Zwischen den Stühlen: Datenschutz, IT-Sicherheit und Aufbewahrungspflichten

Die Email-Falle

BBS
RECHTSANWÄLTE

RA Thomas Brehm
Hamburg

Aus der Vortragsreihe der

Systemhaus for you GmbH
Heidenkampsweg 66
20097 Hamburg

Bei der Gestaltung der Unternehmens-IT besteht ein Spannungsfeld zwischen

Betrieblichen Anforderungen

Speicherpflichten

Datenschutz

Regelungen und Interessen in diesen Bereichen stehen sich in der Praxis „feindlich“ gegenüber.

A. Betriebliche Anforderungen

I. IT-Sicherheit

Unternehmens-IT soll „sicher“ sein:

- Gefährdung von Betriebs-IT (Hard- u. Software)
- Betriebsgeheimnissen und
- personenbezogenen Daten (Mitarbeiter, Geschäftspartner usw.)

sollen vermieden werden.

Beispielhafte Gefahren:

- Viren
- Trojaner
- Keylogger

aber auch sicherheitsrelevante Inhalte eigentlich „ungefährlicher“ Emails wie z.B. Phishing-Mails

Beispiel aus der Praxis: Mitarbeiterin überweist 50.000 € vom Geschäftskonto an Nigeria-Betrüger

Gesetzliche Anforderung der Anlage zu § 9 BDSG

(dort Nr. 4): Betreiber von IT-Anlagen hat

„zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“

II. ordentliche Geschäftsorganisation

Auch jenseits gesetzlicher Anforderungen verlangt eine betriebswirtschaftliche und geordnete Geschäftspraxis Maßnahmen gegen unerwünschte Emails:

Spam „verstopft“ Systeme
Informationskanalisierung (Mitarbeiter sollen nur mit dem belastet werden, was sie wirklich angeht)

II. ordentliche Geschäftsorganisation

Reduktion auf tätigkeitsrelevante Inhalte dient auch der Wahrung von Geschäfts- und Berufsgeheimnissen!

Beispiel: Mitarbeiter einer Anwaltskanzlei leitet wg. „überfülltem“ Postfach Email an Mandanten an Gegenanwalt weiter.

„Haftungsfalle“

denkbar:

Haftung des Unternehmers/Unternehmens als „Virenverbreiter“

Wer an Geschäftspartner schadsoftware-verseuchte Emails verschickt, kann u.U. wg. Verletzung vertraglicher Nebenpflichten haften.

B. Steuerrechtliche Vorschriften

GdPDU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen):

"E-Mails, die für die Besteuerung von Bedeutung sind, sind nach den allgemeinen Vorschriften des § 147 AO aufzubewahren.“

Fristen des 147 AO:

10 Jahre auszubewahren:
Bücher, Bilanzen, Buchungsbelege u. bestimmte Zollanmeldungen

6 Jahre aufzubewahren:
Handels- oder Geschäftsbriefe; sonstige Unterlagen, soweit für die Besteuerung von Bedeutung

B. Steuerrechtliche Vorschriften

Emails und sonstige von GdPDU erfasste digitale Unterlagen müssen in Ursprungsform archiviert werden!!! (Email mit Headern und Anlagen; Archivierung eines Ausdrucks **reicht nicht!**)

GdPDU: Folgen bei Nichtbeachtung

Größtes Risiko:

Nichtanerkennung von (eigentlich) steuermindernden Aufwendungen

Nichtanerkennung abgezogener Vorsteuer

C: sonstige Aufbewahrungspflichten

Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)

MaRisk (Mindestanforderungen an das Risikomanagement ; Umsetzung Basel II)

Sarbanes-Oxley Act (US-börsennotierte Unternehmen)

Fazit:

ein ordentlicher Geschäftsmann (und Steuerpflichtiger) sollte alle Emails auf Schadsoftware scannen, unerwünschte Emails blocken u. Mails GdPDU-konform archivieren.

fehlende Unterlagen gehen zu Lasten des Steuerpflichtigen! Da steuerrelevante Emails nicht immer zweifelsfrei erkannt werden können, sollten (eigentlich) vorsichtshalber **alle** ein- u. ausgehenden Emails archiviert werden.

Aber:

Datenschutzrechtliche Anforderungen

insbesondere: § 88 TKG (Fernmeldegeheimnis)

Gegenstand: Inhalt der Telekommunikation und ihre näheren Umstände

Verpflichtet: jeder Diensteanbieter (nicht nur Diensteanbieter für die Öffentlichkeit)

mögliche Folgen unrichtig gestalteter Filterung und Archivierung von Emails u. sonstiger elektron. Kommunikation:

§ 206 StGB: Verletzung des Post- oder Fernmeldegeheimnisses (Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe)

§ 202b Abfangen von Daten (Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe)

(Noch) Folgen bei Verstößen:

§§ 43, 44 BDSG (Bußgelder und Freiheitsstrafen)

und

Rechte des Betroffenen (Mitarbeiter)
auf Unterlassung, Auskunft, Berichtigung,
Löschung.

Risikoträger: der IT-Betreiber

Finanzbehörden: „GdPDU u. Datenschutz widersprechen sich nicht.“

jedoch: …. keine Hinweise der Finanzverwaltung für datenschutzrechtlich zulässige Gestaltung der Archivierung.

Bei Nichterfüllung der GdPDU trägt aber das Unternehmen die Folgen.

Lösungsmöglichkeiten:

- Einwilligung in Datenverarbeitung
- Untersagung privater Nutzung
- separate Accounts für priv. u. betriebl. Nutzung
- Verweis auf private Webmail-Nutzung
- technische Trennung betriebl./private Nutzung

Herausforderungen:

Einwilligung: „Freiwilligkeit“ bei Arbeitsverhältnissen schwer erfüllbar

Untersagung: nachträglich möglich bei stillschweigender Duldung?/ gewollt?

separate Accounts: Kosten u. Aufwand

Webmail: Sicherheit

Trennung: technisch und rechtlich zulässig und zuverlässig zu gestalten

Vielen Dank!

RA Thomas Brehm
BBS Rechtsanwälte

www.bbs-law.de
bbs@bbs-law.de
040-34 9999 00