RECHTSANWÄLTE
FALKNER & HARTENFELS

www.falknerhartenfels.de

IT-Sicherheit

Auch und gerade ein rechtliches Thema

Tag der IT-Sicherheit, IHK Rhein-Neckar

Mannheim, 09.07.2014
Rechtsanwalt Klaus-Christian Falkner, Mag. rer. publ.

RECHTSANWÄLTE
FALKNER & HARTENFELS

www.falknerhartenfels.de

Inhalt

Das Zauberwort …

… zum Thema IT-Sicherheit aus rechtlicher Sicht heißt:

19.03.2014
Unzureichendes Compliance-System

Vorstandsmitglied auf Schadensersatz in Höhe von 15 Mio. EUR verurteilt

Erstmals hat ein deutsches Gericht den Geschäftsleiter eines deutschen Unternehmens wegen eines unzureichenden Compliance-Systems auf Schadensersatz in Millionenhöhe verurteilt. Spätestens seit diesem Urteil muss sich jedes Unternehmen ernsthaft mit der Einrichtung eines

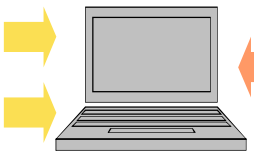
Quelle: http://www.haufe.de/recht/weitere-rechtsgebiete/wirtschaftsrecht/lg-muenchen-i-verurteilt-vorstandsmitglied_210_226942.html

1 Einleitung

IT-Sicherheit umfasst nicht nur technische und organisatorische, sondern zunehmend auch rechtliche Aspekte.

IT-Organisation
- IT-Risiko-Management
- Datenschutzbeauftragter
- IT-Sicherheitsbeauftragter
- …

Sicherheitstechnologie
- IT-Sicherheitsarchitektur
- IDS, IPS, Firewall,
- Gebäudesicherheit
- …



IT-Sicherheit

Rechtlicher Rahmen
- Zivilrecht
- Öffentliches Recht
- Strafrecht
- Verträge

2 Überblick über einige Rechtsgrundlagen

Vorschriften mit Bezug zur IT-Sicherheit

Unternehmens- / Gesellschaftsrecht	KonTraG
Urheberrecht	UrhG
Handels- und Steuerrecht	HGB, AO, GoBS, GDPdU
Wirtschafts-verwaltungsrecht	GewO, TKG, MaRisk
Datenschutzrecht	BDSG, TMG
Strafrecht	StGB, UrhG, UWG, BDSG

2.1 Unternehmens- / Gesellschaftsrecht

KonTraG
(Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)

- Ziele u.a.:
  - Erhöhung der Transparenz
  - Verbesserung der Abschluss-prüfung und Beurteilung der Unternehmenslage
- seit 01.05.1998 in Kraft
- Änderungen in AktG, HGB, u.a.

gilt für

große & mittelgroße Kapitalgesellschaften

aber auch für

prüfungspflichtige OHG und KG

Unternehmens- / Gesellschaftsrecht (2)

KonTraG
(Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)

§ 91 Abs. 2 AktG

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

Erfordert System zur Risiko-früherkennung

IT-Sicherheit

- Verfügbarkeit
- Disaster Recovery
- Business Continuity
- Datenauthentizität und -integrität
- Revisionssicherheit
- Missbrauchsschutz
- etc.

Exkurs: Bring Your Own Device

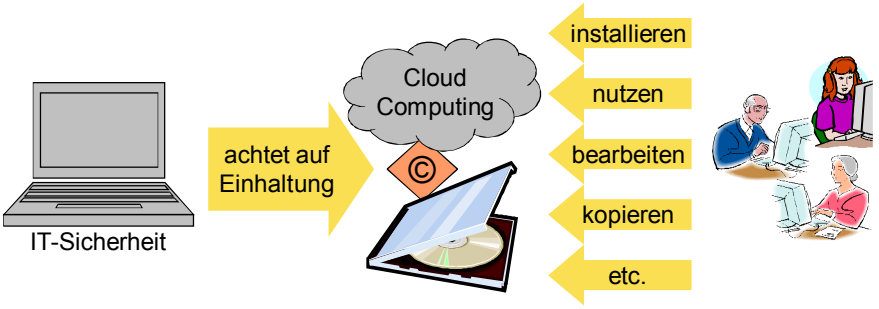
Wer trägt die Verantwortung für den Geräte-Zoo?

Ein paar Problemfelder

- Nutzungsrechte
- Datenzugriff
- Datensicherheit
- Unveränderbarkeit der Daten
- Verfügbarkeit, Wiederherstellbarkeit und Lesbarkeit
- Archivierung
- Schutz gegen Malware
- Trennung von Privatem und Beruflichem
- Herausgabepflichten beim Ausscheiden

2.2 Urheberrecht

Unternehmen sind dafür verantwortlich, nur solche Software und sonstiges urheberrechtliches Material zu verwenden, für die bzw. das sie auch die nötigen Rechte besitzen.



Urheberrecht (2)

Bei Urheberrechtsverstößen haftet das Unternehmen.

Zivilrecht	OWi-/Strafrecht
• Unterlassungsanspruch • Vernichtungsanspruch • Auskunftsanspruch • Schadensersatzanspruch	• Bußgeld bis zu 50.000 € • Geldstrafe • Freiheitsstrafe bis zu 3 bzw. 5 Jahren

Urheberrecht (3)

Zur IT-Sicherheit gehören geeignete Maßnahmen, die Schutzrechtsverletzungen zuverlässig unterbinden.

Kostenlose Arbeitshilfe: BSA Ratgeber zum Risikomanagement
http://ww2.bsa.org/country/Tools and Resources.aspx

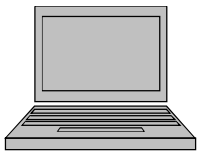
2.3 Handels- und Steuerrecht

Aus dem Handels- und Steuerrecht ergeben sich vor allem Anforderungen an die elektronische Buchführung.

HGB	• Bilanzierungsvorschriften der §§ 238 ff. HGB • §§ 257, 261 HGB: Speicherung von aufbewahrungspflichtigen Unterlagen auf Datenträgern
AO	• Buchführungs- / Aufzeichnungsvorschriften der §§ 140 ff. AO • § 147 AO: Speicherung von aufbewahrungspflichtigen Unterlagen auf Datenträgern
GoBS (07.11.1995)	• Stellen Anforderungen an IT-gestützte Buchführung • Konkretisieren die gesetzlichen Anforderungen • Keine technologischen Vorgaben
GDPdU (16.07.2001)	• Gelten neben den GoBS • Regeln den Datenzugriff der Finanzverwaltung auf Buchführungssysteme des Steuerpflichtigen sowie Anforderungen an digitale Unterlagen und deren Archivierung

Handels- und Steuerrecht (2)

Die gesetzlichen Vorgaben bestimmen nur, welche Anforderungen erfüllt sein müssen. Die technische Umsetzung obliegt allein den Unternehmen.



IT-Sicherheit

Umsetzung
- HGB
- AO
- GoBS
- GDPdU

Auswahl von Anforderungen

- Unveränderbarkeit der Daten
- Jederzeitige Verfügbarkeit, Wiederherstellbarkeit und Lesbarkeit
- Erstellung und Pflege einer Verfahrensdokumentation
- Datensicherheitskonzept
- Archivierung nur in maschinell auswertbaren Formaten (z.B. kein einfaches PDF)

2.4 Wirtschaftsverwaltungsrecht

IT-Sicherheit

GewO
- Gewerbeuntersagung wegen Unzuverlässigkeit
- Auch bei mangelhafter IT-Sicherheit möglich

TKG
- technische Schutzmaßnahmen
- Sicherheitsbeauftrager
- Sicherheitskonzept

Basel II / III
- Differenzierte Risikobemessung bei Kreditvergabe
- IT-Sicherheit stellt operationelles Risiko dar

2.5 Datenschutzrecht

Auch aus dem Datenschutzrecht ergeben sich Anforderungen an die IT-Sicherheit.

BDSG

- § 9 BDSG fordert technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes (sog. „TOMs“)
- Konkretisierung in Anlage zu § 9 BDSG

IT-Sicherheit

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

Datenschutzrecht (2)

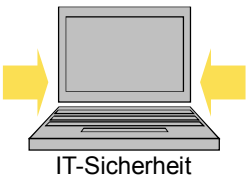
Spezialregelungen zu

Telemedien
(Internet, Telebanking, etc.)

Telekommunikation

TMG

- § 13 Abs. 4: Katalog technischer und organisatorischer Vorkehrungen
- Von Providern einzuhalten
- Bußgeld bis 50.000 €



IT-Sicherheit

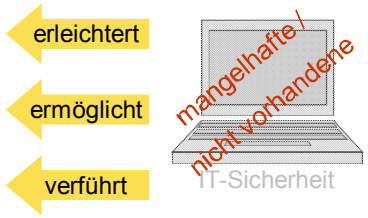
TKG

- § 107 Abs. 2: technische und organisatorische Maßnahmen gegen unbefugtes Offenbaren von Nachrichteninhalten
- Regelmäßige Anpassung an den Stand der Technik

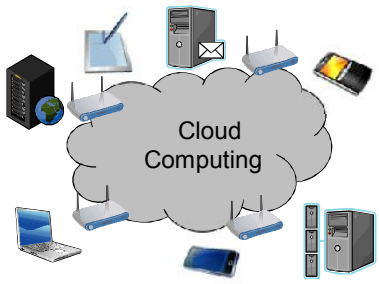
2.6 Strafrecht

Mögliche Straftatbestände

- Verletzung des Post- oder Fernmelde-geheimnisses (§ 206 StGB)
- Verletzung von Privatgeheimnissen (§ 203 StGB)
- Unerlaubte Verwertung urheberrechtlich geschützter Werke (§ 106 UrhG)
- Unerlaubter Eingriff in technische Schutzmaßnahmen (§ 108 b UrhG)
- Verrat von Geschäfts- und Betriebs-geheimnissen (§ 17 UWG)



Exkurs: Cloud Computing



News-Meldung vom 28.04.2014 13:26 Uhr < Vorige | Nach

US-Internetunternehmen müssen im Ausland gespeicherte Daten herausgeben

vorlesen / MP3-Download

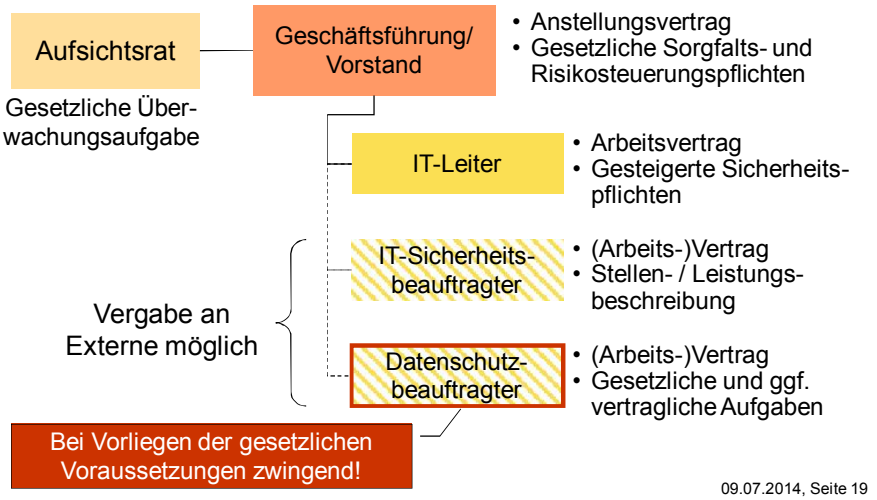
Dem Urteil eines amerikanischen Bundesgerichts zufolge sind US-Internetunternehmen selbst dann zur Datenherausgabe verpflichtet, wenn sich die Server des speichernden Unternehmens nicht in den Vereinigten Staaten befinden.

Quelle: http://www.heise.de/ix/meldung/US-Internetunternehmen-muessen-im-Ausland-gespeicherte-Daten-herausgeben-2178454.html

Ein paar Problemfelder

- Eigentum / Nutzungsrechte
- Datenzugriff / Speicherort
- Datensicherheit / Berufsrecht
- Datenschutz (Auftragsdaten-verarbeitung)
- Unveränderbarkeit der Daten
- Verfügbarkeit, Wiederherstell-barkeit und Lesbarkeit
- Archivierung
- Insolvenzfestigkeit
- Herausgabepflichten bei Vertragsende

3 Zuständigkeiten im Unternehmen



Exkurs: Datenschutzbeauftragter

Voraussetzung	• Betriebe, die mehr als 9 Mitarbeiter mindestens vorübergehend mit automatisierter Datenerhebung, -verarbeitung oder -nutzung beschäftigen • In Sonderfällen unabhängig von der Beschäftigtenzahl
Profil	• Fachkunde (z.B. besondere Qualifikation, Kenntnis der Unternehmensstrukturen, externe Unterstützung) • Zuverlässigkeit (z.B. persönliche Integrität, kein Interessenkonflikt)
Rolle	• Kein Mitglied der Geschäftsführung • Der Geschäftsführung unmittelbar unterstellt • In der Ausübung seiner Fachkunde weisungsfrei
Aufgabe	• Überwacht den Umgang mit personenbezogenen Daten • Ansprechpartner für Datenschutzfragen • Führt Verfahrensübersicht

gemäß §§ 4f - 4g BDSG

RECHTSANWÄLTE FALKNER & HARTENFELS

www.falknerhartenfels.de

4 Konsequenzen mangelnder IT-Sicherheit

Überblick*	Unterlassung	Auskunft	Schadensersatz	Amtskontrolle	Untersagung	Bußgeld	Geld-/Haftstrafe
Unternehmens- / Gesellschaftsrecht			●				
Urheberrecht	●	●	●			●	●
Handels- und Steuerrecht			●	●		●	
Wirtschafts-verwaltungsrecht				●	●	●	●
Datenschutzrecht			●	●		●	●
Strafrecht						●	●

* Es sind nur die wichtigsten, wahrscheinlichsten Konsequenzen aufgezeigt. Abhängig vom Einzelfall kommen für alle Rechtsgebiete nahezu alle Rechtsfolgen in Betracht.

RECHTSANWÄLTE FALKNER & HARTENFELS

www.falknerhartenfels.de

Konsequenzen mangelnder IT-Sicherheit (2)

Vorstand

§ 91 Abs. 2 AktG

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

§ 93 Abs. 2 AktG

„Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so trifft sie die Beweislast."

GmbH-Geschäftsführer haften gemäß § 43 GmbHG, Aufsichtsräte gemäß § 116 AktG!

RECHTSANWÄLTE FALKNER & HARTENFELS

www.falknerhartenfels.de

Konsequenzen mangelnder IT-Sicherheit (3)

IT-Leiter
- Arbeitsrecht
- Schadensersatz

IT-Sicherheits-beauftragter

Datenschutz-beauftragter
- Arbeitsrecht (intern) bzw. allg. Vertragsrecht (extern)
- Schadensersatz


- Verlust von Versicherungsschutz
- Rufschädigung

RECHTSANWÄLTE FALKNER & HARTENFELS

www.falknerhartenfels.de

5 Handlungsbedarf im Unternehmen

- IT-Sicherheit ist kein Produkt! IT-Sicherheit ist Chefsache!
- Überblick über Anforderungen verschaffen
- IT-Administratoren stärken
- Mitarbeiter schulen (Umgang mit E-Mails, Social Media, BYOD, Social Engineering, …)
- Datenschutzbeauftragten und ggf. IT-Sicherheitsbeauftragten ernennen
- Technische Maßnahmen ergreifen (Backup, Firewall, Antivirensoftware, IDS, IPS, DLP, DMZ, USV, Gebäudesicherheit, …)
- …

Handlungsmaßstab: aktueller Stand der Technik
Hilfe: BSI Grundschutz
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

RECHTSANWÄLTE FALKNER & HARTENFELS

www.falknerhartenfels.de

Handlungsbedarf im Unternehmen (2)

IT-Sicherheit

Organisation

- IT-Sicherheitskonzept aufstellen, implementieren und pflegen
- IT-Nutzungsordnung für Mitarbeiter aufstellen (Mitbestimmung!)
- IT-Audit beauftragen

Technologie

- IT-Systeme gegen Angriffe von außen und innen absichern
- Regelmäßige Datensicherung
- Redundante IT-Systeme
- Filter- und Überwachungssoftware einsetzen

Vorsicht: Arbeits-, Datenschutz- und Strafrecht beachten

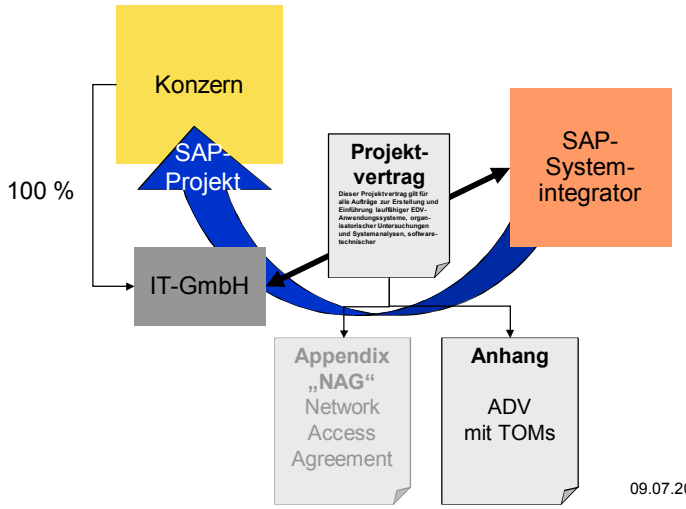
RECHTSANWÄLTE FALKNER & HARTENFELS

www.falknerhartenfels.de

6 Praxisbeispiele

- Einführung von SAP
- Ausgründung der IT-Abteilung im Konzern
- Richtlinie zur Nutzung von Social Media

6.1 Einführung von SAP



Einführung von SAP (2)

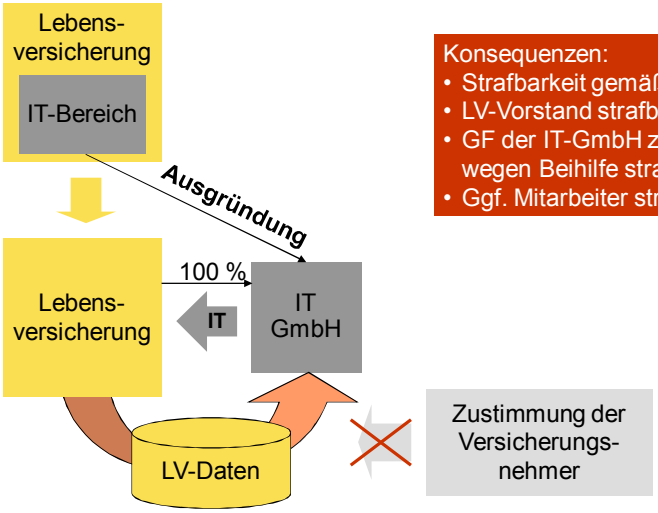
IT-Projektverträge, die personenbezogene Daten betreffen, kommen meist nicht mehr ohne eine ADV-Anlage aus.

§ 11 BDSG	• 10-Punkte-Katalog muss vertraglich geregelt werden • Abs. 5: „… *wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.*“ • Bußgeld bewehrt
Anhang zu § 9 BDSG	• Detaillierte technisch-organistorische Vorgabe • Werden gern vom Kunden vorgeben, sollten aber eigener IT-Realität entsprechen

RECHTSANWÄLTE FALKNER & HARTENFELS

www.falknerhartenfels.de

6.2 Ausgründung der IT-Abteilung



Konsequenzen:
- Strafbarkeit gemäß § 203 StGB
- LV-Vorstand strafbar
- GF der IT-GmbH zumindest wegen Beihilfe strafbar
- Ggf. Mitarbeiter strafbar

Zustimmung der Versicherungs-nehmer

RECHTSANWÄLTE FALKNER & HARTENFELS

www.falknerhartenfels.de

6.3 Richtlinie zur Nutzung von Social Media

Was passiert, wenn statt-dessen Betriebsgeheimnisse im Netz stehen oder Anlass für eine Abmahnung durch Wettbewerber gegeben wird?

Social Media Guide (Mitbestimmung!)
- Einführung
- Anwendungsbereich der Richtlinie
- Abgrenzung der Privatnutzung
- Hinweise
- Empfehlungen
- Verbindliche Handlungsanweisungen
- Kontrolle

7 Zusammenfassung

- IT-Sicherheit ist gesetzlich vorgeschrieben.
- Die gesetzlichen Anforderungen sind in den unterschiedlichsten Vorschriften enthalten.
- Nicht alle die IT-Sicherheit betreffenden Regelungen gelfür alle Unternehmen gleichermaßen.
- Mangelnde IT-Sicherheit kann auch aus rechtlicher Sicht existenzbedrohend sein.
- In jedem Unternehmen besteht Handlungsbedarf.
- Fazit: IT-Sicherheit ist Chefsache! Trotzdem ist Delegation möglich, auch an Externe.

RECHTSANWÄLTE FALKNER & HARTENFELS
www.falknerhartenfels.de

Glossar

AO	= Abgabenordnung
AktG	= Aktiengesetz
Basel II / III	= Eigenkapitalrichtlinien
BDSG	= Bundesdatenschutzgesetz
GDPdU	= Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GewO	= Gewerbeordnung
GmbHG	= Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GoBS	= Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme
HGB	= Handelsgesetzbuch
KonTraG	= Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
OWi	= Ordnungswidrigkeit
StGB	= Strafgesetzbuch
TMG	= Telemediengesetz
TKG	= Telekommunikationsgesetz
UrhG	= Urheberrechtsgesetz
UWG	= Gesetz gegen unlauteren Wettbewerb

Aktuelle Gesetzestexte:
www.gesetze-im-internet.de

Vielen Dank für Ihre Aufmerksamkeit!

Rechtsanwälte Falkner & Hartenfels
RA Klaus-Christian Falkner, Mag. rer. publ.
Im Hosend 10
69221 Dossenheim
Tel.: 0 62 21 – 8 89 08 66
Fax: 0 62 21 – 8 89 08 99
falkner@falknerhartenfels.de
www.falknerhartenfels.de