



# WENDLER TREMML

## RECHTSANWÄLTE

Berlin · Düsseldorf · München · Brüssel · Warschau

best OpenSystems Day  
Herbst 2005



**Rechtsanwalt Dr. Michael Karger, München**

# **Unternehmerisches Handeln unter Sicherheitsanforderungen in der IT (KonTraG, SOX & Basel II)**

## Agenda:

1. Überblick: Rechtliche Anforderungen bzgl. IT-Sicherheit
2. KonTraG
3. SOX
4. Basel II
5. Outsourcing als „Way out“?
6. Zusammenfassung

# Rechtliche Anforderungen an die IT im Unternehmen

- IT ist das Rückgrat aller Unternehmensprozesse
- Focus der Diskussion oft nur auf Prozesse gerichtet
- Relevanz der IT oft unterschätzt
- Kein einheitliches Gesetz, das die rechtlichen Anforderungen an die Unternehmens-IT formuliert

# Rechtliche Anforderungen an die IT im Unternehmen

- Dschungel der rechtlichen Vorgaben
- Forderung nach Kontrolle und Transparenz
  - Corporate Governance
  - KonTraG
  - Basel II
  - Sarbanes Oxley Act
- Forderung nach IT-Sicherheit

## IT-Sicherheit in der Rechtsordnung

### **Einige Gesetze erwähnen IT-Sicherheit unmittelbar:**

- BDSG, TKG: Datenschutzregelungen, Post- und Fernmeldegeheimnis
- StGB: §§ 202a, 206, 263a, 268, 269, 274, 283b, 303a, 303b
- UrhG: Regelungen zum Urheberrechtsschutz

### **weitere Gesetze fordern implizit IT-Sicherheit:**

- BGB: Vertrags- und Deliktsrecht, z.B. gem. §§ 823 ff. BGB
- UWG: Lauterkeit des Wettbewerbs, Einhaltung von Gesetzen
- Strafgesetzbuch: allgemeine Strafgesetze
- KonTraG, AktG, GmbHG, SOX: Riskmanagement im Unternehmen

**Einen Überblick gibt die BITKOM-Matrix der Haftungsrisiken**

# Was ist IT-Sicherheit aus rechtlicher Sicht?

## Definition in § 2 Abs. 2 BSI-Gesetz:

Sicherheit in der Informationstechnik ... bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die **Verfügbarkeit, Unversehrtheit** oder **Vertraulichkeit** von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen oder Komponenten oder
2. bei der Anwendung von informationstechnischen Systemen oder Komponenten.

## Die klassischen Schutzziele der IT-Sicherheit

### **Verfügbarkeit**

Schutz vor unbefugter Vorenthaltung von Informationen oder Betriebsmitteln / des Zugangs zu Daten

### **Unversehrtheit**

Schutz vor unbefugter Veränderung von Informationen/ Manipulation

### **Vertraulichkeit**

Schutz vor unbefugter Preisgabe von Informationen/ vor unbefugter Kenntnisnahme

## KonTraG: Begriff und Anwendungsbereich

- **KonTraG** = Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
- Deutsches Gesetz
- Gilt für deutsche Aktiengesellschaften
- Gilt mittelbar auch für GmbH's

## KonTraG: Gesetzliche Regelungen

### Aktiengesellschaft:

Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. (§ 91 Absatz 2 AktG)

### GmbH:

Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden. (§ 43 Absatz 1 GmbHG)

## Was verlangt das KonTraG praktisch?

- Einrichtung und Aufrechterhaltung eines effektiven Risikomanagements mit
  - systematischer Früherkennung
  - effektiver Prävention
  - effizienter Risikobewältigung
  - ständiger Kontrolle

# KonTraG und IT-Sicherheit

## Bündel von Maßnahmen

- Security Policy, IT-Sicherheitskonzept, Datenschutzkonzept, u.a.
  - Datensicherung
  - Schutz vor Viren
  - Schutz vor Angriffen (von Außen und Innen) z.B. Firewalls
  - Schutz davor, selbst Angreifer zu sein
  - Berechtigungssysteme
  - Richtlinien für Umgang mit eMail und WWW
- Notfall-, Ausfall- bzw. Rettungskonzepte
- regelmäßige Ausbildung der Mitarbeiter

## KonTraG: Rechtsfolgen bei Verstoß

- Persönliche Haftung von Vorständen und Aufsichtsräten, bzw. Geschäftsführern

## KonTraG: Rechtsfolgen bei Verstoß

- Persönliche Haftung von Vorständen und Aufsichtsräten, bzw. Geschäftsführern:
- Aktiengesellschaft:  
Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens (...) verpflichtet. (§ 93 II AktG) Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, **so trifft sie die Beweislast.**  
Aufsichtsrat haftet bei mangelnder Kontrolle nach §§ 111, 116 AktG
- GmbH:  
Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft solidarisch für den entstandenen Schaden. (§ 43 II GmbHG)

## Haftung des Managements unterhalb des Vorstandes bzw. der Geschäftsführung

- keine Haftung nach Vorschriften des KonTraG
- aber trotzdem persönliche Haftung ...
  - aus Arbeitsvertrag,
  - aus Deliktsrecht des BGB,
  - aus Strafgesetzen,
  - aus weiteren Spezialgesetzen wie UrhG, BDSG
- Haftung eingeschränkt durch Rechtsprechung zu Grundsätzen der Arbeitnehmerhaftung
- Risiko von Abmahnung und Kündigung

## Sarbanes Oxley Act

- Auch „SOX“ oder „SOA“
- US-amerikanisches Gesetz
- In Kraft seit Juli 2002
- Reaktion auf ENRON, etc.
- Adressaten: An US-Börsen notierte Unternehmen
- Ziele u.a. Verbesserung
  - der internen Kontrollen und Dokumentationen
  - der Transparenz der Unternehmensprozesse
  - der Information der Adressaten des Financial Reporting
- Sanktionen: Gravierend, u.a. Haftstrafen für Unternehmensleitung (bis zu 20 Jahren)

## SOX in Deutschland ?

- US-Gesetz für US-Unternehmen
- Relevanz für Deutschland ? Ja, u.a. für
  - Deutsche Unternehmen mit US-Börsenzulassung
  - Deutsche Tochterunternehmen einer US-Gesellschaft
  - „Ausstrahlung“ SOX auf Interpretation der deutschen Gesetze, z.B. auf das KonTraG und „Corporate Governance“

## SOX und IT: Regelungen

- Es gibt keine IT-spezifischen SOX-Regelungen
- SOX regelt das Financial Reporting
- Aber: Mittelbar ist durch SOX stets auch IT angesprochen
- Grund: IT unterstützt bzw. ermöglicht technisch die erforderlichen Prozesse und muss deshalb verlässlich und sicher sein

## SOX und IT: Regelungen

- Mehrere SOX-Paragrafen (Sections) mit IT-Relevanz: Sec. 302, Sec. 404, Sec. 409, Sec. 802
- Sec. 404 fordert ein internes Kontrollsystem, die Unternehmensleitung muss regelmäßig einen Internal Control Report vorlegen
- Im Kern geht es darum, sicherzustellen und nachzuweisen, dass alle relevanten Finanzdaten vollständig und richtig sowie die zugrundeliegenden (IT-)Prozesse ordnungsgemäß sind

## SOX und Document Retention

- Sec. 802: Elektronische Dokumente mit Bezug auf Unternehmens-Assets oder -Performance
- 5 Jahre Aufbewahrung (ab Ende betreffender Veranlagungsperiode, in der Audit stattfand)
- Dokumente müssen 5 Jahre technisch verfügbar sein
  - (P) Systemwechsel !
- Dokumente dürfen nicht verändert werden !
- Bei Verstößen: Geld- und Freiheitsstrafe

## SOX und Document Retention

SOX-Report muss Aussagen enthalten u.a. zu Policy und Standards für

- Dokumenten- Aufbewahrung, Schutz und Vernichtung
- Online Storage
- Audit Trails
- Integration in Unternehmensdatenbanken
- Eingesetzte Technologie
- Sox-Software
- Records Management Program

## SOX und IT: IT Controls

- SOX erfordert „IT-Controls“
- Spezifische Informationssysteme zur Unterstützung und Überwachung von Geschäftsprozessen
- Umfassen idR die Kontrolle der IT-Umgebung, des Rechnerbetriebs, des Zugangs zu Programmen und Daten, der Programmentwicklung und von Changes.

## SOX und IT: IT Controls

Gegenstand von allgemeinen IT-Controls insbes.:

- Change Management Verfahren
- Kontrollverfahren für Source Code- und Dokumenten-Versionierung
- Standards für den Lifecycle bei Softwareentwicklung
- Security Standards und -Verfahren
- Incident-Management Policies und Verfahren
- Technical-Support Policies und Verfahren
- Policies für Hard- und Software-Konfiguration, Installation, Testen, etc.
- Verfahren für Disaster Recovery bzw. Backup-Restore

## SOX-Compliance

- Kann idR nicht isoliert durch IT-Department geleistet werden
- Querschnitts-Projekt unter Beteiligung
  - CEO, CFO, CIO
  - Rechnungswesen, Rechtsabteilung
  - Risikomanagement, Controlling, Interne Revision
  - Investor Relations
  - Corporate Governance Bereich
- Implementierungsaufwand ist hoch

## Basel II

- Basel II = Baseler Eigenkapitalvereinbarung
- Am 26.06.2004 vom Baseler Ausschuss für Bankenaufsicht verabschiedet
- Umsetzung in deutsches Recht wohl erst 2006
- Adressaten: Banken
- Ziel: Kapitalanforderungen an Banken werden von den Risiken abhängig gemacht
- Risikomanagement gefordert
- Banken unterziehen ihre Kunden einem Rating

## Basel II und Informationstechnologie

- Für Banken: Erweiterung der Anforderungen; bestehende Regelungen § 25 KWG, § 33 WPHG0
- Für Bankkunden:
  - Rating maßgeblich für Kreditkonditionen
  - Faktor für Rating auch: Riskmanagement
  - Damit auch: Riskmanagement in der IT

## Basel II und Informationstechnologie

- Anhaltspunkte im Arbeitspapier „MaRisk“
- „Mindestanforderungen für das Risikomanagement“  
(Bundesbank und BaFin)
- 2. Entwurf, September 2005

## Basel II und „MaRisk“

- Anforderungen u.a.:
  - IT-Systeme und Prozesse müssen sicherstellen
    - Integrität
    - Verfügbarkeit
    - Authentizität
    - Vertraulichkeit
    - Übliche Standards, fortlaufende Kontrolle
  - Testen und Abnahme von IT-Systemen
  - Trennung von Test- und Produktivumgebung
  - Notfallkonzept und Wiederanlaufpläne

## Outsourcing als „Way Out“ ?

- Antwort: NEIN !
- Verantwortung bleibt beim Auftraggeber
- Kann nicht auf Auftragnehmer übertragen werden
- AG muß sich ggü AN vertraglich meist noch besser als bisher absichern, z.B:
  - AN muß in das Kontrollsystem integriert werden
  - Auditrechte des AG
  - Höhere Anforderungen an das Reporting
  - Höhere Anforderungen an die Dokumentation
  - Adäquate Service Level und Notfallszenarien
  - Leistungsänderungsverfahren

## Zusammenfassung

1. Vielzahl rechtlicher Anforderungen
2. KonTraG, SOX, Basel II u.a.: Überschneidungen
3. Einheitliche Merkmale:
  - Risikomanagement
  - Transparenz
  - Realisierung
  - Dokumentation
  - Kontrolle
4. Compliance vom IT-Department alleine nicht zu realisieren
5. Es spielen zusammen u.a.:
  - Technik, Fachabteilungen, Rechnungswesen, Revision, Recht, WPs

## Ihr Ansprechpartner:



**Dr. Michael Karger**

**Wendler Tremml Rechtsanwälte**  
Martiusstraße 5/II  
80802 München

fon + 49 89 388 99 130  
mkarger@law-wt.de

fax +49 89 388 99 155  
www.law-wt.de