§ §

Rechtslage in der IT-Security: IT-Verantwortliche – mit einem Bein im Gefängnis ?

RA Horst Speichert

Horst Speichert

e|s|b Rechtsanwälte Stuttgart

Rechtsanwalt
Lehrbeauftragter
Universität Stuttgart

horst@speichert.de
www.kanzlei.de

EDV- und Internet-Recht
Security-Policies
Datenschutz
IT-Vertragsgestaltung
Outsourcing

Literaturhinweis

Speichert, Horst
Praxis des IT-Rechts -
Praktische Rechtsfragen der Internetnutzung und IT-Security

Neue KES-Reihe:
Zielorientiertes Business Computing
Vieweg Verlag 2004, geb.
ISBN: 3-528-05815-3
€ 49,90

§ §

Juristische Sicherheit

Ganzheitliche Sicherheit

Technische Sicherheit
Firewall,
Virenscanner,
URL-/Content-Filter
etc

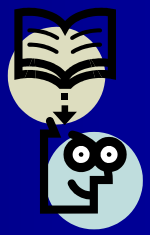
Wirtschaftliche Sicherheit
Restrisiko: Versicherung der IT-Risiken

Juristische Sicherheit
straf- und zivilrechtliche Haftung
Organisationsverschulden
Betriebsvereinbarung, Arbeitsvertrag

Organisatorische Sicherheit
Policy, Audits
Risk-Management
Schulung
Zertifizierung

Haftungsszenario

- Download von Mitarbeittern – Raupkopien, mp3....
- Eintrag von außen– Gästebücher, Foren
- minderjährige Azubis, Jugendschutz
- Beschäftigtenschutzgesetz
- Persönlichkeitsrecht, Belästigung, Beleidigung



Urteil - fremde Inhalte

- OLG Frankfurt vom 13.11.01-11 U 15/01, rechtskräftig
- Urheber- und Markenrechtsverstöße durch raubkopierte Software
- neben GmbH auch persönliche Haftung des Geschäftsführers für Rechtsverstöße der Mitarbeiter
- Verletzung von Aufsichts- und Überwachungs-pflichten
- auch wenn keine Kenntnis vom Rechtsverstoß, allein wegen Wiederholungsgefahr
- Beweislast des Geschäftsführers für Nichtkenntnis, Darlegung der betrieblichen Abläufe

§ §

Kontrolle der Mitarbeiter versus Datenschutz

Datenschutz
Anwendungsbereich

Schutzgegenstand: **personenbezogene Daten**

- Name, Adresse
- Beruf, Stellung
- Personaldaten
- Telefonnummer
- Mail-, IP-Adresse
- Mail-Inhalte, Newsbeiträge
- Logfiles, Verbindungsdaten
- Bestelldaten, Abrechnung

Privatnutzung
Fernmeldegeheimnis

- Ausgangsfrage: ist die private Nutzung erlaubt?
- erlaubte Privatnutzung: AG wird zum TK-Anbieter, da Dienstleistung gegenüber AN
- Geltung Fernmeldegeheimnis: Kontrolle grundsätzlich unzulässig, da Vertrauenstatbestand gegenüber AN
- Kontrolle nur nach § 88, 100 TKG
  - Abrechnungsdaten
  - Gewährleistung sicherer und störungsfreier Ablauf
  - „Erhebung“ zur technischen Datensicherheit, Notfallprävention, Störungsbeseitigung, Datenschutzkontrolle
  - Gefahr im Verzug → z.B. akuter Virus
  - konkreter Hinweis auf Straftat
- AN bleibt auch nach Ausscheiden „Berechtigter“ seiner Mails → nachvertragliche Weiterleitungspflicht des AG
- Verbot nur pro forma, faktisch wird die Privatnutzung geduldet
- Fernmeldegeheimnis, sofern betriebliche Übung
- Privatnutzung kann wieder verboten werden

Dienstliche Nutzung
BDSG

- bei dienstlicher Nutzung oder unerlaubter Privatnutzung, kein Fernmeldegeheimnis
- AN handelt für den AG, keine Dienstleistung
- aber: private Mails sind nicht zu verhindern, Eingang von außen
- allenfalls Adressdaten, kein ständiges Mitlesen wie in USA
- statt TKG gilt BDSG → Güterabwägung der Überwachungsmaßnahmen nach Verhältnismäßigkeitsprinzip
- weitergehende Kontrollen, aber nicht unbeschränkt
- äußere Verbindungsdaten, nicht aber Inhaltskontrollen, da mildere Maßnahmen möglich
- milderes Mittel: Herausgabe der geschäftlichen Mails bei gleichzeitiger Volumenmessung
- AG darf unerwünschte Internet-Angebote ausfiltern → URL-Filter

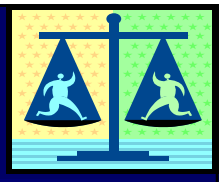
Aktuelle Rechtsprechung

- Ausfiltern von E-Mails ist strafbar
- OLG Karlsruhe vom 10.01.2005, Az. 1 Ws 152/04
- erste obergerichtliche Entscheidung zur Strafbarkeit des Ausfilterns von E-Mails
- ehemals bei einer Hochschule in Baden-Württemberg tätiger wissenschaftlicher Mitarbeiter hatte über Mail-Server der Hochschule weiterhin mit dort tätigen Dozenten, Wissenschaftlern und Freunden Kontakt gehalten und die Nachrichten auf seinem Privatrechner erhalten
- ab Herbst 2003 wurde ihm seitens der Hochschule die Benutzung der Kommunikationseinrichtungen untersagt, gleichzeitig wurden alle an ihn gerichteten und oder von ihm stammenden Nachrichten ausgefiltert, ohne dass Absender oder Empfänger hiervon unterrichtet worden waren

Aktuelle Rechtsprechung

- nach OLG Karlsruhe ist § 206 StGB **weit auszulegen**, denn nur ein solches Verständnis könne dem Gesetzeszweck gerecht werden, das subjektive Recht des Einzelnen auf Geheimhaltung des Inhalts und der näheren Umstände des Postverkehrs und seinen Anspruch auf Übermittlung von Sendungen zu schützen
- Behörden und Unternehmen stehen gleich
- auch von außen kommende E-Mails stehen unter dem Schutz des Fernmeldegeheimnisses
- Strafbarkeit ist gegeben, soweit kein Rechtfertigungsgrund wie etwa eine Virengefahr vorliegt

Interessensausgleich durch rechtliche Gestaltung



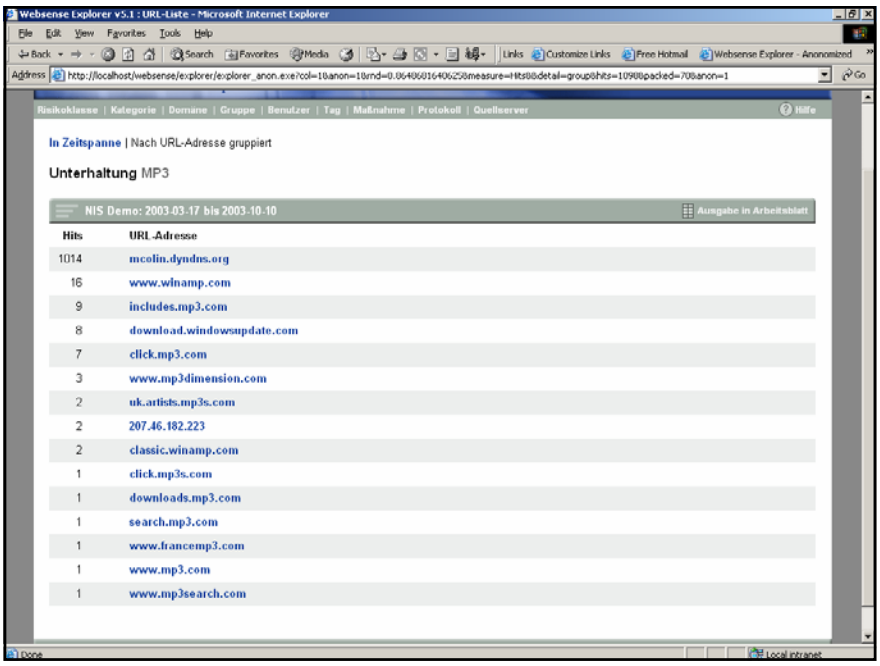
- ungeregelte Zustände: ständiger Graubereich, da Datenschutzrecht schwammig → Verunsicherung bei AG, Admin und AN
- präventives Verbot mit Erlaubnisvorbehalt → Gestaltungsspielraum
- nach Wunsch des Gesetzgebers: Vereinbarungen als legale Handlungsgrundlage
- Vorteile für alle Beteiligten:
  - klare Verhältnisse für Admin : keine Übergriffe/ Strafbarkeit
  - Tansparenz für AN: Vertrauen aber auch Warnfunktion
  - Haftungsprävention bei legaler Kontrolle für AG
- Mitbestimmungsrechte des Betriebs-/Personalrates
- Anpassung der Arbeitsverträge
- Betriebs-/Dienstvereinbarung mit Nutzungsrichtlinien
- individuelle Zustimmung:
  - zusätzliche Legitimation und Information (Verwendung als Info-Broschüre
  - Anhang Betriebs-/Dienstvereinbarung

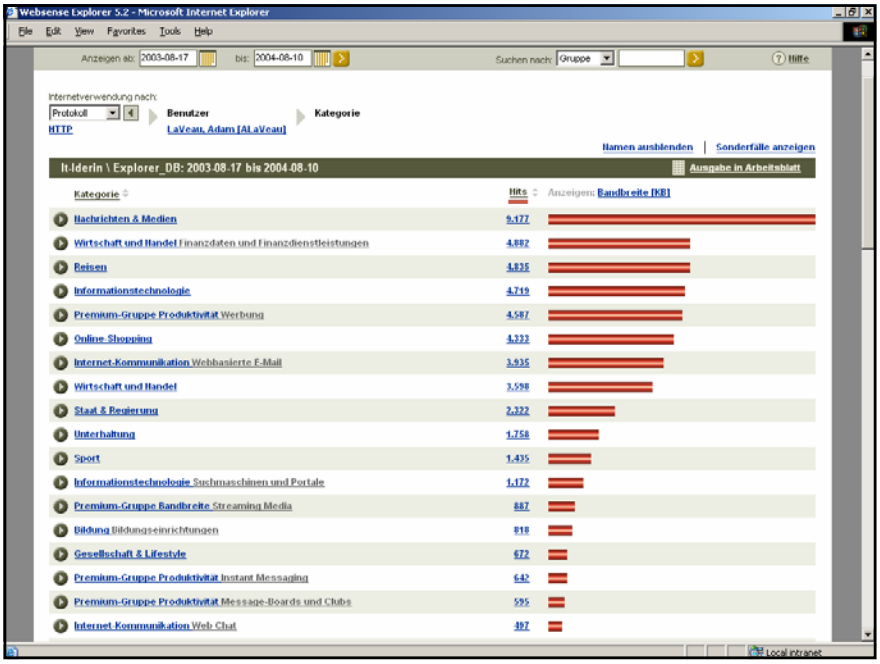
Beweisverwertungsverbot

- Kündigungsschutzklage des Arbeitnehmers gegen Abmahnung und Kündigung
- Datenerhebung verstößt gegen Datenschutz-bestimmungen oder Mitbestimmungsrechte des Betriebsrates
- die rechtswidrige Datenerhebung führt zu Beweis-verwertungsverbot im Prozess
- Arbeitgeber verliert Klage, muss Mitarbeiter weiter beschäftigen oder hohe Abfindung zahlen
- Festschreibung eines legalen Kontrollprozederes in der Betriebsvereinbarung im Interesse des Arbeitgebers
- rechtssichere Beweismittel bei Missbrauchsfällen

Betriebs-/Dienstvereinbarung
Gesamtüberblick

- Umfang einer erlaubten Privatnutzung
- verbotene Nutzungen
- 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
  - Monitoring-Funktionen, etc.
- Abwesenheitsregelung
- Kontrollprozedere:
  - anonymisierte Stichprobenkontrolle
  - grober Missbrauch, Straftat: personenbezogene Kontrolle
  - Beteiligung: Betriebsrat, DatenSchBeauftragter
- Löschungspflichten
- Konsequenzen bei Nichteinhaltung
- Schlussbestimmungen


Websense Explorer v5.1 : URL-Liste - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost/websense/explorer/explorer_anon.exe?col=1&anon=1&rnd=0.06406016406258measure=Hits&detail=group&hits=1090&packed=70&anon=1
Risikoklasse | Kategorie | Domäne | Gruppe | Benutzer | Tag | Maßnahme | Protokoll | Quellserver
Hilfe
In Zeitspanne | Nach URL-Adresse gruppiert
Unterhaltung MP3
NIS Demo: 2003-03-17 bis 2003-10-10
Ausgabe in Arbeitsblatt
Hits URL-Adresse
1014 mcolin.dyndns.org
16 www.winamp.com
9 includes.mp3.com
8 download.windowsupdate.com
7 click.mp3.com
3 www.mp3dimension.com
2 uk.artists.mp3s.com
2 207.46.182.223
2 classic.winamp.com
1 click.mp3s.com
1 downloads.mp3.com
1 search.mp3.com
1 www.francemp3.com
1 www.mp3.com
1 www.mp3search.com
Done
Local intranet

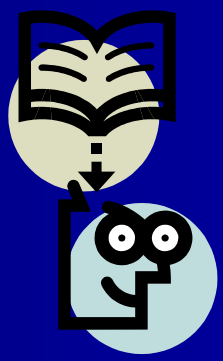

Websense Explorer 5.2 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Anzeigen ab: 2003-08-17 bis: 2004-08-10
Suchen nach: Gruppe
Hilfe
Internetverwendung nach:
Protokoll
HTTP
Benutzer
LaVeau, Adam [ALaVeau]
Kategorie
Namen ausblenden | Sonderfälle anzeigen
It-Iderin \ Explorer_DB: 2003-08-17 bis 2004-08-10
Ausgabe in Arbeitsblatt
Kategorie
Hits
Anzeigen: Bandbreite [KB]
Nachrichten & Medien 9.177
Wirtschaft und Handel Finanzdaten und Finanzdienstleistungen 4.882
Reisen 4.835
Informationstechnologie 4.719
Premium-Gruppe Produktivität Werbung 4.587
Online Shopping 4.333
Internet-Kommunikation Webbasierte E-Mail 3.935
Wirtschaft und Handel 3.598
Staat & Regierung 2.322
Unterhaltung 1.758
Sport 1.435
Informationstechnologie Suchmaschinen und Portale 1.172
Premium-Gruppe Bandbreite Streaming Media 887
Bildung Bildungseinrichtungen 818
Gesellschaft & Lifestyle 672
Premium-Gruppe Produktivität Instant Messaging 642
Premium-Gruppe Produktivität Message-Boards und Clubs 595
Internet Kommunikation Web Chat 407
Local intranet

§ §

Gesetzliche Archivierungs-pflichten

Szenario

- Storage, Backup, Datensicherung
- Speicherplatz und Kostenfaktor
- mindestens gesetzliche Vorgaben
- Handels- und Steuerrecht
- Kostenvermeidung



Handelsrecht

- § 257 Abs. 1 HGB: Pflicht zur geordneten Aufbewahrung
- jeder Kaufmann: GbR, GmbH, AG
- Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Konzernabschlüsse, Konzernlageberichte, sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen, empfangene und versandte Handelsbriefe, Buchungsbelege
- Begriff Handelsgeschäft, nach BGH weit definiert
- entfernter, lockerer Zusammenhang mit betrieblichen Interessen

Handelsrecht

- z. B. Angebot, Annahme, Auftragsbestätigung, Mängelrüge, Arbeitsverträge, Bau von Gebäuden usw.
- nicht umfasst, lediglich reine Privatgeschäfte des Kaufmannes
- zur Vereinfachung die gesamte Geschäftskorrespondenz als aufbewahrungspflichtig einstufen
- bei vorsätzlicher Verletzung von gesetzlichen Aufbewahrungsfristen, sofern Zahlungseinstellung oder Insolvenz, Geldstrafe oder Freiheitsstrafe bis zu 2 Jahren, § 283 b Abs. 1 Nr. 2 StGB
- bei Überschuldung oder Zahlungsunfähigkeit, Strafbarkeit nach § 283 Abs. 1 Nr. 6 StGB

Steuerrecht

- sämtliche kaufmännische Unterlagen
- **sonstige Unterlagen**, soweit sie für die Besteuerung bedeutsam sind, § 147 Abs. 1 AO
- bei Verletzung, keine ordnungsgemäße Buchführung, **Schätzung** der Besteuerungsgrundlagen, § 162 AO
- möglicherweise **Steuerhinterziehung**

Einsetzbare Datenträger

- Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme – **GoBS** - des Bundesfinanzministeriums vom 07.11.1995
- keine bestimmte Technologie, 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
- Unveränderlichkeit, § 146 Abs. 4 AO (revisionssicher)
  - Erfassung aller Informationen, ohne Unterdrückung
  - einmal erfolgte Buchung darf nicht rückgängig gemacht werden
  - Fehlerkorrektur nur durch nachvollziehbare Änderungen (Storno)

Behördenzugriff

- systematische Verzeichnisse
- internes Kontrollsystem
- jederzeitige Verfügbarkeit, prompte Lesbarkeit, § 147 Abs. 5 AO
- Vorlage- und Kostentragungspflicht auf Verlangen
- Außenprüfung, Einsichtnahme im System des Steuerpflichtigen
- nur Lesezugriff, keine Fernabfrage (Online-Zugriff)
- Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen – **GDPdU** - am 16.07.2001 vom Bundesfinanzministerium erlassen, http://www.aufbewahrungspflicht.de/edfs/gdpdu.pdf
- Vorsteuerabzug auch bei elektronischen Rechnungen mit qualifizierter digitaler Signatur

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

Horst Speichert

e|s|b Rechtsanwälte Stuttgart

Rechtsanwalt
Lehrbeauftragter
Universität Stuttgart

horst@speichert.de
www.kanzlei.de

EDV- und Internet-Recht
Security-Policies
Datenschutz
IT-Vertragsgestaltung
Outsourcing