

# IT Security und Juristerei

RAin Michaela Witzel, LL.M.

SOFTWARERING eG

02.10.2007

## Gibt es ein IT-Sicherheitsrecht?

- Ein Recht der IT-Sicherheit im eigentlichen Sinne gibt es (noch) nicht. Die dazu gehörigen Regelungen muss man sich mühsam aus unterschiedlichen gesetzlichen Bestimmungen zusammen suchen.
- Der konkrete Umfang möglicher Rechtspflichten und die mit mangelnder Umsetzung verbundenen Haftungsrisiken sind bislang nicht abschließend geklärt.
- Was versteht „das Gesetz“ unter IT-Sicherheit?
  - Das Gesetz über das Bundesamt für die Sicherheit in der Informationstechnik (BSIG) enthält folgende Definition:

*„Sicherheit in der Informationstechnik im Sinne des Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen, -in informationstechnischen Systemen oder Komponenten;  
-bei der Anwendung von informationstechnischen Systemen oder Komponenten.“*

## Zielsetzung eines IT-Sicherheitsrechts

- Bestimmung, Vermeidung und Begrenzung von Konfliktfällen;
- Bildung einer rechtliche Grundlage für den Aufbau einer sicheren und störungsfreien IT-Infrastruktur innerhalb es Unternehmens;
- IT-Sicherheitsrecht dient zum einem dem Schutz des Unternehmens (insbesondere unternehmenseigene Daten), aber auch dem Schutz externer, von Dritter überlassener Daten;

# IT-Sicherheit als Teil der so genannten IT-Compliance

- Unter dem Oberbegriff „Compliance“ wird generell die **Befolgung von rechtlichen Pflichten und Geboten** durch Unternehmen und die entsprechende Verantwortlichkeit der Unternehmensleitung diskutiert.
- **IT-Compliance** im engeren Sinne: Anforderungen und Vorgaben, die direkt auf die IT abzielen und diese unmittelbar zum Gegenstand haben.
- **IT-Compliance** im weiteren Sinne: Anforderungen und Vorgaben, die weder unmittelbar und direkt auf die IT abzielen, sondern faktisch durch die IT umgesetzt werden.

## Eine Entscheidung des OLG Hamm: Einem Reisebüro wurde der Anspruch auf Schadensersatz verweigert, weil es bei der Datensicherung im eigenen Unternehmen nur unzureichende Sicherungsmaßnahmen getroffen hatte:

- o Das Reisebüro hatten einen PC-Reparaturdienst beauftragt, nach dem Grund für eine Fehlermeldung zu suchen. Bei diesen Arbeiten war der Server abgestürzt, zahlreiche Geschäftsdaten wurden gelöscht. Da das Reisebüro seine Daten noch nicht einmal monatlich gesichert hatte, waren Teile der Daten unwiederbringlich gelöscht.
- o Das Reisebüro verlangte Schadensersatz in Höhe von 14.000,00 € von dem beauftragten PC-Reparaturdienst.
- o Das Gericht hatte zu entscheiden, in wessen Verantwortungsbereich eine unterlassene Datensicherung fällt. Nach Ansicht des Gerichts trifft den IT-Verantwortlichen des Reisebüros „ein überdeckendes Mitverschulden“. Demnach hätte die Sicherung der Daten täglich erfolgen müssen, die Vollsicherung mindestens einmal wöchentlich. Das Verhalten des IT-Verantwortlichen bezeichnete das Gericht als „blauäugig“ und lehnte deshalb Schadensersatzansprüche gegen den Reparaturdienst ab.

## Grundwerte der IT - Sicherheit

- **Vertraulichkeit:** Sensible oder geheime Informationen werden vor unwissentlicher Preisgabe oder unbefugter Kenntnisnahme geschützt.
- **Verfügbarkeit:** Dem Benutzer stehen Dienstleistungen, Funktionalitäten oder auch einzelne Informationen zum richtigen Zeitpunkt zur Verfügung.
- **Integrität:** Alle Daten bleiben während und vor allem nach ihrer Verarbeitung vollständig und unverändert.

Untrennbar mit diesen Werten verknüpft sind die Begriffe **Authentisierung** (Identifikation) und **Autorisierung** (Feststellung ihrer Zugriffsrechte) der Nutzer, die sich nicht nur gegenseitig bedingen, sondern ohne die darüber hinaus weder Vertraulichkeit noch Integrität elektronischer Daten gewährleistet werden kann.

## Haftungsrisiken und Sanktionen

- Vertragliche Schadensersatzhaftung
- Wettbewerbsrecht
- IT Sicherheit als Obliegenheit: Verlust von Versicherungsschutz
- Nichtberücksichtigung bei der Vergabe öffentlicher Aufträge
- Datenschutzrechtliche Haftung

# Das KonTRaG und die persönliche Haftung von Vorständen und Geschäftsführern

- **KonTRaG:** Gesetz zur Kontrolle und Transparenz im Unternehmensbereich;
- Das KonTRaG ist kein eigenständiges Gesetz, sondern ein so genanntes Artikelgesetz, das Ergänzungen und Änderungen in anderen Wirtschaftsgesetzen, z.B. dem Aktiengesetz, dem Handelsgesetzbuch oder dem GmbH-Gesetz bewirkt.
- Ziel des KonTRaG ist es, eine wirtschaftliche Kontrolle und Transparenz der AG und der GmbH zu erreichen.
- Im Hinblick auf die IT-Sicherheit gilt dabei speziell eine Vorschrift als Kernelement, welche die Unternehmensleitungen dazu zwingt, ein unternehmensweites Früherkennungssystem für Risiken (Risikomanagementsystem) einzuführen und zu betreiben.

## Haftung des Vorstandes einer AG (§ 91 Abs. 2 AktG)

Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Informationen zum Wohle der Gesellschaft zu handeln.

Die Haftung hört nicht beim Vorstand auf: wenn der Aufsichtsrat nicht den Vorstand entsprechend überwacht, kann dies sogar zu einer Haftung seitens des Aufsichtsrat bzw. dessen Mitglieder führen (§ 116 AktG).

## Konsequenzen aus KonTraG: Risikofrüherkennung

- Vorstand einer AG und Geschäftsführung einer GmbH werden verpflichtet, **geeignete Maßnahmen zur frühzeitigen Erkennung** von Entwicklungen zu treffen, die den Fortbestand der Gesellschaft konkret gefährden.
- Die Geschäftsleitung wird demzufolge verpflichtet, ein **unternehmensweites Risikomanagement** zu installieren, welches alle Bedrohungen erfasst, die durch IT Systeme und deren Einsatz im Unternehmen entstehen können.
- Es geht also nicht nur um die Einrichtung angemessener Überwachungsmechanismen, sondern auch um **Informations- und Vorsorgemaßnahmen**.

## Stufen eines Risikomanagementsystem

- **Stufe 1:** Zunächst müssen im Rahmen einer Risikoanalyse alle Risiken in Zusammenhang mit dem Einsatz von unternehmenseigener IT-Systemen ermittelt und analysiert werden, um dadurch in die Lage versetzt zu werden, das Gesamtrisiko für das Unternehmen einschätzen zu können.
- **Stufe 2:** Anschließend gilt es ein Sicherheitskonzept zu erstellen, um das ermittelte Risiko basierend auf einer wirksamen Risikoprävention zu reduzieren. Das Sicherheitskonzept sollte zum Ziel haben, die Grundwerte der IT-Sicherheit (Verfügbarkeit, Vertraulichkeit, Unversehrtheit) sicherzustellen.
- **Stufe 3:** Das Sicherheitskonzept ist in der Praxis umzusetzen und vor allem einzuhalten.

# Datenschutzrecht

## Datenschutz

- bezieht sich ausschließlich auf den Schutz **personenbezogener Daten**;
- etabliert das Grundrecht auf informationelle Selbstbestimmung (so genanntes Volkszählungsurteil des Bundesverfassungsgerichts);
- schützt die Privatsphäre: Vertraulichkeit und Anonymität muss gewahrt werden.
- **§ 9 BDSG**: „Öffentliche und nicht-öffentliche Stellen, die (...) personenbezogene Daten erheben, verarbeiten oder nutzen, **haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind**, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

## Vorgaben der Anlage zu § 9 BDSG

1. **Zutrittskontrolle** (z.B. Einrichtung von Sicherheitsbereichen, Vergabe von Berechtigungsausweisen an Mitarbeiter und Besucherausweise; Verschlussene Aufbewahrung von Datenträgern);
2. **Zugangskontrolle** (Verwendung von sicheren Passwort-Verfahren und Benutzererkennungen, Verschlüsselung von Daten)
3. **Zugriffskontrolle** (Zugriffskontrolle auf Programme und Daten durch Benutzerkennungen und Passwörter)
4. **Weitergabekontrolle** (Protokollierung von Datenübertragung, Zentrale Ausgabe und Verwaltung von Datenträgern, Verbot der Verwendung privater Datenträger im Dienst und der Mitnahme dienstlicher Datenträger nach Hause)
5. **Eingabekontrolle** (Festlegung von Zuständigkeiten, Protokollierung)
6. **Auftragskontrolle** (Protokollierung von Kunden-Weisungen)
7. **Verfügbarkeitskontrolle** (Notfallplanung, Auslagerung von Sicherheitskopien)
8. **Datentrennungskontrolle** (Software-technische Mandanten-/Kundentrennung)

# Vertragliche (Rechts-) Pflichten zur Umsetzung von IT-Sicherheitsmaßnahmen

- **Vertraulichkeitsvereinbarungen**

Sind Daten und elektronische Informationen jedermann im Unternehmen frei zugänglich und nicht gegen Einsichtnahme abgesichert, kann die Vertraulichkeit und damit die Einhaltung geschlossener Vereinbarungen nicht gewährleistet werden.

- **Softwarehinterlegungsvereinbarungen**

Gegenstand einer Escrow-Vereinbarung ist unter anderem, den Zugriff auf die hinterlegte Software unbedingt zu verhindern.

- **IT-Outsourcing-Vereinbarungen**

Um sicherzustellen, dass Kundendaten ausschließlich diesem zugänglich sind, ist außer einem hohen Maß an Verfügbarkeit auch die Vertraulichkeit der Daten von erheblicher Relevanz.

# Anerkannte Standards, Best Practices, ISO- und DIN-Normen

- DIN-Normen
- IT-Grundschutzhandbuch des BSI  
(bietet ein Kochrezept für ein mittleres Schutzniveau; durch die Verwendung des Grundschutzhandbuchs entfällt eine aufwändige Sicherheitsanalyse, die Expertenwissen erfordert)
- Common Criteria for Information Technology Security Evaluation  
(Common Criteria oder CC sind ein internationaler Standard über die Kriterien der Bewertung und Zertifizierung der Sicherheit von Computersystemen im Hinblick auf Datensicherheit und Datenschutz);
- ITIL

## **Sarbanes Oxley Act (SOX)**

- US-Gesetz zur Verbesserung der Unternehmensberichterstattung. Ziel des Gesetzes ist es, die Anleger zu schützen und ihr Vertrauen in die Rechnungslegung von Unternehmen wieder herzustellen.
- Das Gesetz betrifft wesentliche Aspekte der Corporate Governance, der Compliance sowie der Berichterstattungspflicht von an der US Börse notierten Aktiengesellschaften.
- SOX steht vor allem für die Notwendigkeit, betriebliche Daten verfügbar zu machen bzw. verfügbar zu halten.
- Alle Unternehmensprozesse müssen detailliert beschrieben und protokolliert werden, in denen Zahlen für die Finanzberichterstattung entstehen.

**Vielen Dank für Ihre Aufmerksamkeit!**