

***“Wie sicher sind Ihre Geheimnisse? Rechtsfolgen  
nachlässiger Datensicherheit im Unternehmen“***

Rechtsanwältin Dr. Bettina Kähler  
PrivCom Datenschutz GmbH, Hamburg

b+m Informatik GmbH Kiel – Knürr AG  
3. Juli 2008

# Kennen Sie das ... ?

---

- Gekündigter externer Netzwerkadmin verfügt auch nach 6 Monaten noch über root Passwörter
- Server mit Kundendaten wird mangels ordentlicher Programmierung von der Pornomafia übernommen
- Krankenhaus verfügt über eine Firewall, dessen Lizenz seit 2 Jahren abgelaufen ist

und dies ... ?

---

- Eine Werbeagentur hat ihre Datensicherung so organisiert, dass bei einem Totalausfall der Systeme das Wiedereinspielen der Sicherung 3 Tage beanspruchen würde
- Ein Anwalt entsorgt seine Akten im Altpapiercontainer. Schuld sei die Ehefrau und der 11jährige behinderte Sohn

# Verstöße ...

---

- Gegen gleich mehrere Gesetze
- Bundesdatenschutzgesetz: unbefugte Übermittlung von personenbezogenen Daten, Verstoß gegen die Verpflichtung technisch-organisatorische Maßnahmen zu gewährleisten

## Verstöße (2)

---

- GmbH Gesetz: Geschäftsführer-Pflicht, in den „Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden“
- Vergleichbar Aktiengesetz: Vorstandsmitglieder müssen bei der Geschäftsführung die „Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anwenden“

## Nicht „nur“ Gesetzesverstöße ...

---

- Unternehmensverluste durch Ausfall der Systeme/Datenverlust
- Verlust von Entwicklungswissen (Werksspionage)
- Imageschaden
- Verteuerung der Unternehmenskredite
- Verlust/Verteuerung von Versicherungsschutz
- Bußgelder (BDSG, UWG)

# Dahinter verbirgt sich ...

---

- Datenschutz
- Datensicherheit

# Datenschutz?

---

- Engl. „privacy“
- Privatheit, Privatsphäre, Intimssphäre
- „Das Recht in Ruhe gelassen zu werden“
- Nicht: der Schutz abstrakter Daten
- Personenbezug

Haben Sie Geheimnisse?

Werden Sie mir die verraten?

„Wir haben doch nichts zu verbergen!“

„Wen sollte das interessieren ...“

# Datensicherheit?

---

- Nicht nur Daten mit Personenbezug
- Unternehmens- Geschäftsgeheimnisse
- Forschungsergebnisse
- Produktpläne
- ... alle Informationen die den Wert eines Unternehmens ausmachen

- Mangelhafte Standards bei der Datensicherheit können Verstöße gegen Datenschutz nach sich ziehen
- § 9 BDSG: Technisch-organisatorische Maßnahmen
- Daher empfehlenswert, das eine zusammen mit dem anderen zu planen

- Nicht nur für Geheimnisse
- Auch für die (vermeintlich) banalen Informationen über uns
- ca. 95% aller Information ist öffentlich verfügbar
- **Der Wert von Daten ergibt sich erst aus dem Zusammenhang!**

## Hinzu kommt ...

---

- Spionage ist einfach
  - Passende Instrumente im Internet verfügbar
- Spionage findet statt
  - Wettbewerber / Konkurrenz
  - Geheimdienste
  - eifersüchtige Ehemänner ...

## Was folgt daraus?

---

- Gehen Sie sorgfältig mit allen Angaben um – und seien sie noch so banal
- Organisieren Sie Fort Knox für die restlichen 5 %

## ALT

- „Volkszählungsurteil“ - Recht auf informationelle Selbstbestimmung (1983)
- Jeder soll das Recht haben, selber zu bestimmen, welche Informationen er über sich preis gibt
- Ausnahmen: Anordnung durch Gesetz
- Art. 1 und Art. 2 Grundgesetz

## NEU

- „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ (27. Februar 2008)
- „Online Durchsuchung“
  - Richterliche Anordnung
  - Gesetz muss Vorkehrungen zum Schutz des „Kernbereichs privater Lebensgestaltung“ enthalten

# Datenschutz?

---

- „ist nur lästig, hält auf und blockiert reibungslose Abläufe“
- „keiner hält sich daran, warum sollten wir uns die Mühe machen“
- Datenschutzbeauftragte? „Verursachen nur Kosten und Umstände“

- Abgesehen von Haftungsrisiken bei Nichteinhaltung der gesetzlichen Vorschriften:
- Ein gutes Niveau von Datenschutz- und Datensicherheit wird zunehmend zu einem Wettbewerbsvorteil
- Vertrauensschutz für Ihre Kunden
  - „We keep your secrets“

# Pflichten (BDSG)

---

- Automatisierte Datenverarbeitung ist nur legal, wenn ein Gesetz sie erlaubt
- oder der Betroffenen eingewilligt hat
- Insbesondere: keine „unbefugte Verarbeitung personenbezogener Daten“
- Einhaltung von technisch-organisatorischen Maßnahmen um Verstöße gegen Datenschutzvorschriften möglichst auszuschließen

# Was heißt das praktisch?

---

- Personaldaten in den USA verarbeiten
  - Einwilligung der Mitarbeiter
- E-Mails Ihrer Mitarbeiter lesen
  - Dienst-/Betriebsvereinbarung zu E-Mail Nutzung im Unternehmen
- Krankenhaus: Patientendaten an Forschungseinrichtung
  - Einwilligung

## Pflichten (GmbHG, AktG)

---

- “Sicherstellen einer bedarfs- und rechtskonformen IT-Nutzung”
- Einführen eines IT-Sicherheitskonzepts u. dessen Aktualisierung
- Unternehmensweites Risikomanagement
- Ordnungsgemäße Abbildung der wirtschaftlichen Verhältnisse des Unternehmens in der Buchführung

## Pflichten (sonstige Gesetze)

---

- Sicherung von Vertraulichkeit und Geheimhaltung (vertragliche Pflichten i.V.m. BGB)
- Professionelle Beschaffung von IT-Systemen u. Durchführung von IT-Projekten (BGB, HGB)
- Datenschutzkonformität sicherstellen (BDSG i.V.m. UWG)
- Bei an US-Börsen notierten Unternehmen: Umfangreiche Pflichten nach Sarbanes-Oxley Act

# Wer wird gehängt ...

---

- ... wenn es schief läuft?
- „Es kommt darauf an ...“

# Verantwortlichkeiten

---

- Vorstand, Geschäftsführung
- Aufsichtsrat
- IT-Leiter
- Datenschutzbeauftragter
- Mitarbeiter

## Vorstand, GF

---

- „Sicherstellung einer bedarfs- und rechtskonformen IT-Nutzung“
  - Beschaffung, Einsatz einer funktionierenden Firewall
  - Back-Up Konzept und Durchführung desselben
  - E-Mail Archivierung
  - ....
- Bei Verstoß (persönlich!) haftbar
  - Schadenersatzansprüche Kunden, Dienstleister

- „Rechtmäßigkeit der DV insgesamt“
- Bestellung eines bDSB
- Einführung eines Datenschutz- und Datensicherheitskonzepts
- Beschaffung von IT-Systemen u. Durchführung von IT-Projekten
- Sicherung von Vertraulichkeit/Geheimhaltung

- Kontrolle, ob Vorstand/GF alle erforderlichen Maßnahmen im Rahmen Risikomanagement getroffen hat
- Wenn unzureichende Kontrolle und Eintritt von Schäden: persönliche Haftung
- Nur bei mangelnder Kontrolle

- Erstellen eines Datenschutz- und Datensicherheitskonzepts
- Aktualisierung
- Regelungen beim Zugang von Externen zu DV-Systemen schaffen
- Beschaffung von IT-Systemen u. Durchführung von IT-Projekten
- bDSB: Rechtmäßigkeit der DV

- Nach den Grundsätzen der Arbeitnehmerhaftung
- Haftung im Innenverhältnis ggü. Arbeitgeber
  - „Normale“ Fahrlässigkeit
  - „grobe“ Fahrlässigkeit
  - Vorsatz

# Kontakt

Rechtsanwältin Dr. Bettina Kähler  
PrivCom Datenschutz GmbH  
Behringstr. 28 a | 22765 Hamburg  
T. 040.48.40.90.10 | E. [bettina.kaehler@privcom.de](mailto:bettina.kaehler@privcom.de)  
[www.privcom.de](http://www.privcom.de)