it.sec
security for your information

Rechtliche Anforderungen am Beispiel der E-Mail-Archivierung

KUMAtronik Systemhaus GmbH

Vortrag zur symantec-Veranstaltung
am 24.04.2007

it.sec
security for your information

Inhalt:

1. Rechtliche Anforderungen an E-Mails
2. Compliance-Anforderungen zur Archivierung
3. Haftung von IT-Verantwortlichen

it.sec
security for your information

Vorstellung des Vortragenden

it.sec
security for your information

Bernhard C. Witt

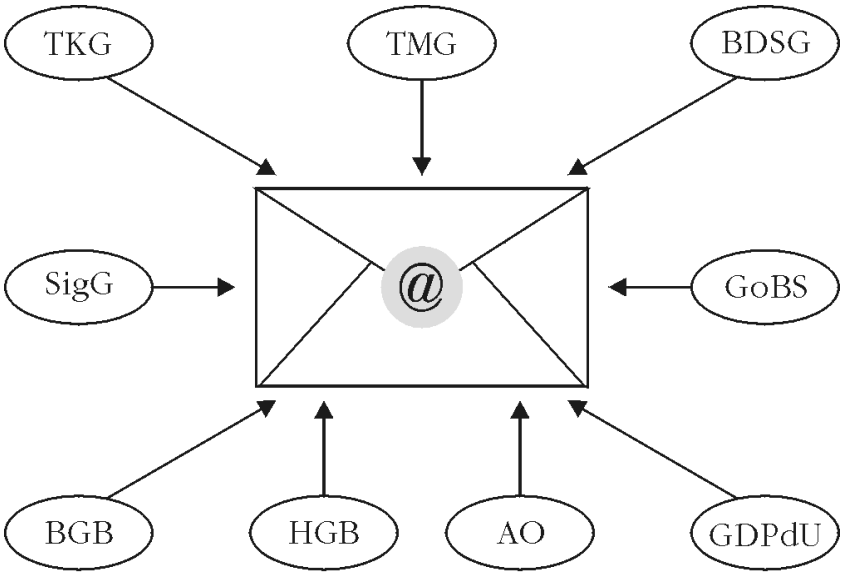
- Berater für Datenschutz und IT-Sicherheit bei der it.sec GmbH & Co. KG
- stellvertretender Datenschutzbeauftragter der KUMAtronik Systemhaus GmbH
- Verantwortlicher zum Thema Compliance der IT-SICHERHEIT praxis
- Buchautor von „IT-Sicherheit kompakt und verständlich“
- geprüfter fachkundiger Datenschutzbeauftragter
- Lehrbeauftragter an der Universität Ulm

it.sec
security for your information

Profil der it.sec GmbH & Co. KG

- spezialisiertes Dienstleistungsunternehmen für IT-Sicherheit und Datenschutz
  - ° Consulting
  - ° Risikomanagement
  - ° Penetrationstests zu Infrastruktur und Web-Applikationen
  - ° Firewall-Audits
  - ° Planung, Integration und Management von Sicherheitssystemen
- seit 1996 mit Standorten in Ulm und München
- bundesweite Tätigkeit
- Bereiche: Banken- und Finanzsektor, Automobilindustrie, IT, Pharmaunternehmen, Krankenkassen, Behörden, …

1a. Übersicht zu E-Mail-Rechtsnormen



it.sec
security for your information

1b. E-Mail als Geschäftsbrief

Dient eine E-Mail
- der Anbahnung,
- dem Abschluss
- oder der Verwerfung

eines Handelsgeschäftes
oder der Mitteilung zur bestehenden Geschäftsbeziehung,
so ergibt sich eine **Archivierungspflicht**!
(u.a. § 37a HGB i.V.m. § 257 HGB bzw. §§ 145-147 AO)
→ 10 Jahre bei Abschlussrelevanz, sonst 6 Jahre

it.sec
security for your information

1b. Rahmenbedingungen

- E-Mails stellen Geschäftsbriefe dar?

→ **Aufbewahrung & Absicherung** der E-Mails!
Bereits Zugang hat ggf. Rechtsfolgen!
Aussonderung von SPAM & Malware!

- Privatnutzung E-Mail gestattet/geduldet?

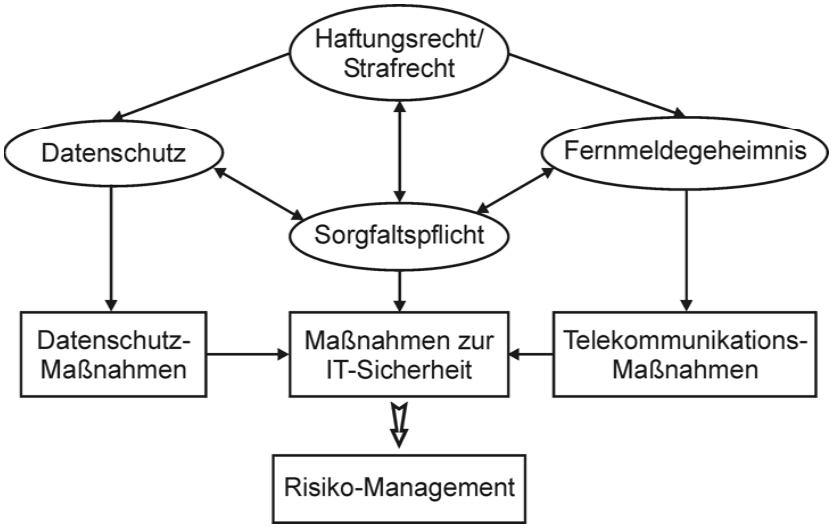
→ E-Mails unterliegen **Fernmeldegeheimnis**!

- Verbindungsdaten sind personenbezogen!

→ E-Mails unterliegen **Datenschutz**!

it.sec
security for your information

1c. Sorgfaltspflicht



1d. Sorgfaltspflichten

= Pflicht

- zur Dokumentation aller Geschäftsvorfälle
- zur Absicherung auch der Mail-Systeme gegen Angriffe und Datenverlust
- zum Virenschutz (Verkehrssicherheit)
- zur Einhaltung von Rechtsvorschriften und Finanzamtsvorgaben

2a. Anforderungen der GoBS

Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme:

- Geschäftsvorfälle müssen vollständig (vom Beleg zur Kontierung bis zur Ablage) nachvollziehbar und korrekt wiedergegeben sein
- internes Kontrollsystem prüft Ordnungsmäßigkeit
- dauerhafte und unveränderliche Datensicherung
- Daten müssen jederzeit lesbar dargestellt werden können
- umfassende Dokumentation DV-gestützter Buchführungssysteme

→ E-Mails davon erfasst, soweit sie Belegfunktion aufweisen

it.sec
security for your information

2b. Anforderungen der GDPdU

Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen:

- nur-lesender Zugriff des Finanzamts auf steuerlich relevante Daten
- Unveränderlichkeit des Datenbestands muss gewährleistet sein
- elektronische Abrechnungen mittels qualifizierter Signatur
- bei Verschlüsselungen sind die Schlüssel zu hinterlegen
- Eingang, Archivierung, Konvertierung und Verarbeitung aufbewahrungspflichtiger Unterlagen sind zu protokollieren
- Datenträger muss maschinell verwertbar sein (E-Mail dagegen als Textdokument nicht, sofern kein entsprechendes Attachment)

it.sec
security for your information

2c. Folgerungen

- vorzugsweise automatisiert erfolgende E-Mail-Archivierung
- Sicherung der Integrität (insb. durch geeigneten Zugriffsschutz) und Verfügbarkeit (insb. durch dauerhafte Datensicherung) der archivierten E-Mails
- Gewährleistung der jederzeitigen Lesbarkeit und Originalität (Fälschungssicherheit) der archivierten E-Mails
- ausführliche Dokumentation & Protokollierung für Revisionssicherheit
- Migrationsfähigkeit auf neue Plattformen bedenken
- Gewährleistung des Datenschutzes & ggf. des Fernmeldegeheimnisses (→ insb. Sicherung der Vertraulichkeit)
- Schnittstelle für Finanzamt bei Architektur berücksichtigen

it.sec
security for your information

2d. Spezielle Fragen

- hohe Speicherkapazität (aber Abstrich bei Zugriffsgeschwindigkeit akzeptabel)
- Überwachungseinrichtungen für Staat ab 1.000 E-Mail-Nutzer
- Filterung von E-Mails auf SPAM & Viren
- Datenschutz und Fernmeldegeheimnis reduzieren u.a. Protokollierungsfunktionen

it.sec
security for your information

3a. Haftung von IT-Verantwortlichen

- Schlechterfüllung arbeitsvertraglicher Pflichten berechtigt zum Schadensersatz (§ 280 I BGB i.V.m. § 611 I BGB)
- Nachweis für Schlechterfüllung obliegt Arbeitgeber (§ 619a BGB)
- Haftung nach Verschuldensgrad gestaffelt (§ 276 BGB i.V.m. § 254 BGB):
  ° Vorsatz → voll
  ° grobe Fahrlässigkeit → voll, sofern verhältnismäßig
  ° „mittlere“ Fahrlässigkeit → anteilig
  ° (leichte) Fahrlässigkeit → nicht
  (Grundlage: diverse BAG-Urteile)
- Schadensersatz bei betrieblich veranlassten Tätigkeiten auch abhängig vom Betriebsrisiko („gefahrgeneigte Arbeit“)

it.sec
security for your information

3b. Haftungsfolgen

- Verletzung der Buchführungspflichten strafrechtlich relevant (§ 283b StGB)
- Urkundenunterdrückung durch Vernichtung, Beschädigung oder Zurüchaltung von Buchführungsunterlagen strafbar (§ 274 StGB)
- Steuerhinterziehung gilt, wenn erhebliche Tatsachen verschleiert werden (§ 370 AO)
- Betroffener kann bei Datenschutzverstoß wider der Sorgfaltspflicht Recht auf Schadensersatz geltend machen (§ 7 BDSG)
  → Beweislast trägt die verantwortliche Stelle!
- Verletzung des Datengeheimnisses berechtigt (je nach Schwere des Vergehens) zur fristlosen Kündigung (ArbG-Urteile)
- Verletzung des Fernmeldegeheimnisses strafbewährt (§ 206 StGB)

it.sec
security for your information

4. Fazit

Unternehmen gut beraten,

- eine leicht umsetzbare E-Mail-Archivierung zu etablieren und
- sich frühzeitig mit Compliance-Fragen zu beschäftigen.

it.sec
security for your information

Noch Fragen?

Kontakt:
Bernhard C. Witt
c/o it.sec GmbH & Co. KG
Sedanstr. 10 / Geb. 17
89077 Ulm
Tel: 0731/20589-11
Fax: 0731/20589-29
Mail: bernhard.witt@it-sec.de