	8
Haftung des Unternehmens / der Geschäftsleitung	9
Archivierungspflichten – insbesondere für E-Mails	10
Empfehlungen für IT-Verantwortliche	21
Fax-Formular für Kontakt zu Websense bzw. RA Speichert	22

Der Autor



Horst Speichert (Email: horst@speichert.de) ist Rechtsanwalt in der **Kanzlei esb** in Stuttgart. Sein Spezialgebiet umfasst die Bereiche Neue Medien, EDV-Recht sowie IT-Vertragsgestaltung. Darüber hinaus fungiert Herr Speichert als Seminarleiter im Internetrecht, IT-Security und Datenschutz bei den professionellen Seminarveranstaltern.

Horst Speichert ist Autor des Fachbuchs „IT-Recht in der Praxis“, das im Vieweg-Verlag erschienen ist. Neben seiner Tätigkeit als Anwalt ist er Lehrbeauftragter an der Universität Stuttgart.

Internet: www.kanzlei.de



Synopsis

Netzwerke in Unternehmen unterliegen einer Vielzahl von Anforderungen, die in erster Linie auf die Optimierung von Geschäftsprozessen ausgerichtet sind. Daneben gibt es aber auch eine Reihe von (rechtlichen) Risiken, die auftreten, sobald Mitarbeiter bzw. Netzwerke in das Internet eingebunden werden. Die Risiken werden nachfolgend detaillierter beschrieben.

Websense als globaler Marktführer im Bereich URL-Filtering und Internet-Security gibt IT-Verantwortlichen geeignete Instrumente zur Hand, um die Ausführung für Unternehmen wichtiger geschäftlicher Prozesse optimal sicherzustellen und Missbräuche jeglicher Art, sei es durch externe Personen und Organisationen oder aber eigene Mitarbeiter, frühzeitig zu unterbinden.

Die Nutzung des „Kommunikationsnetzwerkes“ Internet ist heute - insbesondere im Zeichen stark fortschreitender Globalisierung von Unternehmen und Märkten - eine unbedingte Voraussetzung für alle erfolgsorientierten Unternehmen.

In gleichem Maße aber, wie sich die Anzahl der Internetanwender erhöht, entstehen immer neue Risiken mit nachhaltigsten Auswirkungen. Daher sind Unternehmen heute mehr denn je gefordert, ohne Einschränkung des firmenrelevanten Nutzens alle durch das Internet entstehenden Gefahren frühzeitig zu erkennen und nachhaltig auszuschalten.

Ein weit unterschätztes Risiko ist zum Beispiel das illegale Herunterladen und Verbreiten kopiergeschützter Musik und Filme. Viele Mitarbeiter sehen dies auch heute noch als Kavaliersdelikt und werden somit zum Haftungsrisiko für Unternehmen, die entsprechende Downloads wissentlich dulden und nicht unterbinden. *„In solchen Fällen verletzen Unternehmen, also die jeweiligen Geschäftsleitungen ihre Organisationspflicht“*, erklärt Anwalt Horst Speichert von der Kanzlei e/s/b Rechtsanwälte in Stuttgart. *„Außerdem verstoßen sie gegen das Urheberrecht und können auf Unterlassung verklagt werden.“* Das Strafmaß kann dabei unterschiedlich ausfallen:

Problem	Haftungsrisiko	Strafrahmen bis
Mitarbeiter dürfen ohne Richtlinien eigene Software installieren, schleppen Viren oder trojanische Pferde ein	§ 43 BDSG	1 Jahr

Quelle: www.kanzlei.de/risiko.htm

Synopsis

Problem	Haftungsrisiko	Strafrahmen bis
Mitarbeiter sendet strafbare bzw. illegale Inhalte	§ 184 Abs. 3 StGB Verbreitung harter Pornographie	3 Jahre
	§ 184 Abs. 3 StGB Verbreitung von Kinderpornographie	bis zu 5 Jahren
	§ 86 StGB Verbreiten von Propagandamitteln verfassungswidriger Organisationen	3 Jahre
Mitarbeiter bricht in fremde Unternehmensnetze ein, installiert trojanische Pferde, schießt fremde Rechner ab	§ 202a StGB Ausspähen von Daten	3 Jahre
	§ 303a StGB Datenveränderung	2 Jahre
	§ 303b Datensabotage	5 Jahre
Mitarbeiter nutzt kostenpflichtige Seiten kostenlos mit geknackten Paßworten	§ 263a StGB Computerbetrug	5 Jahre
Kinderpornographie auf Firmenrechnern	§ 184c Abs. 5 StGB	1 Jahr

Quelle: www.kanzlei.de/risiko.htm

Die Gefahr, dass Mitarbeiter ihre Arbeitszeit mißbrauchen und illegale Inhalte downloaden und verbreiten, ist nicht zu unterschätzen. Zeit dafür hätten sie allemal: Laut Marktforscher IDC sind 30 bis 40% der Mitarbeiter-Ausflüge ins Internet nicht arbeitsrelevant. Der einschlägige Content-Provider Sextracker berichtet sogar, dass rund 70% der Zugriffe auf seine Porno-Seiten während der regulären Arbeitszeit (9 bis 17 Uhr) erfolgen. Auch die Statistik des Online-Aktienhandels bei Charles Schwab belegt, dass 92% der Aufträge während der Arbeitszeit eingehen.

Speichert unterstreicht: *„Jedes Unternehmens ohne klar definierte Internet- oder PC-Nutzungsrichtlinien verletzt grundsätzliche Sorgfaltspflichten in der Bereitstellung eines rechtlich einwandfreien Internetzugangs und ist damit voll haftbar, wenn Mitarbeiter, Auszubildende, Praktikanten oder auch freie Mitarbeiter nicht-lizenzierte Software einsetzen oder kopiergeschützte Inhalte über das Web austauschen.“*

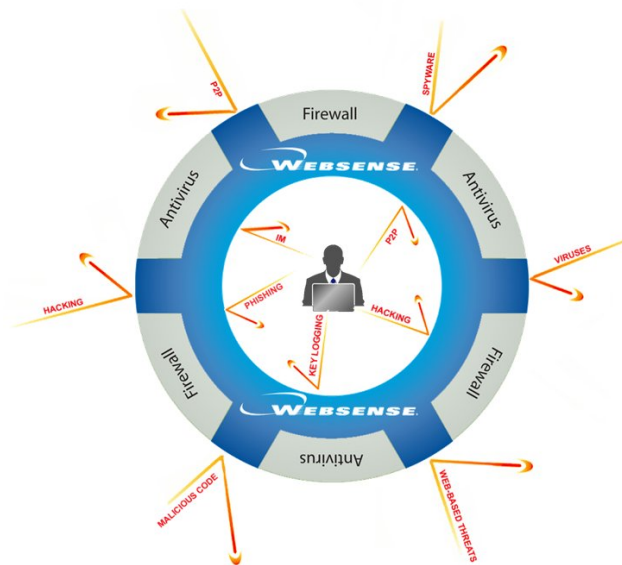
Einleitung

Bekanntermaßen lauern im Zusammenhang mit der Internetnutzung am Arbeitsplatz vielfältige Haftungsrisiken. Die Verantwortlichen stehen vor dem Problem, inwieweit illegale Vorgänge und Inhalte durch Mitarbeiter zur Mitverantwortung des Unternehmens bzw. der Geschäftsleitung führen. Das private Surfen oder Mailen ist auf ein risikoloses Maß zu begrenzen. Die obergerichtlichen Rechtsprechung arbeitet mit einer Haftungssystematik, wonach die Erfüllung von Verkehrssicherungspflichten, bestehend aus betrieblichen Organisationspflichten und Aufsichtsmaßnahmen gegenüber den Arbeitnehmern, erforderlich sind. Überall in den Unternehmen und Behörden werden deshalb datenschutzkonforme Kontrollmaßnahmen, um Missbräuche einzudämmen, verstärkt thematisiert. Im gewerblichen Bereich wird eine zuverlässige, zeitnahe und umfassende Sicherung der IT-Systeme gefordert. Umgesetzt werden die Pflichten durch ein ganzheitliches Bündel von Maßnahmen, bestehend aus Technik, Nutzungsrichtlinien und rechtlicher Gestaltung. Ansonsten können betriebliche Missstände, wie raupkopierte Software oder der strafbare Download von MP3-Files aus Peer-to-peer-Netzwerken nach der aktuellen Rechtsprechung zur Mithaftung im Unternehmen führen.

Die Unternehmensleitung von Kapitalgesellschaften hat ein effektives Risikomanagement zu gewährleisten. Der Gesetzgeber schreibt im KonTraG Sicherungsmaßnahmen vor, wonach ein Überwachungssystem einzurichten ist, um bestandsgefährdende Entwicklungen früh zu erkennen. Die präventive Überwachung und Erkennung von Fehlentwicklungen in der IT-Sicherheit ist im Rahmen dieses Frühwarnsystems erforderlich und wird neuerdings auch explizit im „Leitfaden IT-Sicherheit“ des BSI verankert.

Ganzheitliche Sicherheit – juristische Sicherheit

IT-Sicherheit wird bisher vorwiegend von der Technik dominiert. Sie benötigt aber einen rechtlich-organisatorischen Rahmen. Denn es handelt sich um eine ganzheitliche Disziplin, deren technische, organisatorische und rechtliche Komponenten in enger Wechselbeziehung miteinander verzahnt sind. Die technische Sicherheit steht nicht alleine, sondern 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, das durch die Unternehmensleitung zu gewährleisten ist. Insgesamt ergibt sich eine Pflichtenstruktur, die aus einem Bündel von Maßnahmen besteht.



Diese Ganzheitlichkeit wird allenthalben deutlich: Weite Teile der technischen IT-Sicherheit stehen in Deutschland unter dem Vorbehalt der Mitbestimmungsrechte des Betriebsrates. Denn Geräte, die technisch IT-Sicherheit bieten eignen sich meist auch für die Kontrolle der Mitarbeiter. Am besten lässt sich dieser Tatbestand an einem Beispiel verdeutlichen: Spätestens wenn der Betriebsrat sich gegen den Einsatz von Sicherheitstechnik sperrt, wird deutlich, dass die technische Komponente nicht alleine steht, sondern in ein juristisches Regelwerk eingebunden ist. Ebenso ist für die Vermeidung von Haftungsansprüchen und Schadensersatz nicht allein der Einsatz von Technik ausreichend. Hier sind insbesondere organisatorische Maßnahmen wie die Erstellung und Umsetzung von Nutzungsrichtlinien sowie die Schulung und Beaufsichtigung gegenüber Mitarbeitern erforderlich. Auch hier wird offensichtlich wie eng Technik, Organisation und Recht verzahnt sind.

Mitarbeiterkontrolle versus Datenschutz – mit einem Bein im Gefängnis ?

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

Bei Kontrollmaßnahmen stellt sich zunächst die Ausgangsfrage, ob der Arbeitgeber die private Nutzung des Internet 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. Datenerhebungen sind nur ausnahmsweise nach § 89 TKG möglich. In Frage kommen sie allenfalls in Bezug auf:

- Abrechnungsdaten
- Gewährleistung eines sicheren und störungsfreien Ablaufs
- „Erhebung“ zur technischen Datensicherheit, Notfallprävention, Störungsbeseitigung, Datenschutzkontrolle
- Gefahr im Verzug, beispielsweise durch einen akuten Virus

Ist dagegen die Privatnutzung verboten und nur eine **dienstliche Nutzung** des Internet 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 Web-Inhalte. 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 Eintragungen des Arbeitnehmers auf Web-Seiten, aber unzulässig sind

Mitarbeiterkontrolle versus Datenschutz – mit einem Bein im Gefängnis ?

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

Surfen im Internet

- Betroffen ist in erster Linie die Überwachung der Logfiles
- Trotz Verbot der Privatnutzung keine unbeschränkte Kontrolle möglich

Faustformel: kontrolliert werden können die besuchten URLs, Dauer des Surfens, Umfang der Downloads, nicht aber die auf den Seiten vorgenommene Eintragungen

Versenden 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 ist, der vom Arbeitnehmer nicht beherrscht wird

Faustformel: nur Adressdaten-Kontrolle zulässig; das ständige Mitlesen der E-Mails – wie in den USA – ist nicht erlaubt, denn es existiert ein gegenüber der Inhaltskontrolle milderer Mittel – nämlich die Herausgabe der geschäftlichen E-Mails durch den Arbeitnehmer an den Arbeitgeber

Interessenausgleich durch rechtliche Gestaltung

Unabhängig davon, ob Fernmeldegeheimnis oder Bundesdatenschutzgesetz gelten, bedeuten unregelmäßige Zustände hinsichtlich der Mitarbeiterkontrolle einen ständigen **rechtlichen Graubereich** und Unsicherheit, da die Bestimmungen in TKG und BDSG schwammig 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.

Mitarbeiterkontrolle versus Datenschutz – mit einem Bein im Gefängnis ?

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

- Ungeregelte Zustände: ständiger Graubereich, da Datenschutzrecht zu schwammig, Verunsicherung bei Arbeitgeber, Administrator und Arbeitnehmer
- Präventives Verbot mit Erlaubnisvorbehalt eröffnet Gestaltungsspielraum
- Vereinbarungen als legale Handlungsgrundlage entsprechen dem Wunsch des Gesetzgebers, solange ein klärendes Arbeitnehmerdatenschutzgesetz nicht existiert

Vorteile für alle Beteiligten:

- Klare Verhältnisse für Administratoren: 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 Verkehrssicherungs-pflichten gehört

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- & 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 (zum Beispiel durch Verwendung als Infobroschüre)

Mitarbeiterkontrolle versus Datenschutz – mit einem Bein im Gefängnis ?

Betriebs-/Dienstvereinbarung

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, Arbeitnehmersverhalten
 - 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

Mitarbeiterkontrolle versus Datenschutz – mit einem Bein im Gefängnis ?

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 – zum Beispiel sexistisch, rechtsradikal, gewaltverherrlichend und mehr
- Welche Daten werden zur Kontrolle erfasst:
 - Protokollierung von E-Mail- und Internetaktivitäten
 - Gesamtdatenvolumen etc.
- Technische Einrichtungen, die optional der Kontrolle dienen:
 - Firewall, Proxy, Spamfilter und andere
 - Reporting-Tool URL-Filter
- Monitoring-Funktionen etc.
- Abwesenheitsregelung: Umgang mit der Mailbox im Falle von Urlaub, Krankheit, Kündigung usw.
- 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, Datenschutzbeauftragtem
- Löschungspflichten
- Konsequenzen bei Nichteinhaltung
- Kündigung, Evaluierung

Haftung des Unternehmens / der Geschäftsleitung

In den Unternehmen und Behörden müssen sich die Verantwortlichen verstärkt fragen, inwieweit illegale Vorgänge und Inhalte im Firmennetz zur Mitverantwortung des Arbeitgebers oder der Geschäftsleitung führen können. Zum einführenden Verständnis in die Haftungssystematik sollte man sich zunächst die obergerichtliche Rechtsprechung zu den Verkehrssicherungspflichten sowie die Vorgaben des KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) für ein verbindliches Risikomanagement deutlich machen.

Verkehrssicherungspflichten

- 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 der betrieblichen 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
- Rechtsfolgen:
 - Bei Verstoß gegen die Pflichten: Verschulden, Schadensersatz und möglicherweise Strafbarkeit
 - Bei Erfüllung der Pflichten: präventive Haftungsfreizeichnung, denn für Schäden, die trotz Pflichterfüllung eintreten, wird nicht gehaftet
- Auch die vertraglichen Schutzpflichten orientieren sich an den Verkehrssicherungspflichten

Überträgt man diese Systematik auf die spezielle Situation in der IT, so ergibt sich das nachfolgende **Haftungsszenario**:

- Download von Mitarbeitern zum Beispiel: Raupkopien, illegale mp3-Files, mögliche Mitverantwortlichkeit für illegale oder strafbare Inhalte
- Eintrag von außen beispielsweise in Gästebücher oder Foren: Gefahr illegaler Inhalte wie Beleidigungen, Obszönitäten, Marken- oder Urheberrechtsverletzungen und mehr
- Webspaces für Dritte: ebenfalls Gefahr, dass die ge-hosteten Inhalte illegal sind
- Minderjährige Azubis: Verstoß gegen Jugendschutz, der Arbeitgeber hat hier eine Garantenstellung

Haftung des Unternehmens / der Geschäftsleitung

- Schutz des Persönlichkeitsrechts am Arbeitsplatz: vor Belästigung, Beleidigung etwa durch Spams oder E-Mail-Anhänge, konkretisiert zum Beispiel im Beschäftigtenschutzgesetz (BeschSG)
- Viren und Spams in Kombination mit Hackerangriffen: Verletzung von...
- Eigentum und Gewerbebetrieb durch Datenbeschädigung oder -verlust
- Persönlichkeitsrecht, wenn beispielsweise ein Virus personenbezogene Daten ausspioniert und versendet
- Verlust von Arbeitszeit/Produktivität und Bandbreite

Gesetzliche Haftung

Die Aussagen des Gesetzgebers im Teledienstgesetz beschränken sich auf notwendige technische Privilegierungen und die Unterscheidung zwischen eigenen und fremden Inhalten. Voraussetzung der Haftung für Fremdinhalte ist die Kenntnis des Anbieters von der Existenz der Inhalte.

Die gesetzliche Haftungssystematik bleibt allgemein und schablonenhaft, so dass sich die praktischen Fälle mit dem Teledienstgesetz allein nicht befriedigend lösen lassen. Klar ist aber, dass ein Anbieter – wie ein Provider – für fremde Inhalte haftet, wenn er trotz Kenntnis eindeutiger Hinweise nichts unternimmt. Im übrigen arbeitet die Rechtsprechung mit den geschilderten Verkehrssicherungspflichten.

Diese lassen sich auch einer Reihe von gesetzlichen Bestimmungen entnehmen:

- § 25a Abs. 1 Nr. 2 KWG: Kredit- und Finanzinstitute müssen über angemessene Sicherheitsvorkehrungen für die Datenverarbeitung verfügen
- § 203 StGB: statuiert Verschwiegenheitspflichten und eine strafbewährte Garantenstellung für besonders sensible Daten
- Vorgaben der Finanzbehörden nach der GoBS: Risiken für die steuerlich relevanten Datenbestände sind zu vermeiden
- § 9 BDSG plus Anlage: es ist sicherzustellen, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben

Die konkretisierenden Normen werden von der Rechtsprechung als Maßstab für die angemessenen Sicherungserwartungen herangezogen.

Haftung des Unternehmens / der Geschäftsleitung

Der **Umfang der Verkehrssicherungspflichten** bestimmt sich insbesondere nach...

- Sicherheitserwartungen der beteiligten Verkehrskreise
- Marktüblichkeit der Sicherheits-Hardware und –Software beispielsweise hinsichtlich der notwendigen Update-Intervalle eines Virens scanners
- Quantität der Datenverarbeitung
- Gefährlichkeit des Tuns
- Prinzip der Verhältnismäßigkeit, also der Erforderlichkeit und Angemessenheit von Maßnahmen
- Wirtschaftlicher Zumutbarkeit, also 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 raupkopierte Software oder der strafbare Download von mp3-Files aus Peer-to-Peer-Netzwerken (P2P) 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: Bündel aus technischen, organisatorischen und rechtlichen Maßnahmen
- Technisch: aktueller Virenschutz, URL-Filter (Warnbildschirm), Content-, Spam-Filter und mehr
- Organisatorisch: Zuständigkeits-, Verantwortlichkeitsverteilung, Policy, Nutzungsrichtlinien, Überwachung der Beschäftigten, Meldestelle etc.
- Rechtliche Gestaltung: Betriebs-/Dienstvereinbarung, Steuerung durch Verträge, Service Level Agreements (SLAs), AGB etc.
- Transparenz der Regeln: erzeugt Vertrauen und dient als Warnfunktion mit Lenkungswirkung

Risikomanagement

Die Unternehmensleitung der Kapitalgesellschaften hat ein wirksames Risikomanagementsystem einzurichten. Im **KonTraG** schreibt der Gesetzgeber Sicherungsmaßnahmen vor. Danach ist ein Überwachungssystem einzurichten, das bestandsgefährdende Entwicklungen in der Gesellschaft früh erkennt. Dieses Frühwarnsystem erfordert unter anderem eine präventive Überwachung und Erkennung von Fehlentwicklungen in der IT-Sicherheit.

Haftung des Unternehmens / der Geschäftsleitung

Im „Leitfaden IT-Sicherheit“ des zuständigen Bundesamtes BSI wird nun auf die Vorgaben des **KonTraG** explizit verwiesen.

- KonTraG: Gesetz zur Kontrolle und Transparenz im Unternehmensbereich vom 27.04.1998
- Zweck:
 - soll Prüfung von Unternehmen erleichtern – Früherkennung von Schieflagen
 - Verpflichtung des Vorstands zu Risikomanagement soll betont werden
- 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.“
- Frühwarnsystem: präventive Überwachung und Erkennung von Fehlentwicklungen, z.B. IT-Security
- Risikomanagement: Klassifizierung und Risiko-Controlling
- Persönliche Haftung des Vorstands
- Anwendungsbereich: mittlere und große AG, entsprechende Anwendung auf vergleichbar große GmbHs
- Eingriff des Gesetzgebers in die „Corporate Governance“ (= Führung und Überwachung) des Unternehmens

Zertifizierung

Den effektivsten Schutz vor persönlicher Haftung und Organisationsverschulden bieten Zertifizierungen, die Sicherheit belegbar machen.

- 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**
- Standards:
 - ISO 17799, BS 7799
 - IT-Grundschutz des BSI
- Erwerb durch Audit eines zertifizierten Auditors

Archivierungspflichten – insbesondere für E-Mails

Die Umstellung auf die elektronischen Kommunikationsformen sollte nicht darüber hinwegtäuschen, dass die umfangreichen gesetzlichen Archivierungspflichten auch für den E-Mail-Verkehr gelten. In Unternehmen und Behörden muss auf breiter Front Datensicherung betrieben werden. Dabei verursachen Storage und Backup-Systeme erhebliche Kosten. Auch unter dem Gesichtspunkt der Kostenvermeidung sind deshalb die umfangreichen Aufbewahrungspflichten insbesondere aus dem Handels- und Steuerrecht zu beachten.

Handelsrecht

- Jeder Kaufmann (GbR, GmbH, AG) hat nach § 257 Abs. 1 HGB die Pflicht zur geordneten Aufbewahrung von geschäftlichen Unterlagen
- Hierzu gehören Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Konzernabschlüsse, Konzernlageberichte sowie die erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen, empfangene und versandte Handelsbriefe, Buchungsbelege
- Dabei ist der Begriff des Handelsgeschäft nach der Rechtsprechung des BGH weit definiert. Es genügt ein entfernter, lockerer Zusammenhang mit betrieblichen Interessen zum Beispiel Angebot, Annahme, Auftragsbestätigung, Mängelrüge, Arbeitsverträge, Bau von Gebäuden usw.
- Nicht umfasst sind lediglich reine Privatgeschäfte des Kaufmannes

Zur Vereinfachung sollte die **gesamte** Geschäftskorrespondenz als aufbewahrungspflichtig eingestuft werden.

Die vorsätzliche Verletzung von gesetzlichen Aufbewahrungsfristen ist gemäß § 283 b Abs. 1 Nr. 2 StGB – sofern Zahlungseinstellung oder Insolvenz vorliegen – mit Geldstrafe oder Freiheitsstrafe bis zu zwei Jahren bedroht. Bei Überschuldung oder Zahlungsunfähigkeit trifft eine Strafbarkeit nach § 283 Abs. 1 Nr. 6 StGB zu.

Es können die nachfolgenden Datenträger zur Archivierung eingesetzt werden:

- Bild- oder Datenträger – § 257 Abs. 3 HGB
- Ausnahme: Eröffnungsbilanzen, Jahresabschlüsse, Konzernabschlüsse
- Ein Wechsel des Mediums – etwa von Papier auf digital – ist möglich

Generell ist dabei sicherzustellen:

- die Übereinstimmung mit dem Original
- die jederzeitige Verfügbarkeit und Lesbarkeit

Archivierungspflichten – insbesondere für E-Mails

Es gelten die folgenden Aufbewahrungsfristen:

- Handelsbriefe – **6 Jahre lang**, § 257 Abs. 4 HGB
- Im übrigen (Handelsbücher, Bilanzen, Lageberichte, Buchungsbelege usw.) – **10 Jahre lang**, § 257 Abs. 1 Nr. 1 und 4 HGB
- Fristbeginn: erst am Ende des Jahres, § 257 Abs. 5 HGB
- Die steuerrechtlichen Aufbewahrungsfristen bleiben unberührt

Steuerrecht

Daneben gelten steuerliche Aufbewahrungspflichten

- Bezüglich sämtlicher kaufmännische Unterlagen (siehe von oben)
- Sonstiger Unterlagen soweit sie für die Besteuerung bedeutsam sind, § 147 Abs. 1 AO

Bei Verletzung der Archivierungspflichten, liegt keine ordnungsgemäße Buchführung vor und es erfolgt zumindest eine ungünstige **Schätzung** der Besteuerungsgrundlagen, § 162 AO, sofern nicht sogar der Verdacht der Steuerhinterziehung entsteht.

Auch hier können die nachfolgenden Datenträger zur Archivierung eingesetzt werden:

- Es gelten die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) des Bundesfinanzministeriums vom 07.11.1995
- Danach ist keine bestimmte Technologie vorgeschrieben, möglich sind:
 - Bildträger (Mikrofilm, Fotokopie), COM (?)
 - Maschinenlesbare Datenträger (Disketten, Magnetbänder, elektrooptische Speichermedien)
 - Dokumenten-Managementsysteme
 - Digitale Datenträger (CD-Rom, DVD), § 147 Abs. 2 AO
 - Ausnahme: Eröffnungsbilanzen, Jahresabschlüsse

Dabei ist sicherzustellen:

- Die Unveränderlichkeit, § 146 Abs. 4 AO
- Das Vorliegen systematischer Verzeichnisse
- Ein internes Kontrollsystem

Archivierungspflichten – insbesondere für E-Mails

Für den **Behördenzugriff** ist sicherzustellen:

- Die jederzeitige Verfügbarkeit und Lesbarkeit, § 147 Abs. 5 AO
- Es besteht: Vorlagepflicht des Steuerpflichtigen auf Verlangen der Behörde
- Kostentragungspflicht des Steuerpflichtigen
- Außenprüfung durch Behörde möglich, Einsichtnahme im System des Steuerpflichtigen: nur Lesezugriff, keine Fernabfrage (Online-Zugriff)
- Es gelten: die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), am 16.07.2001 vom Bundesfinanzministerium erlassen, <http://www.aufbewahrungspflicht.de/edfs/gdpdu.pdf>

Ein Vorsteuerabzug ist auch bei elektronischen Rechnungen mit qualifizierter Signatur möglich.

Es gelten die folgenden Aufbewahrungsfristen:

- Handels- oder Geschäftsbriefe sowie alle sonstigen Unterlagen, soweit für die Besteuerung bedeutsam – 6 Jahre lang, § 147 Abs. 3 AO
- Bücher, Jahresabschlüsse, Buchungsbelege etc. – 10 Jahre lang
- Ablaufhemmung: die Frist läuft nicht ab, so lange die Unterlagen für die Besteuerung von Bedeutung sind, 147 Abs. 3 Satz 3 AO
- Kürzere Aufbewahrungsfristen nach HGB bleiben unberührt, § 147 Abs. 3 Satz 2 AO

Es gilt also: die Fristen nach Steuer- und Handelsrecht stehen unberührt nebeneinander, so dass die längere einzuhalten ist.

Archivierungspflichten – insbesondere für E-Mails

Andere Vorschriften

Neben Handels- und Steuerrecht existieren eine ganze Reihe weiterer Aufbewahrungspflichten:

- Alle gesetzlichen Bestimmungen, die Ansprüche auf Auskunft und Rechnungslegung gewähren – so etwa §§ 259, 666, 667 BGB
- Vorlegungspflichten und Beweislast im Prozess
- Bei Verletzung, nach § 444 ZPO wird ohne Beweisverfahren der vom Gegner behauptete Vortrag als bewiesen angesehen, OLG Düsseldorf
- Bei Verletzung von Aufbewahrungspflichten droht Prozessverlust
- Bei Fristsetzung des Gerichts, muss rechtzeitiger Zugriff auf Archivdaten gewährleistet sein, ansonsten droht Ausschluss des Vortragsrechts (Präklusion)
- Ordentliche Geschäftsführung erfordert: grundsätzliche Aufbewahrungs- und Archivierungspflicht – etwa die gesamte E-Mail-Korrespondenz, Protokolle von Meetings, Entwürfe und Notizen aller Art etc. – die im Streitfall gebraucht werden könnten

Fragenkatalog für IT-Verantwortliche in Unternehmen

Die nachfolgend aufgeführten Fragen* sollen IT-Verantwortlichen helfen, effektive Regelungen zu treffen, um rechtliche Klarheit zu schaffen und die Sicherheit der Mitarbeiter, der Daten und des Netzwerks zu gewährleisten.

Prüfung der vorhandenen IT-Systeme auf...

- Kompatibilität zu den Geschäftsprozessen des Unternehmens:
 - Sind vorhandene technische Ressourcen ausreichend dimensioniert?
 - Unterstützen die IT-Ressourcen den Geschäftsbetrieb eher gut oder schlecht?
- Krisenfestigkeit:
 - Welche Art von Störungen sind existenzbedrohend für das Unternehmen?
 - Existieren getestete Notfallpläne für den Fall solcher Störungen?
 - Gibt es klare Abwesenheitsregelungen (bei Krankheit, Urlaub, Kündigung)?
- rechtliche Konformität / Compliance:
 - Wurden IT-Systeme vor der Implementierung durch Betriebsvereinbarungen bzw. Richtlinien an die Mitarbeiter kommuniziert, wo dies das Gesetz verlangt?
 - Wer trägt die Verantwortung für gesetzeswidrigen Einsatz / Missbrauch?
 - Gibt es neben Richtlinien in Papierform auch Automatisierungs-Mechanismen, um unakzeptablen Risiken ganz aus dem Weg zu gehen?

Was passiert, wenn es im täglichen Betrieb...

- zu einem Viren-Ausbruch kommt: Wie lange dauert es, bis alle PCs mit den neuesten Signaturen aktualisiert sind (Minuten / Stunden / Tage)?
- zum Bekanntwerden einer Verwundbarkeit von Systemen kommt: Wie lange dauert die routine-mässige Aktualisierung aller PCs mit neuen Patches?

Wie stellen Sie sicher, dass...

- Mitarbeiter potenziell gefährliche Dateianhänge nicht öffnen können?
- der Einsatz nicht-lizensierter Software verhindert wird?
- Laptops auch ausserhalb des Netzwerks vor Gefahren sicher sind?
- illegale Inhalte nicht ins Netzwerk bzw. auf Desktops gelangen?
- die private Nutzung oder der Missbrauch von IT-Systemen nicht die Leistungsfähigkeit von unternehmenskritischen Anwendungen beeinflusst?
- einmal definierte Richtlinien analog zur Entwicklung der technischen Systeme überprüft und angepasst werden?

* Erstellt in Zusammenarbeit von Websense mit Rechtsanwalt Horst Speichert

Fax-Formular für Kontakt zu Websense bzw. RA Speichert*Fax-Nr. 0049 (221) 5694 354*

Firma:

Name:

Position:

Telefon:

Email:

Kommentar:

Bitte: Rückruf zum Thema

 Audit meiner IT-Systeme

 Rechtliche Beratung zu

Websense Deutschland GmbH
Kaiser-Wilhelm-Ring 27-29
50672 Köln

(C) 2005 Websense. Alle Rechte vorbehalten. NP33-WPLEGALGR R.06.05