„Alles was Recht ist!”

Juristische Aspekte der E-Mail- und Internetnutzung sowie gesetzliche Archivierungspflichten

RA Horst Speichert

Horst Speichert

e|s|b Rechtsanwälte Stuttgart

Rechtsanwalt

Lehrbeauftragter
Universität Stuttgart

- EDV- und Internet-Recht
- IT-Vertragsgestaltung
- Datenschutz und IT-Audits
- Security-Policies, Richtlinien
- Datenschutzbeauftragter (DSB)
- Schulung DSB
- Vorträge, Seminare

E-Mail: horst@speichert.de
Internet:http://www.kanzlei.de
http://www.speichert.de

Literaturhinweis

Speichert, Horst

Praxis des IT-Rechts -

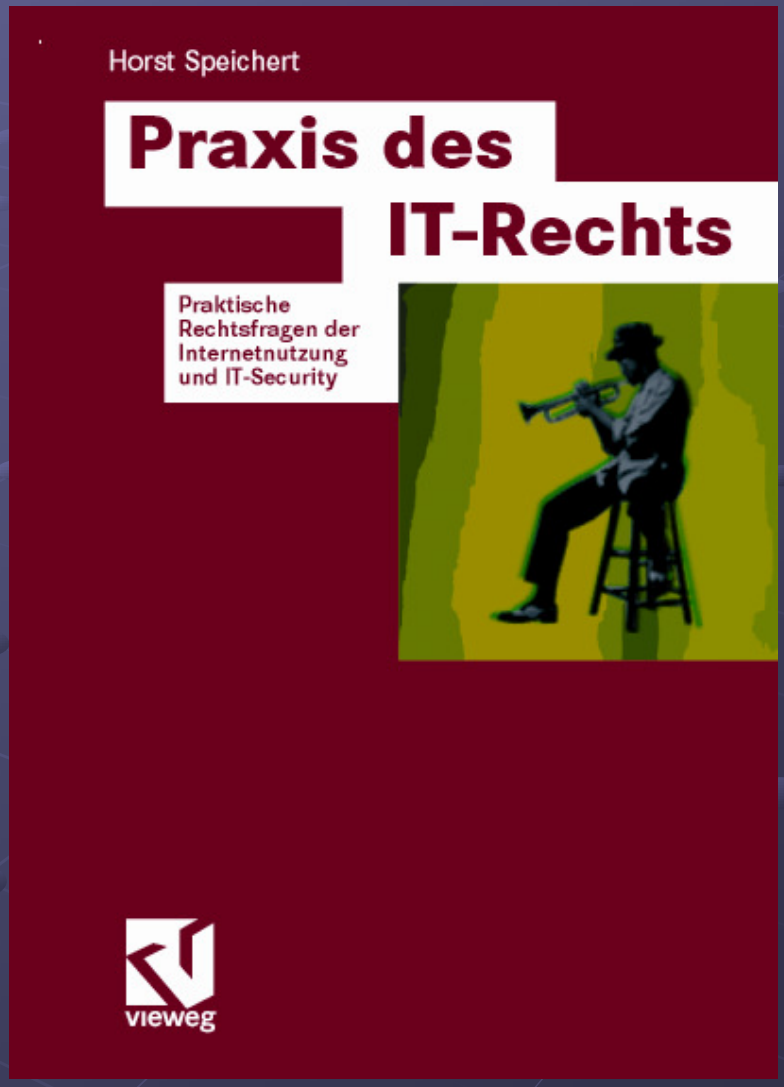
Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung

Vieweg Verlag, 2. Auflage, Mai 2007, geb.

KES-Reihe

ISBN: 3-528-05815-3

€ 49,90



Ganzheitliche Informationssicherheit

Technische Sicherheit

Archivierung, Backup,
Firewall, AV,
URL-/Spam-
Content-Filter
Verschlüsselung

Wirtschaftliche Sicherheit

Restrisiko: Versicherung
der IT-Risiken

Juristische Sicherheit

Vertragsgestaltung, AGB
straf- und zivilrechtliche Haftung
Organisationsverschulden
Betriebsvereinbarung, Arbeitsvertrag

Organisatorische Sicherheit

Policy, Audit
Risiko-Management
Nutzungsrichtlinien
Kontrolle, Schulung
Zertifizierung

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**

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

GoBS

- Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme – **GoBS** - des Bundesfinanzministeriums vom 07.11.1995
- Datenträger, keine bestimmte Technologie
  - Bildträger, maschinenlesbare Datenträger (Disketten), 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)

GDPdU - Behördenzugriff

- systematische Verzeichnisse, z.B. nach Jahr, Monat, etc.
- internes Kontrollsystem
- jederzeitige Verfügbarkeit, prompte Lesbarkeit, § 147 Abs. 5 AO
- Vorlagepflicht auf Verlangen
- Außenprüfung, Einsichtnahme im System des Steuerpflichtigen
- Lesezugriff vor Ort, aber 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

Zugriffsmöglichkeiten der Prüfer

nach I1 GDPdu

- **Unmittelbarer Zugriff**

  Prüfung auf dem Inhouse-System des zu prüfenden Unternehmens.

- **Mittelbarer Zugriff**

  Das Unternehmen oder ein beauftragter Dritter werten die Daten nach Vorgaben des Prüfers aus.

- **Datenträgerüberlassung**

  Überlassung der Daten an den Prüfer auf einem geeigneten Medium z.B. auf selbsttragendem IPro3i-IDEA-Archiv

Wichtig:

- Wahlmöglichkeit des Prüfers auch kumulativ
- Nur Zugriff auf steuerrechtlich relevante Unterlagen

Rechtssichere Trennung

- Gratwanderung zwischen Datensicherheit und Datenschutz
- Archivierung kann mit Datenschutz, Fernmeldegeheimnis kollidieren
- Archivierung der Buchungsdaten → zumeist gewährleistet
- Archivierung der E-Mails
  - Gemenge zwischen privaten und geschäftlichen E-Mails
  - vollständiges Speicherungsverbot privater Mails?
- Betriebsvereinbarungen (Arbeitsvertrag) schaffen Abhilfe bei der Datenschutzproblematik
- umfassende E-Mail-Policy

Rechtssichere Trennung

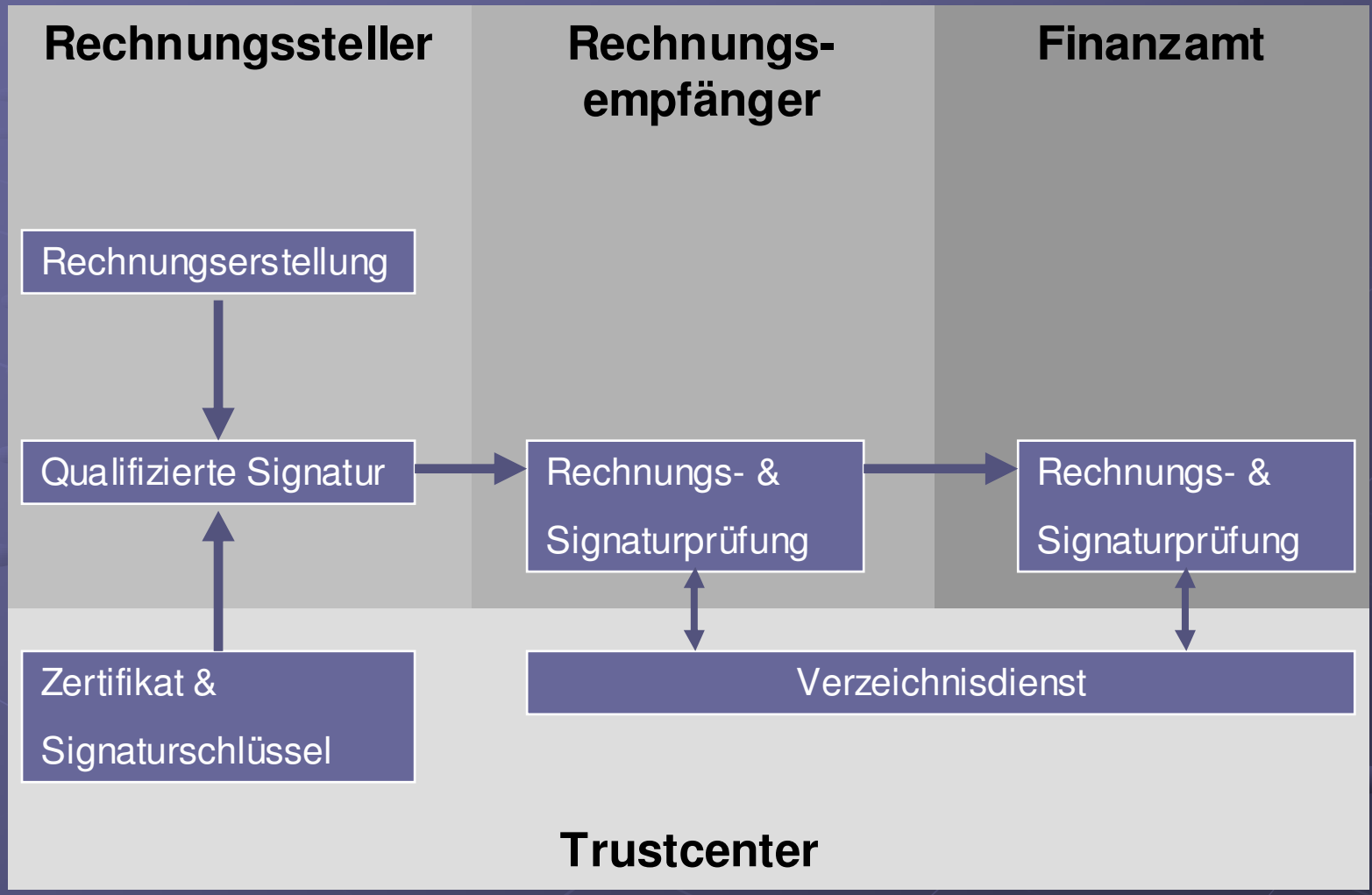
- Trennung der Gemengelage
- grundsätzlich drei Lösungsansätze
- Komplettarchivierung
  - höchste Sicherheit gegen Missbrauch
  - Problem: private Inhalte werden mitarchiviert → lange Aufbewahrungsfristen
- „Bereinigungslösung“ bei betriebswichtigen Mitarbeitern - Verfallsdatum für private E-Mails
- Weiterleitung durch Indizierung (Markierung, Tag)
  - geringe Sicherheit gegen Missbrauch
  - aktive Mitwirkung des Mitarbeiters erforderlich
  - hohe Datenschutzkonformität

Elektronische Rechnungen

Digitale Rechung

- Nach **GDPdU** Vorsteuerabzug bei elektronischen Rechnungen nur mit qualifizierter digitaler Signatur mit Anbieter-Akkreditierung nach § 15 Abs. 1 SigG
- übliche Geschäftspraxis (z.B. der Fluglinien) nicht ausreichend
- mögliche Folgen: hohe Schäden, weil Prüfer die gezogene Vorsteuer aberkennt
- Unzufriedenheit, Haftung beim Kunden

Prinzip der elektronischen Rechnung



§

Informations- und Risiko-management

GoBS

- Internes Kontrollsystem
  - Sicherung und Schutz des vorhandenen Vermögens und vorhandener Informationen vor Verlusten aller Art
  - Bereitstellung vollständiger, genauer, aussagefähiger und zeitnaher Aufzeichnungen
  - Förderung der betrieblichen Effizienz durch Auswertung und Kontrolle der Aufzeichnungen
  - Unterstützung der Befolgung der Regeln der vorgeschriebenen Geschäftspolitik
- Datensicherheit
  - Datensicherheitskonzept
  - Sicherung gegen Datenverlust
  - Stand der Technik
- Dokumentation und Prüfbarkeit


SOX

SOX

- 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
- in Kraft seit 30.07.2002
- Aufschub für ausländische Unternehmen, die US-börsennotiert ➔ verbindlich erst ab 15.07.2006

Euro-SOX

- EU wird Regelungen aus dem SOA in adaptierter Form einführen
- Reaktion auf Finanzskandale wie Parmalat oder Ahold
- Richtlinie 2006/43/EG vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Anpassung der 8. EU-Prüferrichtlinie
- Anwendungsbereich: Unternehmen des öffentlichen Interesses
  - börsennotierte Unternehmen
  - Banken, Versicherungen
  - Monopolunternehmen → Energieversorger, Post, Bahn etc.
- Prüfungsausschuss (Audit Committee)
- Zusammenarbeit zwischen Audit Committee und Wirtschaftsprüfer
  - Abschlussprüfer muss das Audit Committee insbesondere über wesentliche Schwachstellen im IKS informieren
  - künftig höhere Anforderungen an das IKS

Basel II

Basel II

- regelt Kreditvergabe und Kreditbedingungen
- bisher gesetzlich nicht verbindlich, wird aber im Hinblick auf die gesetzliche Umsetzung bereits heute allgemein beachtet und angewendet
- 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 wird
- voraussichtlich Ende 2006 treten die neuen Bestimmungen in Kraft

Umsetzung von Basel II

- Kreditwesengesetz, KWG

  → § 25a Abs. 1 und 1a (Säule II), § 25a Abs. 4–7 (Säule III), § 45b (zusätzliche Kapitalanforderungen)
- Solvabilitätsverordnung, SolvV und Groß- und Millionenkreditverordnung, GroMiKV

  → Regelwerk für Eigenmittelanforderungen, insbesondere Risikomessverfahren und Zulassungsvoraussetzungen (Säule I und III)
- Mindestanforderungen an das Risikomanagement, MaRisk

  → Ausbau zu qualitativem Regelwerk, das auf der Basis des § 25a Abs. 1, 1a KWG die Anforderungen an das Risikomanagement zusammenführt (Säule II)

MaRisk

- Mindestanforderungen an das Risikomanagement des BaFin vom Dez. 2005
- 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
  - Test und Abnahme durch Verantwortliche
- Notfallkonzept
- Outsourcing

Basel II

- 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

  (dort S. 9):

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

Basel II

- vorhandenes Sicherheitsniveau kann z. B. durch Zertifizierungen (etwa BSI-Grundschutz oder ISO 17799) 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
- z.B. Rating der Sparkassen-Finanzgruppe:
  - Controlling (4,5%): Wie beurteilen Sie das Risikofrüherkennungssystem?
  - Spezielle Risken (10 %): Wie beurteilen Sie die Abhängigkeit von sonstigen Risiken?

Rechtsfolgen Non-Compliance

- **BDSG** → Auskunfts-, Berichtigungs-, Sperrungs-, Löschungs-, Unterlassungs-, und Schadensersatzansprüche nach §§ 6,7,34,35 BDSG
- **SOX**
  - Testatsverweigerung des Wirtschaftsprüfers (§322 HGB), entsprechendes Bußgeld nach § 334 HGB
  - Entlastung von Vorstand und Aufsichtsrat, §120 AktG
  - Bußgeld der SEC bis hin zum Verlust der Börsenzulassung
  - Imageschaden, Auftragsverluste bei Bekanntwerden
- **KonTraG**
  - dto
  - persönliche Haftung des Vorstands
- **Vergabeverfahren**
  - Eigenerklärung oder Nachweis von IT-Compliance
  - Ausschluss oder Nichtberücksichtigung, z.B. § 25 Nr. 2 VOL/A

Rechtsfolgen Non-Compliance

- **Basel II (Kreditnehmer)** → schlechtere Kreditbedingungen (höhere Zinsen oder Sicherheiten)
- **Basel II (Kreditgeber)**
  - Testatsverweigerung des Wirtschaftsprüfers (§322 HGB), entsprechendes Bußgeld nach § 334 HGB
  - Entlastung von Vorstand und Aufsichtsrat, §120 AktG
  - Sanktionen durch BaFin
    - Nachbesserung der Verträge gemäß § 6 Abs. 3 KWG
    - Bußgeld nach § 56 Abs. 2 Nr. 4 KWG
    - bis hin zum Verlust der Bankenerlaubnis nach 35 Abs. 2 Nr. 6 KWG
    - Abberufung des Geschäftsführers nach § 36 Abs. 1,2 KWG
  - Imageschaden, Auftragsverluste bei Bekanntwerden
- Nachteile beim **Versicherungsschutz**
  - Verlust oder Leistungskürzung aufgrund mangelnder IT-Compliance
  - Verletzung von Anzeigepflichten nach § 16 VVG, § 153 VVG
  - Erhöhung der versicherten Gefahr, § 23 Abs. 1 VVG
  - grob fahrlässige Unkenntnis aufgrund fehlender IKS, kann Leistungspflicht entfallen, § 6 Abs. 3 VVG

§

Strafverfolgung der Ermittlungsbehörden

Strafverfolgung

Medienbericht vom 23.05.2006:
„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.“

Auskunftsansprüche

- Strafbares Verhalten → z.B. illegale Pornografie, raubkopierte Inhalte
- Geschädigte erstatten Strafanzeige
- Auskunftsansprüche der TK-Anbieter (Provider) nach §§ 89 VI, 113 TKG
  - nach der neuen Rechtsprechung anerkannt
  - öffentliche Provider → IP-Adresse
  - Arbeitgeber → persönliche Zuordnung
- Arbeitgeber = TK-Anbieter bei erlaubter Privatnutzung
- schwierige Situation
  - Passwortverwaltung unzureichend
  - Strafanzeige Mitarbeiter

Vorratsdaten-speicherung

Vorratsdatenspeicherung

- EU-Richtlinie → am 21.02.06 vom Ministerrat abgesegnet
- betroffen: E-Mail, SMS, Telefonie, Surfen, Filesharing, VoIP
- Terrorismusbekämpfung, TK-Anbieter verpflichtet, Verbindungs- und Standortdaten 6 bis 24 Monate vorzuhalten
- Bundestag hat bereits zugestimmt, die Richtlinie restriktiv umzusetzen, also 6 Monate
- BVG hält Richtlinie für verfassungskonform
- Herausforderung für Provider, da Datenmengen im Internet ungleich größer als bei Telefonie

Urteil – offenes W-LAN

- Landgericht Hamburg vom 26.07.2006,
  Az 308 O 407 / 06
- öffentliches Zugänglichmachen von Musikfiles über P2P Gnutella
- offenes W-LAN ohne Passwort, Datenübertragung nicht gesichert
- urheberrechtswidrige Down- bzw. Uploads
- Störerhaftung bejaht
  - zumutbare Prüfungspflichten
  - wer seine Internetverbindung drahtlos betreibt, muss für die Sicherung des Routers sorgen

Gesetzliche Bestimmungen

- **KonTraG, SOX, Basel II** → konkretisiert durch **MaRisk**
- **GoBS, GDPdU** → Vorgaben der Finanzbehörden, Risiken für die steuerlich relevanten Datenbestände sind zu vermeiden
- **BDSG**
  - Vorgaben für die **technisch-organisatorische Datensicherheit,** § 9 BDSG plus Anlage
  - Outsourcing, § 11 BDSG
- § 25a Abs. 1 Nr. 2 KWG → Kredit- und Finanzinstitute müssen über angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung verfügen → konkretisiert durch **MaRisk**
- Die Normen werden von der BGH-Rechtssprechung als Maßstab für die Sicherungserwartungen herangezogen, (BGH NJW-RR 2002, 525, 526; 2001, 2019, 2020)

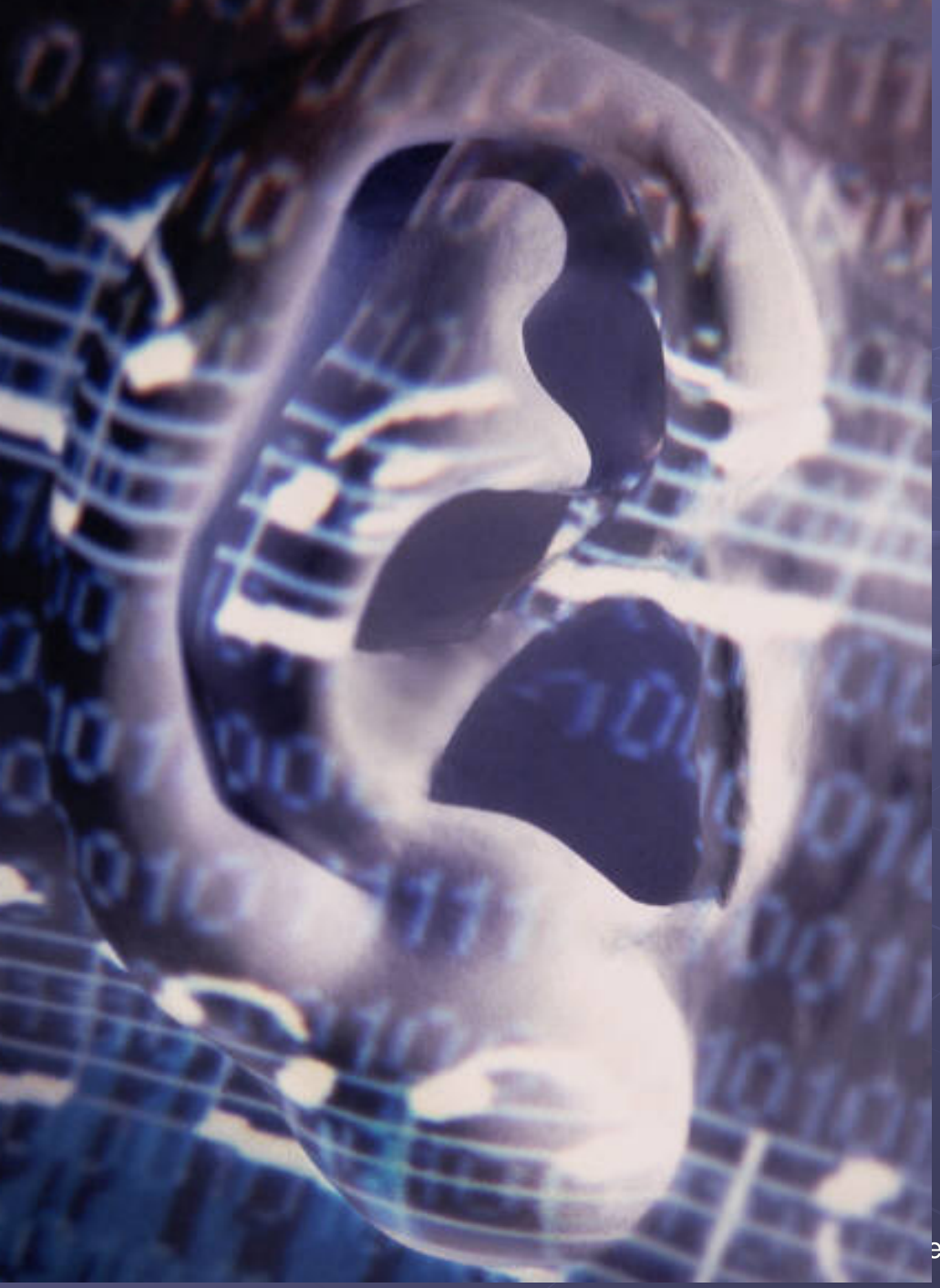
Anlage zu § 9 BDSG

- Grundsätze ordnungsgemäßer DV
- technisches Sicherheitskonzept
- technische Konkretisierung
  - Zutrittskontrolle → räumliche, physische Sicherung
  - Zugangskontrolle → Paßwort, Firewall, Festplattenverschlüsselung
  - Zugriffskontrolle → effektive, rollenbasierte, Rechteverwaltung
  - Weitergabekontrolle → Verschlüsselung
  - Verfügbarkeitskontrolle → Virenschutz, Backup, Archivierung
  - Protokollierung

Schadensersatz nach § 7 BDSG

- Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet.

- Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat → **Beweislastumkehr**



§

Mitarbeiter-Kontrolle in der IT

Private Nutzung am Arbeitsplatz

Privatnutzung Fernmeldegeheimnis

- Ausgangsfrage: ist die private Nutzung erlaubt?
- erlaubte Privatnutzung: Arbeitgeber wird zum TK-Anbieter, da Dienstleistung gegenüber Arbeitnehmer
- Unter Geltung Fernmeldegeheimnis: Kontrolle grundsätzlich unzulässig, da Vertrauenstatbestand gegenüber Arbeitnehmer
- 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

Privatnutzung Fernmeldegeheimnis

- Arbeitnehmer bleibt auch nach Ausscheiden Berechtigter seiner Mails → nachvertragliche Weiterleitungspflicht des Arbeitgebers?
- Arbeitgeber darf unerwünschte Internet-Angebote ausfiltern → URL-Filter
- Verbot nur pro forma, faktische Duldung der Privatnutzung
  - Fernmeldegeheimnis, sofern Duldung
  - betriebliche Übung?
  - Privatnutzung kann wieder verboten werden, einseitig durch Arbeitgeber, keine Mitbestimmung
- Privatnutzung bei fehlendem Verbot
  - Erforderlichkeit eines ausdrücklichen Verbots
  - BAG vom 07.07.2005, Az. 2 AZR 581/04
- Arbeitsrechtliche Sanktionen bei Verstößen
  - Abmahnung
  - fristlose Kündigung, neueste Rechtsprechung, BAG vom 12.01.2006, Az. 2 AZR 179/05

Aktuelle Rechtsprechung

- OLG Karlsruhe vom 10.01.2005, Az. 1 Ws 152/04
- erste obergerichtliche Entscheidung zur Strafbarkeit des Ausfilterns von E-Mails ohne Einwilligung
- ehemaliger wissenschaftlicher Mitarbeiter hatte weiterhin E-Mail-Kommunikation mit den Kollegen
- alle E-Mails wurden ausgefiltert, ohne Einwilligung von Absender oder Empfänger
- nach OLG Karlsruhe ist § 206 StGB **weit auszulegen**, 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

Dienstliche Nutzung

BDSG

- bei dienstlicher Nutzung oder unerlaubter Privatnutzung, kein Fernmeldegeheimnis
- Arbeitnehmer handelt für den Arbeitgeber, keine Dienstleistung
- statt TKG gilt BDSG → Güterabwägung der Überwachungsmaßnahmen nach Verhältnismäßigkeitsprinzip
- weitergehende Eingriffe, aber nicht unbeschränkt
- äußere Verbindungsdaten, nicht aber Inhaltskontrollen, da mildere Maßnahmen möglich

Beweisverwertungsverbot

- Kündigungsschutzklage des Arbeitnehmers gegen Abmahnung und Kündigung
- Datenerhebung verstößt gegen Datenschutz-bestimmungen oder Mitbestimmungsrechte der MV
- 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 Betriebs- Dienstvereinbarung im Interesse des Arbeitgebers
- rechtssichere Beweismittel bei Missbrauchsfällen

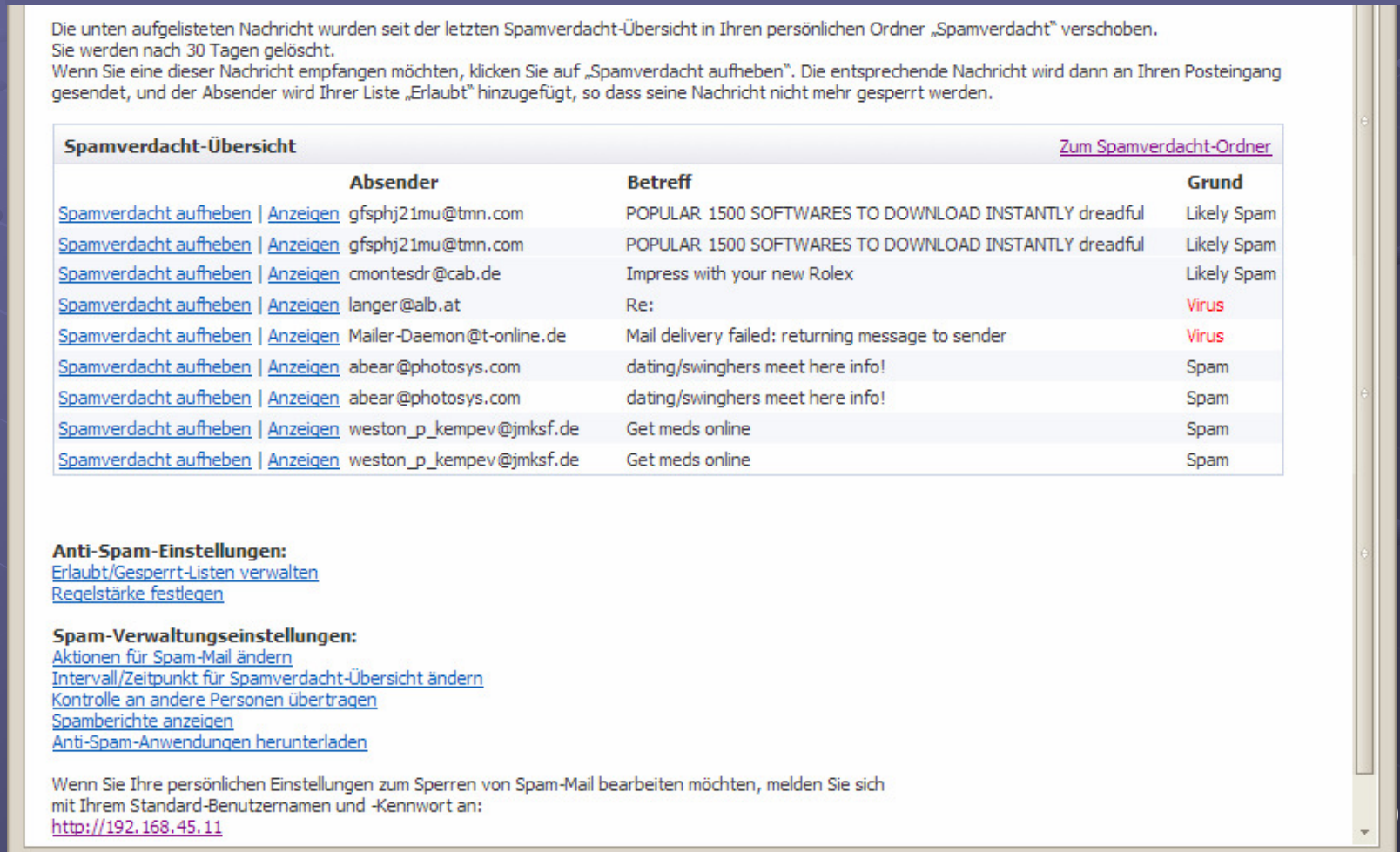
§

Rechtssichere Spam- und Content-Filter

§ §

Spamfilter

Daily Report



Die unten aufgelisteten Nachricht wurden seit der letzten Spamverdacht-Übersicht in Ihren persönlichen Ordner „Spamverdacht" verschoben.
Sie werden nach 30 Tagen gelöscht.
Wenn Sie eine dieser Nachricht empfangen möchten, klicken Sie auf „Spamverdacht aufheben". Die entsprechende Nachricht wird dann an Ihren Posteingang gesendet, und der Absender wird Ihrer Liste „Erlaubt" hinzugefügt, so dass seine Nachricht nicht mehr gesperrt werden.

Spamverdacht-Übersicht — Zum Spamverdacht-Ordner

	Absender	Betreff	Grund
Spamverdacht aufheben | Anzeigen	gfsphj21mu@tmn.com	POPULAR 1500 SOFTWARES TO DOWNLOAD INSTANTLY dreadful	Likely Spam
Spamverdacht aufheben | Anzeigen	gfsphj21mu@tmn.com	POPULAR 1500 SOFTWARES TO DOWNLOAD INSTANTLY dreadful	Likely Spam
Spamverdacht aufheben | Anzeigen	cmontesdr@cab.de	Impress with your new Rolex	Likely Spam
Spamverdacht aufheben | Anzeigen	langer@alb.at	Re:	Virus
Spamverdacht aufheben | Anzeigen	Mailer-Daemon@t-online.de	Mail delivery failed: returning message to sender	Virus
Spamverdacht aufheben | Anzeigen	abear@photosys.com	dating/swinghers meet here info!	Spam
Spamverdacht aufheben | Anzeigen	abear@photosys.com	dating/swinghers meet here info!	Spam
Spamverdacht aufheben | Anzeigen	weston_p_kempev@jmksf.de	Get meds online	Spam
Spamverdacht aufheben | Anzeigen	weston_p_kempev@jmksf.de	Get meds online	Spam

Anti-Spam-Einstellungen:
Erlaubt/Gesperrt-Listen verwalten
Regelstärke festlegen

Spam-Verwaltungseinstellungen:
Aktionen für Spam-Mail ändern
Intervall/Zeitpunkt für Spamverdacht-Übersicht ändern
Kontrolle an andere Personen übertragen
Spamberichte anzeigen
Anti-Spam-Anwendungen herunterladen

Wenn Sie Ihre persönlichen Einstellungen zum Sperren von Spam-Mail bearbeiten möchten, melden Sie sich mit Ihrem Standard-Benutzernamen und -Kennwort an:
http://192.168.45.11

Horst Speichert

e|s|b Rechtsanwälte Stuttgart

Rechtsanwalt

Lehrbeauftragter der Universität Stuttgart

- EDV- und Internet-Recht
- Security-Policies/-Audits*
- Datenschutz*
- Schulung Datenschutz-beauftragter
- Vorträge, Seminare
- IT-Vertragsgestaltung
- Outsourcing*

E-Mail: horst@speichert.de
Internet: http://www.kanzlei.de
http://www.speichert.de

* rechtliche Beratung, Gestaltung, Begutachtung