



Bremen im Mai 2008

HERFURTH & PARTNER
RECHT INTERNATIONAL.

IT-Sicherheit – ein rechtliches Update

Monika Sekara

Rechtsanwältin in Hannover

Themenüberblick

- Risikomanagement als IT-Compliance
- Haftung von Geschäftsführern
- Haftung von IT-Leitern
- Weitere Haftungsfallen: Kommunikation, Datenschutz, Datensicherheit
- Haftungsvermeidung



Risikomanagement als IT-Compliance

Uni-Studie zum strategischen Risikomanagement

- Bewertung von Risikomanagementumfang, Einbindung und risikoorientierter Unternehmenskultur.
- Nur ein Großunternehmen der Elektroindustrie hat ein vollständiges strategisches Risikomanagement
- Bis zu 47% der großen und mittelgroßen Unternehmen haben mangelhaftes strategisches Risikomanagement (68% bei Kleinunternehmen).
- Schwachstelle: organisatorische Einbindung.

Uni-Studie zum operativen Risikomanagement

- Bewertung von Qualität und Umfang der Risikoanalyse (Frühwarnsysteme, Risikobewertungsmethoden), Risikobewältigung, Nachbereitung und prozessbegleitende Kontrolle (Effizienz).
- Risikonachbereitung nur bei ca. 3% der Großunternehmen sehr gut; bei 62,3 der GU und 67,2 % der KMU mangelhaft.
- Ca. 15% der GU kein funktionsfähiges operatives Risikomanagement. Problem: Keine Risikoziele!
- Gute Ergebnisse: Chemische Industrie u. Elektroindustrie.

Ziele des Risikomanagements

- wirtschaftlich: Maximierung des Werts des Eigenkapitals durch Optimierung des Risikoprofils.
- rechtlich: Umsetzung von Compliance-Anforderungen (KonTraG, §§ 91 II, 116 AktG, § 43 GmbHG, BDSG, Basel II, SOX) bzw. die Vermeidung von Haftung.

Problem

- Fehlende Kompetenz im Compliance-Bereich
- ca. 8 bis 10 Unternehmensberichte wöchentlich über die Verletzung der eigenen IT-Sicherheit (London School of Economics; ähnlich Uni-Hamburg)

Auswirkungen in der Praxis

LG München I (Urt. v. 05.04.2007) :

- Risikofrüherkennungssystem muss dokumentiert werden. Unterbliebene Dokumentation ist ein **wesentlicher Gesetzesverstoß**.
- Erforderlich: Organisation von unmissverständlichen Zuständigkeiten, engmaschigem Berichtswesen und entsprechende Dokumentation.
- „Es ist sicherzustellen, dass vom verantwortlichen Sachbearbeiter über die jeweiligen Hierarchieebenen bis hin zur Unternehmensleitung sämtliche relevante Stellen von vorhandenen Risiken Kenntnis erlangen, um die entsprechenden Maßnahmen zur Beherrschung dieser Risiken einleiten zu können.“

Folgen mangelnder IT-Sicherheit im Unternehmen

- Datenverluste, Verluste von Betriebsgeheimnissen und Ausfälle in der Produktion
- Schadensersatz und Schmerzensgeld Betroffener
- Beweisprobleme in gerichtlichen Verfahren (Beweissicherheit nur bei Dokumenten mit qualif. digitaler Signatur, sonst freie Beweiswürdigung durch Richter anhand von Indizien)
- Überprüfung durch Datenschutzbehörde
- Bußgeld i.H.v. 25.000,- EUR oder 250.000,- EUR
- Haft- oder Geldstrafe bei Verletzung des Fernmeldegeheimnisses
- Verlust der gewerblichen Zuverlässigkeit
- Verteuerung der Unternehmenskredite - Insolvenz



Haftung von Geschäftsführern

Regelwerke

- § 93 Abs. 1 S. 1 AktG, § 43 Abs. 1 GmbHG
- Vertragsrechtliche Regelungen
- Basel II
- Sarbanes-Oxley-Act (Auswirkungen: §§ 325, 328 HGB = Veröffentlichung von Jahresabschlüssen in elektronischem Bundesanzeiger)
- Grundsätze zur Datenprüfung digitaler Unterlagen (GDPdU)
- Grundsätze ordnungsgemäßer DV-gestützter Buchführung (GoBS)
- Brief-, Post- u. Fernmeldegeheimnis (Art. 10 GG) und Allgemeines Persönlichkeitsrecht (Art. 2 GG)

Managementhaftung:

- Geschäftsführer nach GmbHG
- Haftungsmaßstab: Sorgfalt eines ordentlichen und gewissenhaften Geschäftsführers
- Pflicht: Ergreifen geeigneter Maßnahmen zur frühzeitigen Erkennung von Risiken, Risikomanagement, Risikobewertung
- Haftungsumfang: Persönliche Haftung gegenüber der Gesellschaft, auch dann wenn keine Kenntnis von Rechtsverletzung (OLG Hamburg, Urt. v. 17.04.2002, 5 U 24/01)
- Verjährung: 5 Jahre ab Eintritt des Schadens

Folgen der Nichtbeachtung gesetzlicher Vorgaben:

- Abmahnung
- Unterlassen
- Auskunft
- Schadensersatz
- Schätzung der Besteuerungsgrundlagen (§ 162 AO) bei Verstößen gegen revisionssichere Archivierung nach GdPDU.



Haftung von IT-Leitern

HERFURTH & PARTNER
RECHT INTERNATIONAL.

Haftung von IT-Leitern



Schadenshaftung von Mitarbeitern:

- Mitarbeiter haften idR nur für Vorsatz und grobe Fahrlässigkeit.
- Bei mittlerer Fahrlässigkeit kann der Mitarbeiter anteilig nach der Höhe seines Verursachungsbeitrags haften.
- Bei Schäden infolge leichter Fahrlässigkeit ist der AN von der Haftung durch AG freigestellt.

Fahrlässigkeitsformen:

- Fahrlässigkeit liegt vor, wenn die im Verkehr erforderliche Sorgfalt außer Acht gelassen wird.
- Grobe Fahrlässigkeit = besonders schweres Maß, d. h. einfachste, nahe liegende Überlegungen wurden nicht angestellt und es wurde das nicht beachtet, was in der Situation jedem hätte einleuchten müssen.
- Anteilige Haftung des AN: Ergebnis der Abwägung aller Einzelfallsumstände, z. B. Wert des geschädigten Wirtschaftsguts, Betriebsrisiko, Organisationsverschulden.



Weitere Haftungsfallen

HERFURTH & PARTNER
RECHT INTERNATIONAL.

Weitere Haftungsfallen



Überblick

- Elektronische Kommunikation
- Datenschutz
- Datensicherung



„Schuld an dieser Selbstschädigung ist eine Sicherheitslücke im Unternehmensnetzwerk. Hacker manipulierten Firmencomputer so, dass sie auf ihren Befehl hin Spam-Mails verschickten.“

INTERNET

Potenz für die Konkurrenz

Viagra“-Hersteller Pfizer machte monatelang ungewollt Werbung für die Konkurrenz: In Spam-Mails bot das Pharma-Unternehmen die Pille Cialis an, einen Potenzsteigerer der Firma Eli Lilly. Schuld an dieser Selbstschädigung ist eine Sicherheitslücke im Unternehmensnetzwerk. Hacker manipulierten Firmencomputer so, dass sie auf ihren Befehl hin Spam-Mails verschickten.

Auch Penisverlängerungen, Luxusuhren-Repliken und Schlaftabletten wurden von Pfizer-Rechnern angepriesen. Aufgedeckt hat die Panne die Firma für Internet-Sicherheit Support Intelligence. Das Unternehmen aus Kalifornien sammelte rund 600 E-Mails von Pfizer-Computern. Peinlich für Pfizer, denn normalerweise ermittelt der Konzern gegen Händler, die seine Potenzpille auf dem Internet-Schwarzmarkt anbieten, und bringt sie, wenn möglich, vor Gericht. Nun muss Pfizer die Sicherheitslücke im eigenen Haus finden. Der Konzern droht, er werde gegen den Täter juristisch vorgehen.



LAG Hamm, Beschl. v. 07.04.2006, 10 TaBV 1/06:

- Nutzung von Internet und E-Mail für private Zwecke ist freiwillige Leistung des AG, die AG per Dienstanweisung jederzeit vollumfänglich einstellen kann.
- Betriebliche Übung entsteht nicht, wenn die Gestattung erkennbar nur vorübergehend war.
- Betriebsrat hat kein Mitbestimmungsrecht, wenn Privatnutzung umfassend und vollständig untersagt wird. Diese Maßnahme zielt nicht auf Ordnung im Betrieb, sondern regelt Arbeitsverhalten.
- Mitbestimmung kommt nur in Betracht, wenn AG sich zur Gestattung der Privatnutzung entschieden hat und geregelt werden soll, in welcher Weise dies geschehen soll.

Personenbezogene Daten
(Art. 2 a RL 95/46/EG, § 3 BDSG):

- Alle Informationen über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person.
- Eine Person ist bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Schutzumfang:

- Geschützt sind Angaben zu Einzelpersonen:
 - Vor- und Familienname,
 - Anschrift,
 - Staatsangehörigkeit,
 - Beruf,
 - persönliche eMail (nicht: sales@muster.com).
- Kein Schutz von jur. Personen (GmbH, AG, e. V., e. G.) und Personengesellschaften (OHG, KG).

Haftungsrisiken bei personenbezogenen Daten:

- Verschuldensunabhängige Haftung nach BDSG für öffentliche Stellen, Bußgeld bis 250.000,- EUR.
- Im privatwirtschaftlichen Bereich:
 - Beseitigungs- und Unterlassungsansprüche
 - Schadensersatz und Schmerzensgeld
 - Bußgeld von 25.000,- EUR bis 250.000,- EUR.



OLG Hamm, Urt. v. 01.12.2003, 13 U 133/03:

- Jeder gewerbliche Betrieb muss selbst regelmäßig und zuverlässig für geeignete, lückenlose Datensicherung sorgen (voraussetzende Selbstverständlichkeit).
- Sicherung muss täglich erfolgen, Vollsicherung mindestens einmal wöchentlich. Monatliche Komplettsicherung reicht nicht.
- „Blauäugigkeit“ führt zu sog. haftungsüberdeckender Verantwortung und damit zum Ausschluss von Ansprüchen.



Praktische Tipps zur Haftungsvermeidung

Vermeidung einer Haftung durch optimierte IT-Systeme (sog. Sicherheitskriterien):

- Schutz sensibler Daten (Vertraulichkeit)
- Daten bleiben nach Verarbeitung unveränderlich (Integrität)
- Nachweis der Identität des Nutzers (Authentizität)
- Ermöglichen eines ungestörten Zugangs für den registrierten User (Verfügbarkeit)
- Abgeschottete Kommunikation innerhalb eines Betriebs, jederzeitige Zurechenbarkeit von Daten
- Überwachung der Kommunikation



Risikomanagementhandbuch

- Leitlinien zu Risikokultur + Risikopolitik + organisatorische Einbindung + Ablauforganisation
- Überblick über bestehende Versicherungsverträge
- Überblick über bestehende IT-Verträge
- Verhaltensanweisungen an Mitarbeiter
- Nutzungsordnung / Betriebsvereinbarung
- Notfallplanung (Notfallmanagement)
- Datenschutz (Überblick über Systemschutz, Datensicherung, Kontrollen, Umgang mit personenbezogenen Daten.
- Dokumentation von Schulungen.



Überwachung von E-Mail und Internet

- Überwachung zugelassener privater E-Mails ist nach h. M. unzulässig, ggf. sogar strafbar.
- Datenerfassung nur zulässig, wenn Teilnehmer individuell eingewilligt hat.
- Verbot der privaten Kommunikation ist möglich. Dann ist auch Überwachung durch Erfassen von Inhalts- und Verbindungsdaten erlaubt.
- Einsicht in Inhalte von E-Mails bleibt problematisch.



Rechtliche Möglichkeiten zur Haftungsminde- rung bei Datensicherung:

- Übertragung der Ausführung der Datensicherung an externe führt zur Haftungsverlagerung.
- Outsourcingpartner haftet i.d.R. für den Erfolg einer Datensicherung (Maßstab ist Stand der Technik); Ausnahme, wenn Haftung vertraglich ausgeschlossen.
- Wichtig: Sicherungsmaßnahmen und Sicherungshandlungen detailliert regeln.
- Durchgeführte Datensicherung regelmäßig (tägl./wöchentl.) kontrollieren.

Auswahl eines Outsourcingpartners

- Bauchgefühl ggü. Projektteam
- vorhandene Zertifizierungen: für Einrichtung und Betrieb von IT-Systemen z. B. ISO-Standard 17799, COBIT oder ITIL; für IT Risikomanagement-Systeme ISO-Norm 27001
- Kaufmännisches Angebot
- Rechtlich: Entgegenkommen bei Verhandlungen, keine harten Haftungsklauseln, kein Beharren auf ausschließlichem Dienstleistungscharakter der Services, Bereitschaft zu Audits und Benchmarks



Lösung:

- Im Rahmen einer Arbeitsteilung Aufgaben verteilen und delegieren – auch an externe Dienstleister
 - ⇒ führt zu Haftungsverlagerung bzw. Haftungsminimierung
- Risikomanagementhandbuch
- Kommunikationsüberwachung



www.herfurth.de

sekara@herfurth.de

Copyright by

HERFURTH & PARTNER
Rechtsanwälte GbR

Luisenstr.5,
30159 Hannover

FON 0511 307 56-0
FAX 0511 307 56-10
info@herfurth.de
www.herfurth.de

Member of
ALLIURIS GROUP
www.alliuris.org