Matrix der Haftungsrisiken

IT-Sicherheit - Pflichten und Risiken

Stand April 2005

BITKOM
Connecting visions - creating solutions

Impressum

Herausgeber:
BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 – 0
Fax: 030/27 576 – 400
bitkom@bitkom.org
www.bitkom.org

Redaktion:	Bernd H. Harder, Dr. Sandra Schulz
Verantwortliches BITKOM-Gremium:	Projektgruppe Haftungsrisiken
Redaktionsassistenz:	Leila Ambrosio
Stand:	April 2005, Version 1.1

Ansprechpartnerin:
Dr. Sandra Schulz
Tel: +49 (0)30 / 27576 – 242
E-Mail: s.schulz@bitkom.org

Inhaltsverzeichnis

1 Einleitung

In Medien, Seminaren und Kongressen wird immer wieder der Spruch zitiert „IT-Sicherheit ist Chefsache“. Entweder kümmert sich die Geschäftsführung schon um die IT-Sicherheit oder aber die IT wird spätestens im Schadensfall automatisch zur Chefsache gemacht, so wie beim folgenden Urteil.

Das Oberlandesgericht Hamm traf im Dezember 2003 ein für die Wirtschaft und für die ITK-Branche weit reichendes Urteil: Das Unternehmen A hatte Probleme mit einem Computerkabel. Es beauftragte den IT-Dienstleister B. Ein Angestellter von B tauschte das Kabel aus, doch einige Tage später gab es Fehlermeldungen im Computersystem von A. Der Angestellte von B wollte daraufhin eine Festplatte bei A austauschen. Er fragte nach, ob die Daten auf der Platte gesichert seien. Dies wurde vom Unternehmen A bejaht. Der Server des Unternehmens stürzte beim Austausch ab, wichtige Firmendaten gingen verloren, denn die Daten waren doch nicht gesichert. Das Unternehmen A ließ von einem zweiten Dienstleister einen Teil der Daten wiederherstellen, und wollte den ersten nicht bezahlen. B klagte vor dem Landgericht Bochum und bekam Recht. A ging in die Berufung vor dem Oberlandesgericht Hamm, doch auch die Berufung wurde abgewiesen, diesmal in letztinstanzlicher Entscheidung.

Beinahe noch interessanter als die Entscheidung selbst ist die Urteilsbegründung: Das geschädigte Unternehmen A habe, so schrieb das OLG Hamm, „nicht für eine zuverlässige Sicherheitsroutine gesorgt, sondern diese grob vernachlässigt“. Eine Sicherung der Unternehmensdaten hätte „täglich erfolgen müssen, die Vollsicherung mindestens einmal wöchentlich“. Stattdessen wurde nicht einmal monatlich komplett gesichert: Der nach dem Absturz festgestellte Stand der Komplettsicherung entsprach dem Stand vier Monate vor den Wartungsarbeiten. Das sei, so das OLG, „grob fahrlässig (blauäugig)“ gewesen. Und das Gericht legte in seiner Urteilsbegründung gleich noch nach: Selbst wenn der IT-Dienstleister B seine Kontrollpflichten vor dem Austausch vernachlässigt hätte – was ihm in diesem Fall jedoch nicht nachgewiesen werden konnte – , hätte ein überwiegendes Mitverschulden des Unternehmen A vorgelegen. Mit anderen Worten: Egal wie dilettantisch Wartungsarbeiten durchgeführt werden, derart „blauäugige“ Unternehmen müssen für solche Schäden wie den Datenverlust selbst aufkommen.

Derartige Fälle, wie beim OLG Hamm, dringen jedoch eher selten an die Öffentlichkeit und kommen selten vor Gericht, die betroffenen Firmen haben Sorge um ihr Image. Wer gibt schon „öffentlich gerne zu“, dass seine Datensicherung Lücken hat oder seine Software nicht vollständig lizenziert ist und dadurch dem Unternehmen Schäden entstanden sind.

BITKOM hat diese Entscheidung zum Anlass genommen, besonders relevante Haftungsrisiken im Bereich IT-Sicherheit in einer „Matrix der Haftungsrisiken“ zusammenzustellen.

Die Inhalte dieses Leitfadens sind sorgfältig recherchiert. Sie spiegeln die Auffassung im BITKOM zum Zeitpunkt der Veröffentlichung wider. Der Leitfaden erhebt jedoch keinen Anspruch auf Vollständigkeit. Die dargestellte Materie ist der fortlaufenden Entwicklung des Rechts und der Technik unterworfen. Letztlich versteht sich dieser Leitfaden daher als Einführung in die Problematik und Aufbereitung möglicher Haftungsrisiken und Handlungspflichten, die jedoch die Einbindung professioneller unternehmensinterner oder externer Berater nicht überflüssig macht. Entscheidend ist darüber hinaus immer die Situation im konkreten Einzelfall.

2 Matrix der Haftungsrisiken

Ausgehend von besonders relevanten Pflichten bzw. Regelungsbedarf im Unternehmen bzgl. der Gewährleistung der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität) ist die „Matrix der Haftungsrisiken“ erstellt worden. Die Pflichten und der Regelungsbedarf sind in den folgenden drei Aufgabenbereichen zusammengefasst:

- Strategische Aufgaben (siehe Kapitel 2.1)
  1. Sicherstellung einer bedarfs- und rechtskonformen IT-Nutzung
  2. Bestellung eines betrieblichen Datenschutzbeauftragten
- Konzeptionelle Aufgaben (siehe Kapitel 2.2)
  1. Einführung eines Sicherheitskonzepts (inkl. Katastrophen- und Zugriffsschutz) und eines Datenschutzkonzeptes
  2. Ständige Aktualisierung des Sicherheits-/Datenschutzkonzeptes
  3. Regelungen beim Zugang von externen Dritten zu Datenverarbeitungssystemen
  4. Professionelle Beschaffung von IT-Systemen und Durchführung von IT-Projekten
  5. Sicherung von Vertraulichkeit und Geheimhaltung
- Operative Aufgaben (siehe Kapitel 2.3)
  1. Ordnungsgemäße Abbildung der wirtschaftlichen Verhältnisse des Unternehmens in der Buchführung
  2. Datenschutzrechtliche Konformität sicherstellen
  3. Einsatz von SPAM- und Viren-Filtern abwägen
  4. Regelung für die Nutzung von E-Mail und Internet am Arbeitsplatz
  5. Verhinderung von Schädigung Dritter durch firmeneigene IT insbesondere Virenfreier Daten-/Datenträgeraustausch
  6. Durchführung regelmäßiger Backups
  7. Verwendung lizenzierter Software
  8. Einhaltung der Urheberrechte

Für die strategischen Aufgaben ist der Vorstand bzw. der Geschäftsführer zuständig. Die rechtliche Verpflichtung ergibt sich hierfür insbesondere aus dem Gesellschaftsrecht bzw. dem KonTraG, dem „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“. Damit sollen Kontrolle und Transparenz in Aktiengesellschaften und größeren GmbHs verbessert werden, z.B. indem ein Überwachungssystem eingeführt wird. Das vorhandene Aktiengesetz sowie das GmbH-Gesetz wurden entsprechend ergänzt (§91 II AktG, §116 AktG) bzw. werden entsprechend angewendet (§ 43 GmbHG). Nach § 91 II AktG hat der Vorstand einer AG geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit eine Entwicklung, die den Fortbestand der Gesellschaft gefährdet, früh erkannt werden kann. Diese Verpflichtung gilt nach § 43 GmbHG auch für Geschäftsführer einer GmbH und unter bestimmten Umständen auch für Personalgesellschaften wie OHG und KG.

Das Überwachungssystem soll frühzeitig Alarm schlagen, wenn die Existenz eines Unternehmens gefährdet ist. Zudem verpflichtet das Gesetz die Geschäftsführung, ein unternehmensweites Risikomanagement zu installieren. Dies betrifft eben nicht nur den Finanzbereich sondern auch alle sonstigen Bedrohungen, die auch durch IT-Systeme und den IT-Einsatz entstehen können. Im Rahmen eines IT-Risikomanagements werden in einer Risikoanalyse Risiken erfasst und bewertet, um das Gesamtrisiko für das Unternehmen zu ermitteln. Das anschließende Ziel ist es mittels Sicherheitsstrategie und darauf basierendem Sicherheitskonzept die Risiken zu reduzieren. Zur Risikoprävention können z. B. Maßnahmen zum Schutz der IT-Infrastruktur (z. B. durch Datensicherung, Sabo-

tage- und Ausfallschutz) und der Schutz vor missbräuchlicher IT-Nutzung (durch Mitarbeiter oder Dritte) gehören. Verletzen Geschäftsführer oder Vorstand – als Verantwortliche – diese Risikovorsorgepflicht, so kann dies zu Schadensersatzforderungen führen. In einem solchen Falle sind, und das ist natürlich besonders wichtig, die Mitglieder des Vorstands und der Geschäftsführung unter Umständen auch Aufsichtsratmitglieder (§116 AktG) persönlich haftbar. Zwar können sich Manager auch in Deutschland versichern lassen, z.B. gegen Ansprüche ihres Unternehmens gegen sie. Diese so genannten „directors & officers liabilty insurance“ umfassen normalerweise auch Haftung aus IT-Problemen. Allerdings erlischt der Versicherungsschutz bei Vorsatz oder einer „wissentlichen Pflichtverletzung“ – wenn ein Manager beispielsweise in einem Expertengutachten explizit auf die mangelhafte IT-Sicherheit in seinem Unternehmen hingewiesen wurde und untätig bleibt.

Auch wenn die Versicherung den Schaden der persönlichen Verantwortlichen bis zu einer gewissen Höhe trägt sind weitere Nachteile, insbesondere für das Unternehmen, zu befürchten wie z.B.:

- Unternehmensverluste / Insolvenz durch Ausfall der Systeme bei sehr hohen Schäden
- Ggf. Verlust von Versicherungsschutz des Unternehmens
- Verteuerung der Unternehmenskredite (Basel II)
- Imageschaden nach Verlust von personenbezogenen Daten aufgrund von Sicherheitslücken

Der Aufsichtsrat hat zu kontrollieren, ob der Vorstand alle erforderlichen Maßnahmen im Rahmen des Risikomanagements getroffen hat. Führt er diese Kontrolle unzureichend aus und treten erhebliche Schäden, insbesondere Insolvenz, ein, haftet auch der Aufsichtsrat persönlich.

Für jede Pflicht bzw. jeden Regelungs-/Handlungsbedarf sind in der Matrix – sofern möglich – die Verantwortlichen, deren persönliche Haftung, die jeweilige Rechtsgrundlage, potentielle Schäden bzw. Nachteile für das Unternehmen, Ansprüche Dritter, Anmerkungen sowie ausgewählte Entscheidungen aufgeführt:

- Verantwortliche und persönliche Haftung
  Während für die strategischen Aufgaben grundsätzlich der Vorstand (die Geschäftsführung/der Aufsichtsrat) zuständig und verantwortlich ist, sind bei den konzeptionellen und operativen Aufgaben auch Mitarbeiter (aufgrund ihrer Rolle als betrieblicher Datenschutzbeauftragter oder IT-Leiter) im Unternehmen für die Erfüllung von Pflichten bzw. bestimmte Regelung verantwortlich. Des Weiteren kann auch der einzelne Mitarbeiter davon betroffen sein, z. B. im Falle der Verwendung nicht ausreichend lizenzierter Software. Die jeweiligen Haftungsrisiken sind unterschiedlich. Bei Schäden durch die Pflichtverletzung oder durch die Nichtregelung haftet das Unternehmen und in besonderen Fällen auch der Vorstand. Der Mitarbeiter haftet gegenüber dem Unternehmen (und Dritten) im Rahmen seiner Rolle als Arbeitnehmer, siehe dazu ausführlich weitere Erläuterungen im Anhang auf Seite 15.

- Rechtsgrundlage
  In der Matrix ist für die Pflicht/den Regelungsbedarf auch die jeweilige Rechtsgrundlage aufgeführt. Existiert keine explizite Rechtsgrundlage so sollte daraus nicht der Schluss gezogen werden, dass kein Handlungsbedarf für den Verantwortlichen besteht. Das Urteil des OLG Hamm (siehe Einleitung) zeigt, dass es auch bei Fehlen einer ausdrücklichen Rechtsgrundlage (siehe „Operative Aufgaben, 6. Durchführung regelmäßiger Backups“) zu einer Schadensersatzhaftung kommen kann.

- Schäden und Nachteile für das Unternehmen, Ansprüche Dritter
  Die Schäden und Nachteile für das Unternehmen sind vielfältig. Je nach Umfang der Pflichtverletzung bzw. der Nichtregelungen können z. B. Datenverluste bzw. Ausfälle in der Produktion eintreten, Schadensersatzansprüche geltend gemacht werden. Zusätzlich zu diesen „bezifferbaren“ Schäden entsteht ein Imageschaden für das Unternehmen, der u. U. größere Auswirkungen auf Geschäftsbeziehungen zu Partnern und Kunden haben kann.

- Anmerkungen sowie ausgewählte Entscheidungen
  In der letzten Spalte der Matrix befinden sich weitere Erläuterungen sowie ausgewählte Entscheidungen zur jeweiligen Pflicht bzw. zum jeweiligen Regelungsbedarf. Diese erheben keinen Anspruch auf Vollständigkeit können eine qualifizierte Rechtsberatung nicht ersetzen. Sofern vorhanden, wird auf weitere BITKOM-Publikationen verwiesen, die das Thema detaillierter beschreiben.

Bei der Anwendung der Matrix ist die jeweilige Abhängigkeit des Unternehmens von der IT und der konkrete Zusammenhang des möglichen Haftungsrisikos zu betrachten. Bei einem Handwerksbetrieb mit einem Server können naturgemäß nicht derart hohe Schäden entstehen wie z. B. bei einem Online Broker. Existenz gefährdend können „unsichere“ IT-Systeme jedoch für beide Unternehmen sein. Für beide Unternehmen sind der Einsatz und die Verwendung ihrer IT auf jeden Fall kein „rechts- und sanktionsfreier“ Raum, wie die Matrix zeigt.

Legende:

	Verantwortlicher für die Pflicht/den Regelungs-/Handlungsbedarf
	Verantwortlicher hat Kontrollpflicht
	Persönliche Haftung des Verantwortlichen möglich
*AN	Persönliche Haftung des Arbeitnehmers nach den Grundsätzen der Arbeitnehmerhaftung (siehe Erläuterungen auf Seite 15)

2.1 Strategische Aufgaben

Nr.	Pflicht bzw. Regelungs-/ Handlungs-bedarf	Verant-wortlich-keiten		Persönliche Haftung ggü.		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarfs	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nicht-regelung	Ansprüche Dritter (z.B. Kunden, Be-troffene)	Anmerkungen sowie ausgewählte Entschei-dungen
		Vorstand/GF	Aufsichtsrat	Unternehmen	Dritten				
1.	Sicherstellung einer bedarfs- und rechtskon-formen IT-Nutzung					▪ Gesellschaftsrecht § 91 II AktG § 43 GmbHG ▪ (KonTraG)	▪ Unternehmensverluste durch Ausfall der Systeme ▪ Insolvenz ▪ Verteuerung der Unternehmenskredite ▪ Ggf. Verlust von Versicherungsschutz für das Unternehmens ▪ Imageschaden nach Verlust von personenbezogenen Daten aufgrund von Sicherheitslücken	▪ Schadensersatz	▪ Siehe Erläuterungen in der Einleitung zu Kapitel 2 ▪ Bietet ein Unternehmen über seinen Internetauftritt auch seine Produkte oder Dienstleistungen an, muss es vielfältige gesetzliche Pflichten beachten, Verstöße sind sanktionsbewehrt, zu diesem Themenkomplex siehe BITKOM-Publikation „Checkliste-Onlinegeschäft“ (Ausgabe: März 2005)
						▪ Gesellschaftsrecht § 116 AktG ▪ (KonTraG)			▪ Der Aufsichtsrat hat zu kontrollieren, ob der Vorstand alle erforderlichen Maßnahmen im Rahmen des Risi-komanagements getroffen hat. Führt er diese Kontrol-le unzureichend aus und treten erhebliche Schäden, insbesondere Insolvenz, ein, haftet auch der Auf-sichtsrat persönlich. ▪ Haftung nur bei mangelnder Kontrolle (BGH, NJW 1997, ARAG / Garmenbeck)
2	Bestellung eines betrieblichen Datenschutzbe-auftragten					▪ Datenschutzrecht § 4f, § 43, I und II BDSG).	▪ Bußgeld bis zu 25.000 EUR		▪ Eine Bestellung ist unverzüglich erforderlich wenn vier oder mehr Arbeitnehmer mit der Erhebung, Verarbei-tung oder Nutzung personenbezogener Daten be-schäftigt sind. ▪ Die Bestellung sollte dabei schriftlich erfolgen.

2.2 Konzeptionelle Aufgaben

Nr.	Pflicht bzw. Regelungs-/ Handlungs-bedarf	Verantwortlichkeiten			Persönliche Haftung ggü.		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarf	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nichtregelung	Ansprüche Dritter (z.B. Kunden, Betroffene)	Anmerkungen sowie ausgewählte Entscheidungen
		Vorstand/GF	betr. DSB	IT-Leiter	Unternehmen	Dritten				
1.	Einführung eines Sicherheitskonzepts (inkl. Katastrophen- und Zugriffsschutz) und eines Datenschutzkonzeptes						▪ Gesellschaftsrecht § 91 II AktG / § 43 GmbHG	▪ Unternehmensverluste durch Ausfall der Systeme ▪ Insolvenz ▪ Verlust von Daten aufgrund von Sicherheitslücken ▪ Ggf. Verlust von Versicherungsschutz für das Unternehmen ▪ Verteuerung der Unternehmenskredite	▪ Schadensersatz	▪ Delegierung möglich, aber Verantwortung für Kontrolle bleibt bei Unternehmensleitung ▪ Kontrolle sollte wegen der späteren Nachweisbarkeit dokumentiert werden. ▪ Siehe BITKOM-Leitfaden „Sicherheit für Systeme und Netze in Unternehmen“ ▪ Siehe BITKOM-Leitfaden „Kompass der IT-Sicherheitsstandards“
					*AN	*AN	▪ Datenschutzrecht §9 und Anlage zu § 9			▪ Sanktion: ggf. Abberufung des betriebl. DSB, s. u. 2.3. Ziffer 2 ▪ Ohne Datenschutzkonzept besteht die Gefahr weiterer Datenschutzverletzungen, s. u. 2.3. Ziff 2 ▪ Siehe Seite 15 im Anhang „Erläuterungen zur Arbeitnehmerhaftung“
					*AN	*AN	▪ Ergibt sich regelmäßig aus dem Arbeitsvertrag			
2.	Ständige Aktualisierung des Sicherheits-/ Datenschutzkonzepts				*AN	*AN	▪ s. o. Ziffer 1	▪ Unternehmensverluste durch Ausfall der Systeme ▪ Verlust von Daten aufgrund von Sicherheitslücken	▪ Schadensersatz	▪ Siehe Seite 15 im Anhang „Erläuterungen zur Arbeitnehmerhaftung“
					*AN	*AN				
3.	Regelungen beim Zugang von externen Dritten zu Datenverarbeitungssystemen						▪ Datenschutzrecht § 9 BDSG i.V.m. §823 BGB	▪ Zugang zu personenbez. Daten von unbefugten Dritten ▪ Imageschaden ▪ Ggf. Virenverseuchung bei Wartung, Fernwartung, Offshoring, Outsourcing	▪ Schadensersatz Zivilrecht § 280 I BGB, § 823 II BGB i.V.m. BDSG	▪ Klar geregelte Verträge mit externen Dritten z. B. bei Fernwartung, Outsourcing, Offshoring notwendig ▪ Technische und organisatorische Vorkehrungen bei dem Zugang von externen Dritten im Unternehmen notwendig ▪ siehe BITKOM-Publikation „Mustervertragsanlage zur Auftragsdatenverarbeitung“ ▪ Siehe Seite 15 im Anhang „Erläuterungen zur Arbeitnehmerhaftung“
					*AN	*AN				
					*AN	*AN				

Nr.	Pflicht bzw. Regelungs-/ Handlungs-bedarf	Verantwortlichkeiten			Persönliche Haftung ggü.		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarf	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nichtregelung	Ansprüche Dritter (z.B. Kunden, Betroffene)	Anmerkungen sowie ausgewählte Entscheidungen
		Vorstand/GF	betr. DSB	IT-Leiter	Unternehmen	Dritten				
4.	Professionelle Beschaffung von IT-Systemen und Durchführung von IT-Projekten						▪ Zivilrecht § 634 BGB § 437 / 634 BGB ▪ Handelsgesetzbuch § 377 HGB	▪ Beschaffung von fehlerhafter HW/SW ▪ Unternehmensverluste durch erheblich verzögerte oder gescheiterte Projekte, evtl. Ausfall essentieller IT-Systeme oder Datenverlust ▪ Verlust von Ansprüchen gegen Lieferant wegen unprofessioneller Abnahme	▪ Schadensersatz	▪ Beweislast für fehlerhafte Implementierung liegt nach Abnahme grundsätzlich beim Besteller ▪ Beweislast-Umkehr allerdings, wenn Implementierung eines Programms zur Datensicherung auf einer EDV-Anlage geschuldet ist und Auftragnehmer die gebotene Überprüfung der Sicherungsroutine unterlässt. vgl. BGH, 02.07.1996 (AZ: X ZR 64/94) = NJW 96, 2924 ff.
					*AN		▪ Zivilrecht § 280 BGB			▪ Siehe Seite 15 im Anhang „Erläuterungen zur Arbeitnehmerhaftung“
5.	Sicherung von Vertraulichkeit und Geheimhaltung						▪ Zivilrecht Vertragliche Vertraulichkeitsverpflichtung i.V.m. § 280 BGB, Vorvertraglich ggf. § 311, Abs. 2 BGB ▪ Sicherheitsüberprüfungsgesetz §2, 7-10 SüG	▪ Verlust von Entwicklungs-Know-how (Werkspionage) ▪ Imageschaden ▪ Ggf. Verlust von Geschäftspartnern ▪	▪ Schadensersatz ▪ Vertragsstrafe	▪ Umsetzung der besonderen vertraglichen und gesetzlichen Geheimhaltungsverpflichtungen

2.3 Operative Aufgaben

Nr.	Pflicht bzw. Regelungs-/ Handlungs-bedarf	Verantwortlichkeit				Persönliche Haftung ggü		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarfs	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nicht-regelung	Ansprüche Dritter (z.B. Kunden, Betroffene)	Anmerkungen sowie ausgewählte Entscheidungen
		Vorstand/GF	betr. DSB	IT-Leiter	Mitarbeiter	Unternehmen	Dritten				
1.	Ordnungsgemäße Abbildung der wirtschaftlichen Verhältnisse des Unternehmens in der Buchführung							▪ Handelsrecht § 239 Abs. 4 HGB Steuerrecht: § 146 Abs. 5 AO ▪ Gesellschaftsrecht § 91 II AktG	▪ Bestätigungsvermerk in der Jahresendprüfung wird nicht erteilt ▪ Bei nicht ordnungsgemäßer Buchführung Schätzung der Besteuerungsgrundlagen ▪ Imageschaden ▪ Geldstrafen, Bußgelder (§§ 331, 334 HGB) ▪ Finanzierungs- und Kreditbeeinträchtigungen	▪ Schadensersatzforderungen von Gläubigern und Anlegern	▪ Aufgrund von Bilanzskandalen in jüngster Vergangenheit ein zentrales Thema in der Geschäftsführung ▪ Neue Vorschriften entstehen: 10-Punkte-Programm der Bundesregierung "Zur Stärkung der Unternehmensintegrität und zum Anlegerschutz", Sarbanes Oxley Act u. a.
						*AN					
						*AN					
2.	Datenschutzrechtliche Konformität sicherstellen							▪ Datenschutzrecht § 7 BDSG / § 9 BDSG § 43 BDSG § 44 BDSG ▪ Gesetz gegen unlauteren Wettbewerb § 3, 4 Nr. 11 UWG § 10	▪ Aufsichtsbehörde kann Maßnahmen zur Beseitigung anordnen oder auch den Einsatz einzelner Verfahren untersagen, dadurch erhebliche Behinderungen bis hin zum Unternehmensstillstand, Produktionsausfall, sonstige Vermögensverluste, z.B. Ersatz bzw. Modifikation der Verfahren ▪ Kosten durch Pflicht zur Abberufung des DS-Beauftragten und Einsetzung eines neuen ▪ Bußgeld bis € 250.000 § 43 BDSG ▪ Zwangsgelder ▪ Freiheitsstrafe bis 2 Jahre Strafrecht § 203 StGB	▪ Schadensersatz Zivilrecht § 823, Abs. II BGB ▪ Unterlassung ▪ Abmahnung ▪ U. U. Gewinnabschöpfung § 10 UWG	▪ Datenschutz sollte Teil des Berechtigungskonzeptes sein ▪ Datenschutzkonzept nach § 9 BDSG erforderlich (s.o. 2.2. Ziff. 1)
						*AN	*AN	▪ Datenschutzrecht §§ 4g, 38, Abs. 5 BDSG			▪ U. U. kann die Aufsichtsbehörde die Abberufung des DSB verlangen

Nr.	Pflicht bzw. Regelungs-/ Handlungs-bedarf	Verantwortlichkeit				Persönliche Haftung ggü		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarfs	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nicht-regelung	Ansprüche Dritter (z.B. Kunden, Betroffene)	Anmerkungen sowie ausgewählte Entscheidungen
		Vorstand/GF	betr. DSB	IT-Leiter	Mitarbeiter	Unternehmen	Dritten				
3.	Einsatz von SPAM- und Viren-Filtern abwägen							▪ TKG § 88 TKG § 206 II Nr. 2 StGB ▪ Strafrecht § 85 II TKG i.V.m. § 206 II Nr. 2 StGB oder § 303 a StGB	▪ Schäden und Nachteile unterschiedlich, je nach Vorgehen der Unternehmensleitung: ▪ Verzicht auf E-Mail Filter: Haftung ggü. Dritten bei tatsächlichen Schäden (z.B. Datenverlust durch Viren) ▪ Einsatz von E-Mail Filter: u. U. rechtliche und praktische Probleme mit Mitarbeitern und Dritten ▪ Schaden durch Vernichtung wichtiger Information ▪ Freiheitsstrafe bis zu 5 Jahren oder Geldstrafe	▪ Unterlassung ▪ Schadensersatz Zivilrecht § 823 Abs. 2 BGB § 1004 BGB i.V.m. § 40 TKG ▪ Schadensersatz ▪ Kosten bei Unterlassungsklage, evtl. einstweiligem Verfügungsverfahren bzw. Abmahnung	▪ Hilfreich ist, wenn eine Einwilligung der Mitarbeiter für das Filtern von E-Mail vorliegt, z. B. im Arbeitsvertrag. ▪ OLG Karlsruhe, 10.1.2005 (AZ: 1 Ws 152/04) ▪ Siehe Seite 15 im Anhang „Erläuterungen zur Arbeitnehmerhaftung“
						*AN	*AN				
						*AN	*AN				
4.	Regelung für die Nutzung von E-Mail und Internet am Arbeitsplatz							▪ Grundgesetz Art.2 i.V.m. Art.1 ▪ Zivilrecht §§ 611, 242 BGB ▪ Datenschutzrecht §§ 1 II; 27 I BDSG ▪ Telekommunikationsgesetz §§ 1, 88, 89, 91ff TKG ▪ Teledienstegesetz §§ 1f. TDG ▪ Teledienstedatenschutzgesetz §§ 3-6 TDDSG. ▪ Ggf. Betriebsverfassungsgesetz §§ 75, 80, 87, 88, 90 BetrVG	▪ Verstöße gegen Datenschutzvorschriften ▪ Mangelnde Transparenz/Mangelnde Kontrollmöglichkeiten ▪ Kosten durch die Dienstenutzung durch die Mitarbeiter ▪ Imageschäden ▪ Beschlagnahme		▪ siehe BITKOM-Leitfaden „Die Nutzung von E-Mail und Internet am Arbeitsplatz“
						*AN	*AN				
						*AN	*AN				

Nr.	Pflicht bzw. Regelungs-/ Handlungs-bedarf	Verantwortlich-keit				Persönliche Haftung ggü		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarfs	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nicht-regelung	Ansprüche Dritter (z.B. Kunden, Betroffene)	Anmerkungen sowie ausgewählte Entscheidungen
		Vorstand/GF	betr. DSB	IT-Leiter	Mitarbeiter	Unternehmen	Dritten				
5.	**Verhinderung von Schädigung Dritter durch firmeneigene IT**							▪ Gesellschaftsrecht § 91 II AktG / § 43 GmbHG ▪ §§ 823, 1004, 280 BGB	▪ Imageschaden ▪ Ggf. Verlust von Geschäftspartnern ▪ Schadensersatz- und Unterlassungs-ansprüche	▪ Unterlassung § 1004 BGB ▪ ggf. Schadensersatz §§ 823, 280 I BGB	▪ Teil des Sicherheitskonzepts (Ziff. 1) ▪ Einsatz von Firewalls, Virenscan-nern etc. zur Prävention ▪ Zur Überwachung der Internet-Nutzung siehe auch BITKOM-Leitfaden „Die Nutzung von E-Mail und Internet am Arbeitsplatz“
						*AN	*AN	▪ Zivilrecht §§ 823, 1004, 280 BGB			
	insbesondere **Virenfreier Daten-/ Datenträgeraus-tausch**							▪ Datenschutzrecht § 9 BDSG ▪ Zivilrecht §§ 823, 1004 BGB § 280 I BGB	▪ Nichtverfügbarkeit von betrieblichen, personenbezogenen oder persön-lichen Daten ▪ Ungewollte Weiterverbreitung von betrieblichen, personenbezogenen oder persönlichen Daten ▪ Unternehmensstillstand ▪ Produktionsausfall ▪ Vermögensverluste ▪ Imageschäden ▪ Schädigung Dritter durch Verbreitung von Viren	▪ Schadensersatz Zivilrecht § 280 BGB § 823 BGB	▪ Grundsätzlich besteht Verbot der Schädigung Dritter durch Viren etc. grundsätzlich besteht aber auch Pflicht für Empfänger elekt-ronischer Daten zum Einsatz von Virenschutzprogrammen. ▪ Gerichte sprechen deshalb mehr-fach keinen Schadenersatz we-gen Mitverschuldens des Emp-fängers zu. vgl. LG Kleve, 29.06.1995 (AZ: 7 O 17/95) = CR 96, 292 ff., LG Köln, 21.07.1999 (AZ: 20 S 5/99) = CR 00, 362, LG Hamburg, 18.07.2001 (AZ: 401 O 63/00) = NJW 01, 3486
						*AN	*AN				▪ Siehe Seite 15 im Anhang „Erläu-terungen zur Arbeitnehmerhaf-tung“
						*AN	*AN				

Nr.	Pflicht bzw. Regelungs-/ Handlungs-bedarf	Verantwortlich-keit				Persönliche Haftung ggü		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarfs	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nicht-regelung	Ansprüche Dritter (z.B. Kunden, Betroffene)	Anmerkungen sowie ausgewählte Entscheidungen
		Vorstand/GF	betr. DSB	IT-Leiter	Mitarbeiter	Unternehmen	Dritten				
6.	Durchführung regelmäßiger Backups								▪ Erhebliche Behinderungen bis hin zum Unternehmensstillstand bei Datenverlusten ▪ Produktionsausfall ▪ Sonstige Vermögensverluste ▪ Imageverlust ▪ Datenverlust ▪ Wegen überwiegenden Mitverschuldens auch kein Schadensersatz von Dritten, die Datenverluste verursachen	▪ Schadensersatz von Vertragspartnern Zivilrecht §§ 280 I / § 254 BGB (nur ggü. Dritten)	▪ OLG Hamm, Urteil vom 01.12.2003, 13 U 133/03 (Fundstellen: MMR 2004, 487, CR 2004, 654)
						*AN	*AN				▪ Ergibt sich regelmäßig aus dem Arbeitsvertrag ▪ Siehe Seite 15 im Anhang „Erläuterungen zur Arbeitnehmerhaftung“
						*AN	*AN				
7.	Verwendung lizenzierter Software							▪ Urheberrecht §§ 97 ff. i.V.m. § 100 UrhG ▪ Gesellschaftsrecht § 91 II AktG / § 43 GmbHG	▪ Unternehmensstillstand, Produktionsausfall durch staatsanwaltliche Handlung (Beschlagnahme, Hausdurchsuchung, etc.) oder durch zivilrechtliche Unterlassungsverfügung ▪ Sachverlust durch Einziehung bzw. Herausgabeverpflichtung ▪ Imageschaden ▪ Lizenzgebühr für Nutzung in der Vergangenheit, weitere Vermögensverluste ▪ Bei Verstoß gegen OS-Lizenzbedingungen, z.B. GPL Rechtsverlust mit Folgeproblemen wie zusätzliche Lizenzkosten , Kosten für Nachlizenzierung bei Kunden etc.	▪ Einziehung Hardware / Unterlassung / Lizenzgebühren ▪ Bei Vorsatz oder Fahrlässigkeit: Schadensersatz (§§ 97 ff UrhG, §§ 823, 812 BGB)	▪ Haftung ggü. Lizenzgeber z.B. bei planmäßiger Lizenzüberschreitung „over use“ ▪ Bei Verstoß gegen GPL entfallen Rechte auf kostenlose Nutzung und Weitergabe daraus: LG München, 19.5.2004, AZ: 21 O 6123/04, Fundstellen: MMR 2004, 693, GRUR-RR 2004, 350)
						*AN	*AN				
8.	Einhaltung der Urheberrechte (insbes. auch bei vermeintlich freier Software wie OSS)					*AN	*AN	▪ Urheberrecht §§ 97 ff.		▪ Eigenhaftung der Mitarbeiter bei Verschulden ▪ Bußgeld o. Geld- bzw. Freiheitsstrafe Urheberrecht §§ 97 ff. i.V.m. ▪ Lizenzgebühren	

Anhang

- Erläuterungen zur Arbeitnehmerhaftung

Die Arbeitnehmerhaftung bei Arbeiten, die durch den Betrieb veranlasst sind, ist gesetzlich nur allgemein, im Detail durch eine umfangreiche Rechtsprechung geregelt. Voraussetzungen für eine Arbeitnehmerhaftung ist zunächst eine schuldhaft begangene Pflichtverletzung (Schlechterfüllung, unerlaubte Handlung) im Rahmen eines bestehenden Arbeitsverhältnisses, die den Arbeitnehmer zum Schadensersatz verpflichtet.
Für alle Arbeiten, die durch den Betrieb veranlasst sind und auf Grund eines Arbeitsverhältnisses geleistet werden, gelten dann die „Grundsätze über die Beschränkung der Arbeitnehmerhaftung“. Diese haben bestimmte Rechtsfolgen:

- Ist der Schaden auf leichteste und leichte Fahrlässigkeit zurückzuführen, haftet der Arbeitnehmer gar nicht.
- Bei normaler („mittlerer“) Fahrlässigkeit ist der Schaden in aller Regel zwischen Arbeitgeber und Arbeitnehmer quotal zu verteilen ist, wobei die Gesamtumstände von Schadensanlass und Schadensfolgen nach Billigkeitsgrundsätzen und Zumutbarkeitsgesichtspunkten gegeneinander abzuwägen sind. Ein Kriterium ist dabei auch die Höhe der Entlohnung. Zumeist führt dies zu einem Höchstbetrag (z.B. zwei Monatsgehälter), über den hinaus der Arbeitnehmer nicht gegenüber dem Arbeitsgeber einzustehen hat.
- Bei grober Fahrlässigkeit des Arbeitnehmers hat dieser in aller Regel den gesamten Schaden zu tragen, eine Haftungserleichterung zu seinen Gunsten ist aber nicht ausgeschlossen, jedoch von einer Abwägung im Einzelfall abhängig.
- Vorsätzlich verursachte Schäden hat der Arbeitnehmer grundsätzlich in vollem Umfang zu tragen.

Die oben geschilderten Grundsätze gelten nur im Innenverhältnis zwischen dem Arbeitgeber und dem Arbeitnehmer. Schädigt der Arbeitnehmer im Rahmen seiner betrieblichen Tätigkeit einen Vertragspartner oder einen sonstigen außen stehenden Dritten, dann haften Arbeitgeber und Arbeitnehmer als sog. Gesamtschuldner. In diesen Fällen kann der Dritte seinen Schaden sowohl gegenüber dem Arbeitgeber als auch gegenüber dem Arbeitnehmer geltend machen kann.

Danksagung

Der vorliegende Leitfaden entstand in der BITKOM-Projektgruppe „Haftungsrisiken“ des Kompetenzbereiches Sicherheit.

Wir danken allen Mitgliedern der Projektgruppe und des Arbeitskreises Sicherheitsmanagenent für die Initiierung des Themas und die zahlreichen Anregungen. Besonderer Dank gilt den federführenden Autoren der erläuterten Rechtspflichten für ihre Textbeiträge und wissenschaftliche, rechtliche Diskussion, die diesen Leitfaden erst ermöglichten:

- Bernd H. Harder (Harder Rechtsanwälte)
- Gerold Hübner (Microsoft Deutschland GmbH)
- Norman Müller (Rechtsanwälte Wendler Tremml) sowie
- Dr. Kai Kuhlmann (BITKOM e.V.)

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 - 0
Fax: 030/27 576 - 400

bitkom@bitkom.org
www.bitkom.org