

Wolfgang Straßer
Geschäftsführer
Dipl.-Kfm.



IT-Sicherheitsmanagement und Haftungsrisiken für Geschäftsführer

@-yet Geschäftsbereiche



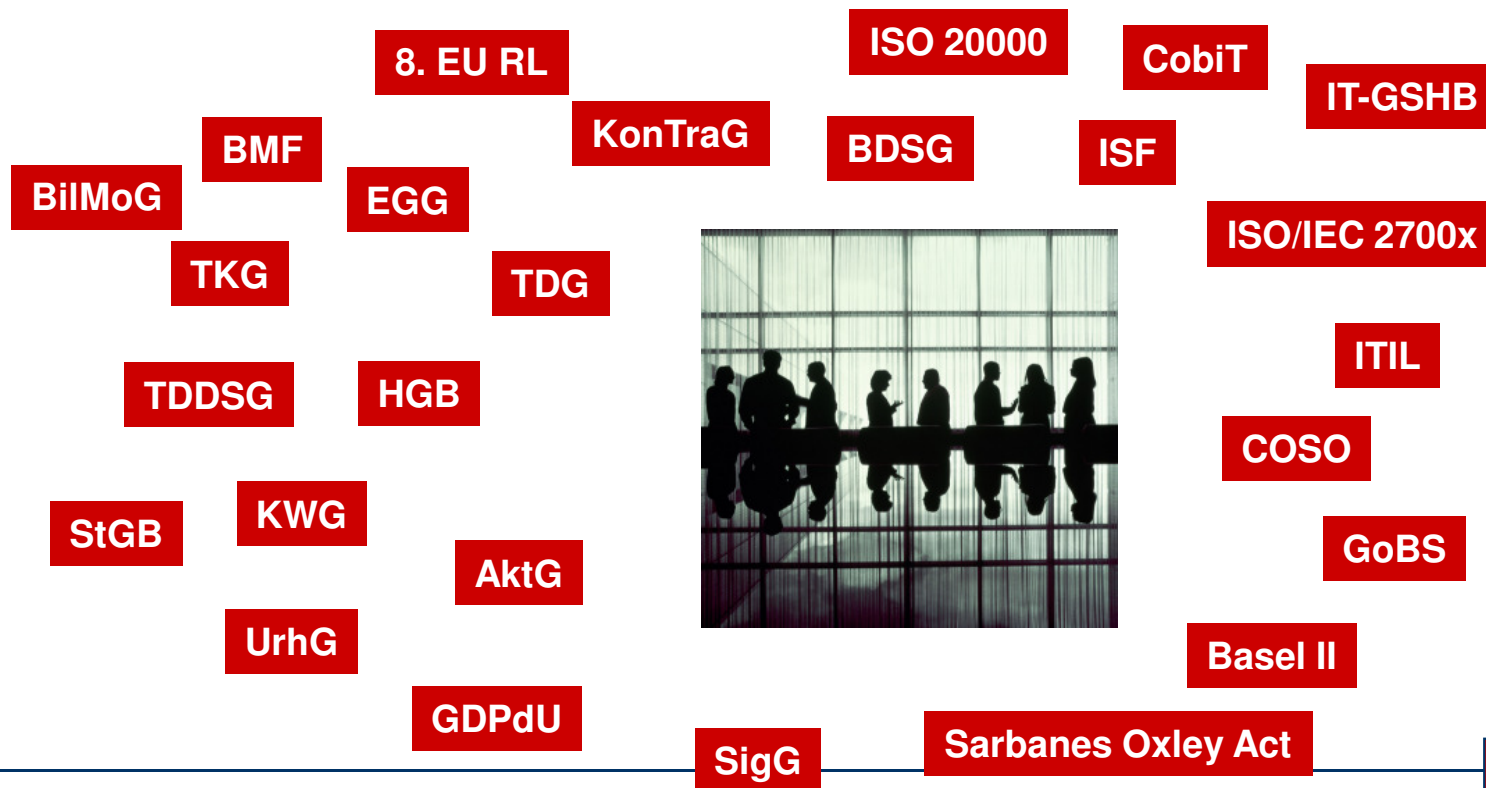
IT-Risikomanagement ist kein Selbstzweck

✓ Warum IT-Risikomanagement?

- Schutz vor Ausfällen/Stillständen
 - Produktion
 - Auslieferung etc.
- Schutz vor Know-how-Verlust
- Schutz vor dem Gesetzgeber
 - Compliance

Überblick

- der regulatorische Dschungel mit Bezug auf IT-Sicherheit (Auszug):



Haftungskonstellationen

- ✓ zivilrechtliche Haftung gegenüber dem eigenen Unternehmen
- ✓ zivilrechtliche Haftung gegenüber Dritten
- ✓ strafrechtliche Verantwortlichkeit

Haftungsfallen -1-

- Datenspeicherung
 - Bsp.: Aufbewahrungspflicht für E-Mails
 - Aufbewahrungspflicht für „Handelsbriefe“ (§ 257 HGB)
 - Aufbewahrungspflicht für „Handels- und Geschäftsbriefe“ (§ 147 AO)
 - Aufbewahrungsdauer: 6 Jahre ab Ende des Kalenderjahres, in dem Handels- oder Geschäftsbrief empfangen oder verschickt worden ist.
 - Art der Aufbewahrung
 - Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
 - Grundsätze DV-gestützter Buchführungssysteme (GoBS)

Haftungsfallen -2-

- **Datenschutz**
 - § 9 BDSG i.V. mit der Anlage zu § 9 BDSG:
 - insbesondere: Verpflichtung zur Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle
 - **Schutz von Arbeitnehmerdaten**
 - Unternehmen wird zum TK-Diensteanbieter, wenn es private E-Mails erlaubt
 - Problem: Kontrolle/Ausfilterung von E-Mails
 - strafrechtliche Risiken (Störung des Fernmeldeverkehrs [§ 206 StGB]; Datenunterdrückung [§ 303a StGB])
 - **Textziffer 5 GoBS**
 - Verpflichtung der Buchungspflichtigen zu Datensicherungsmaßnahmen gegen unberechtigte Kenntnisnahme

Haftungsfallen -3-

- Datensicherheit
 - Sind die Unternehmensdaten nach dem Stand der Technik gegen Verlust/Beschädigung gesichert?
 - § 9 BDSG i.V.m. Ziff. 9 der Anlage zu § 9 BDSG:
 - Verpflichtung zur Verfügbarkeitskontrolle
 - § 91 Abs. 2 AktG:
 - Verpflichtung zu geeigneten Maßnahmen, um Fortbestand der Gesellschaft zu sichern -> IT-Risikomanagement gegen Datenverlust

Haftungsfallen -4-

- Textziffer 5 GoBS
 - Verpflichtung des Buchungspflichtigen zu Datensicherungsmaßnahmen gegen Vernichtung, Diebstahl und Unauffindbarkeit

- Bsp: OLG Hamm, Urteil vom 1.12.2003 - 13 U 133/03 für Datensicherung in einem Reisebüro:
 - „...Die Sicherung hätte täglich erfolgen müssen, die Vollsicherung mindestens einmal wöchentlich.
 - ... hat der Sachverständige zu Recht entnommen, dass die Sicherung von Daten im Betrieb der Bekl. schon grob fahrlässig (blauäugig) vernachlässigt wurde. Nach dessen Bekundungen kann davon ausgegangen werden, dass nicht einmal eine monatliche Komplettsicherung erfolgte.“

Haftungsfallen -5-

- Bestehen Sicherungsmechanismen die die Verbreitung von Viren an Dritte nach dem Stand der Technik verhindern?
 - Bsp.: AG Köln, DuD 2001, 298:
 - Pflichtverletzung kann darin bestehen, „entweder keine Schutzmechanismen gegen Virenbefall zu verwenden oder aber trotz bekannten Virenbefall zu einer Weiterverbreitung beizutragen.“

Haftungsfallen -6-

- IT Infrastruktur
 - § 91 Abs. 2 AktG:
 - Verpflichtung zu geeigneten Maßnahmen, um den Fortbestand der Gesellschaft zu sichern -> Schaffung sicherer Netzinfrastrukturen
 - Hat Ihre IT-Infrastruktur ausreichende Kapazitäten?
 - Ist Ihre IT-Infrastruktur angemessen gegen Ausfallrisiken gesichert?
 - Haben Sie Ihren Outsourcing-Partner sorgfältig und fachkundig ausgewählt?
 - Haben Sie ausreichende vertragliche Regelungen mit Ihren Outsourcing-Partnern?

Haftungsfallen -7-

- Gewerbliche Schutzrechte
 - Sind Sie sicher, dass Ihr Unternehmen über alle erforderlichen Software-Lizenzen verfügt?
 - Bsp. Bericht des Bundesrechnungshofs über Computersysteme der Bundesbehörden (2004): Fund einer Vielzahl von unerlaubt installierten Computerprogrammen
 - Wer kontrolliert die Implementierung von Softwarekopien?
 - Risiken:
 - zivilrechtliche Haftung der Geschäftsleitung als Störer
 - Strafbarkeit vorsätzlicher Verstöße gegen das Urheberrechtsgesetz (§ 106 UrhG)

Haftungsfallen -8-

- E-Mail-Werbung
 - E-Mail-Werbung ist grundsätzlich unzulässig (§ 7 UWG)
 - Wer kontrolliert den Einsatz von E-Mail-Werbung?
 - Haftungsrisiko der Geschäftsleitung als Störer bei illegaler E-Mail-Werbung

Haftungsfallen -9-

- Pflichtangaben, z.B. bei E-Mails
 - § 37a HGB
 - § 80 Abs. 1 Satz 1 AktG
 - § 35a Abs. 1 Satz 1 GmbHG

- Zwangsgeld

- Abmahnrisiko

Reduzierung von Haftungsrisiken -1-

- Organisation
 - Ressortaufteilung: IT Vorstand; Datenschutzbeauftragter; Lizenzmanagement; Datensicherungskonzept

- Richtlinien/Dokumentation
 - z.B. IT Sicherheit, E-Mail-Nutzung

- technische Maßnahmen
 - Firewalls, Antivirusprogramme; Verschlüsselung von E-Mails; Verhinderung individueller Software-Kopien

- vertragliche Regelungen mit Dritten
- regelmäßige Audits
- externe Berater

Reduzierung von Haftungsrisiken -2-

- Zusammenstellung & Klassifizierung der individuell relevanten Anforderungen
 - Vorschriften der Gesetzgeber oder anderer Regulierungsinstitutionen (national: z.B. HGB, AktG, BDSG, EGG, international: z.B. SOX, Basel II)
 - nationale / internationale IT-Sicherheitsstandards (national: z.B. IT-GSHB, international: z.B. ISO/IEC 17799:2005, CobiT, ISF)
 - unternehmenseigene IT-Sicherheitsvorgaben (z.B. Richtlinien, Sicherheitspolitik)

Praxiserprobte Vorgehensweise

- ✓ Bestimmen Sie ihren Schutzbedarf
 - Anforderungsdefinition

- ✓ Stellen Sie fest wo Sie stehen
 - Ist-Analyse

- ✓ Erarbeitung Soll

- ✓ Umsetzung

- ✓ Etablierung eines Sicherheitsprozesses

Vorgehensweise

- ✓ Bestimmen Sie ihren Schutzbedarf
 1. Welche Daten sind für Ihr Unternehmen wie wichtig?
 2. Welche Prozesse sind wie wichtig?
 3. Welche gesetzlichen Mindestauflagen müssen Sie erfüllen?

Vorgehensweise

- ✓ Stellen Sie dann fest, wo Sie überhaupt stehen
 - Status organisatorische Sicherheit
 - Policycheck
 - Awareness
 - SocialEngineering etc.
 - Status physische Sicherheit
 - Gebäudsicherheit
 - RZ Sicherheit
 - Status IT Sicherheit
 - Pentesting
 - Netzwerksicherheit
 - Infrastrukturcheck

Vorgehensweise

- ✓ Lücken schließen
- ✓ Etablierung eines Sicherheitsprozesses
 - Sicherheitsbewusstsein in der Belegschaft als PE Prozess etablieren
 - regelmäßige technische Überprüfungen
 - regelmäßiger Policycheck
 - Sicherheitsbeauftragten bestimmen
 - usw.
- ✓ Vor allem aber:
 - **Sicherheit ist Chefsache**

Text and a picture page

Vielen Dank!

Fragen bitte!

