Risikoverantwortung und Haftung

IT-Betrieb zwischen Compliance und Effizienz

38. COURSE Tagung am 18. Mai 2009

Rechtsanwalt
Ernst Dieter Naber
Fachanwalt für Informationstechnologierecht

Risikomanagement

Rechtliche Grundlagen

- KonTraG => § 91 Abs. 2 AktG
  - Geeignete Maßnahmen zur Früherkennung von Entwicklungen, die den Fortbestand des Unternehmens gefährden
  - Insbesondere: Einrichtung eines Überwachungssystems
  - Lagebericht (Bilanzrechtsreformgesetz 2004)
    - Nichtfinanzielle Leistungsindikatoren
      - » bei großen Kapitalgesellschaften, § 289 Abs. 3 HGB
      - » im Konzernabschluss, § 315 HGB
- Ausstrahlungswirkung => § 43 GmbHG, § 34 GenG
  - "Sorgfalt eines ordentlichen Geschäftsmannes"
- Adressat: Geschäftsleitung
  - Horizontale und vertikale Kontrolle
- Sanktion: Persönliche Haftung

Exkurs: Arbeitsrechtliche Haftung

- **Voraussetzungen**
  - Pflichtverletzung
  - Schaden
  - Verschulden (Vorsatz oder Fahrlässigkeit)
- **Folge => Schadensersatz**

aber

- **Arbeitsrechtlicher Verschuldensbegriff:**
  - Vorsatz, grobe Fahrlässigkeit => Gesamtschaden (in der Regel)
    - Rote Ampel, Alkohol, Auflösung eines Raid trotz Warnung
  - Leichteste Fahrlässigkeit => keine Haftung
    - Extreme Überforderung
  - Mittlere, normale Fahrlässigkeit => Aufteilung des Schadens

Risikomanagement

- **Marktmechanismen**
  - Basel II
    - Eigenkapitalvorschriften für Banken
    - Formalisierte Risikobewertung mittels Rating
      - Vorteilhaft: Risikomanagement und Compliance
  - Sarbanes-Oxley-Act, SOX
  - EuroSOX seit 2008
  - Audits durch:
    - Kunden
    - Datenschutzbeauftragter
    - Wirtschaftsprüfer
    - Due Diligence
- **Interne Regelwerke**
  - Deutscher Corporate Governance Kodex von 2002
  - Governance Kodex für Familienunternehmen

Anleitungen

Normen, Empfehlungen, Standards (Stand der Technik)

- BSI Kataloge zum Grundschutz
  - Zertifizierung nach ISO/IEC 27001
- MaRisk des BaFin
  - Mindestanforderungen Risikovorsorge, Basel II
- ISO/IEC 27002
  - Kontrollmechanismen für die Informationssicherheit
  - Zertifizierung
- CobiT
  - Control Objectives for Information and Related Technology
  - Werkzeug für die Steuerung der IT aus Unternehmenssicht
  - Integration der IT-Governance in die Corporate Governance

Anleitungen

- **Normen, Empfehlungen, Standards (Stand der Technik)**
  - ITIL
    - IT Infrastructure Library
    - Prozessbeschreibung
    - Grundlage für ein IT-Service-Management
    - Best-Practice-Ansatz, Zertifizierung
  - Finanzverwaltung
    - GoBS, GDPdU
  - Prüfungsstandards der Wirtschaftsprüfer
    - PS 330 Abschlussprüfung bei Einsatz von Informationstechnologie
    - PS 331 dto. bei teilweiser Auslagerung auf Dienstleister
    - PS 880 Erteilung und Verwendung von SW-Bescheinigungen

Risikomanagement

- **Ganzheitlich**
  - Technisch - z.B. Desaster Recovery
  - Wirtschaftlich - z.B. Versicherung des Restrisikos
  - Rechtlich - z.B. Contract and Claim Management
  - Organisatorisch - z.B. Zugangskontrollen
- **In allen Unternehmensbereichen**
  - Finanzwesen
  - Produktion
  - Informationstechnologie
    - bei der Unterstützung geschäftskritischer Prozesse
    - als geschäftskritischer Prozess

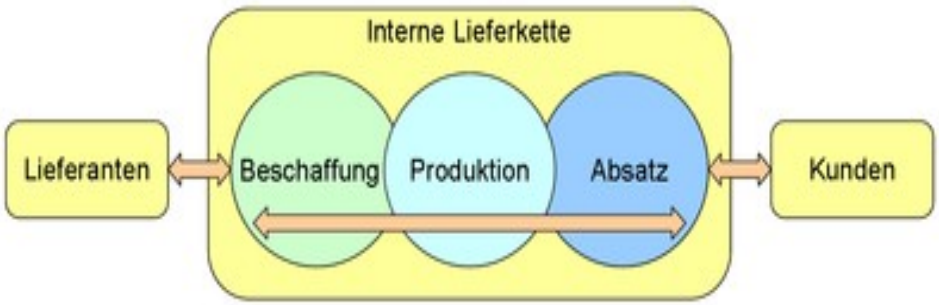
IT-Compliance

Compliance *durch* IT

- Finanzwesen / Handels- und Steuerrecht
  - Steuerliche Erklärungs- und Nachweispflichten
  - arbeits- und sozialversicherungsrechtliche Abrechnungen
- SOX und EuroSOX
  - Finanzdaten, Dokumentation (Ausstrahlungswirkung)
- Produkt-Compliance
  - RoHS, Elektro- und Elektronikgerätegesetz
  - Produkthaftung
  - Automotive ELV
  - Internationales Werkstoffdaten-System (IMDS)
  - Global Automotive Declarable Substance List (GADSL)

Prozess-Compliance

- Beispiel Pharma: GMP, GAMP, GLP, GxP
- Supply Chain (Rückverfolgbarkeit)



Compliance *der* IT

- Allgemeiner Schutz personenbezogener Daten, BDSG
- Spezifische Datenschutznormen
  - Telemediengesetz §§ 11 - 15 TMG
  - Fernmeldegeheimnis § 206 StGB, § 88 TKG (private eMail)
- Arbeitsschutzrecht
  - Bildschirmarbeitsplatz (BildschArbV)
- Betriebsverfassungsrecht
  - Mitwirkungs-/Beteiligungsrechte des Betriebsrats
  - Leistungskontrolle durch Arbeitszeiterfassung
  - Regelung privater Internetnutzung

IT-Compliance

Compliance *der* IT

- Urheberrecht, Strafrecht
  - Installation von SW nur durch autorisierte MA
  - Kontrolle der tatsächlichen Praxis, Richtlinien allein reichen nicht
  - Verantwortung der Geschäftsführung
  - Software Asset and License Management
  - Dual Use Software, § 202 c StGB
- Steuerrecht
  - Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme, GoBS
  - Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen, GDPdU
  - Verrechnungspreisdokumentation
  - geschäftliche Korrespondenz

Compliance *der* IT

- Wettbewerbsrecht, Gewerbl. Schutzrechte
  - Außendarstellung, Webauftritt
  - Impressum, rechtswidrige Inhalte, Haftung für Links
  - Domainnamen - Marken
  - Workflow des Webshop
  - persönliche Haftung des Admin-C
- Schutz durch Strafrecht
  - § 202a StGB Ausspähen von Daten
    - "die gegen unberechtigten Zugang besonders gesichert sind"
  - § 17 UWG Verrat von Geschäftsgeheimnissen
  - § 206 StGB Verletzung des Post- und Fernmeldegeheimnisses
  - § 263 a StGB Computerbetrug
  - § 303 a, b StGB Datenveränderung, Computersabotage

Datensicherheit

Sicherung vor

- Verlust
- Veränderung
- Unauffindbarkeit
- unauthorisiertem Zugriff

Kritisch:

- Mobile Geräte
  - Laptop, Handy, Smartphone, PDA
- DFÜ durch fremde Netze
- Faktor Mensch

IT-Security Studie 2008:

- 50% der deutschen Unternehmen setzen Sicherheitsstandards, wie z.B. BSI Grundschutz, nicht in die Praxis um

Rechtspflichten

- Allgemeine Risikovorsorge
- Anlage zu § 9 Satz 1 BDSG:
  - Schutz "gegen zufällige Zerstörung oder Verlust"
  - Eingabekontrolle (Eingabe, Veränderung, Entfernung)
- TMG: Kommunikation "gegen Kenntnisnahme Dritter geschützt"
- Indirekt
  - §§ 17 UWG, 202a, 206 StGB
  - versicherungsrechtliche Obliegenheiten
  - Mitverschulden, § 254 BGB
- Haftungsrisiken:
  - § 7 BDSG: Schadensersatz
  - § 43 BDSG: Bußgeld 25 -250 T€, § 44 BDSG: < 2 Jahre Gefängnis
  - § 16 TMG: (Bußgeld bis 50 T€)

Datensicherung/Archivierung

- **Sicherung/Archivierung zur**
  - Erfüllung gesetzlicher Anforderungen
    - Handels- und Steuerrecht
    - Produkthaftung, Branchenanforderungen
  - Innerbetrieblichen Zwecken
    - Bewahrung von Know-how
    - Planungszwecke
- **Revisionssichere Archivierung**
  - Kontext, Historie, Authentizität
- **Infrastruktur**
  - Hardware, Software (Lizenzen), Datenformate
- **Unterstützende Methoden/Tools**
  - Dokumentenverw.systeme, Records Management, Information Lifecycle Management (IML), Enterprise Content Managment (ECM)

Archivierung

Warum + Was?	Wie lange?
§ 147 Abs. 1, 3 AO, § 257 HGB:	
Handelsbücher, Abschlüsse und die zum Verständnis erforderlichen Unterlagen	**10 Jahre**
Buchungsbelege	**10 Jahre**
Handelsbriefe/Geschäftsbriefe	**6 Jahre**
für Besteuerung bedeutsam	**6 Jahre**
§ 14 b UStG:	
Rechnungen	**10 Jahre**
Branchenbezogene Fristen:	
RöntgenVO, StrahlenschutzVO	**bis zu 30 Jahre**
Luftfahrzeugbau	

Verletzung von Aufbewahrungspflichten

- Buchführungspflicht, § 283 b StGB
  - Freiheitsstrafe bis 2 Jahre oder Geldstrafe
- Bei Überschuldung oder Zahlungsunfähigkeit, § 283 StGB
  - Freiheitsstrafe bis 5 Jahre oder Geldstrafe
- Besonders schwerer Fall (Gewinnsucht), § 283 a StGB
  - Freiheitsstrafe 6 Monate bis zu 10 Jahre
- Steuerhinterziehung, § 370 AO:
  - Freiheitsstrafe bis 10 Jahre
- Kein Vorsteuerabzug; Steuerschätzung
- Beweismittelverlust
- Non-Compliance

Löschung

- **TMG, TKG Nutzungsdaten:**
  - Nach Nutzung
  - Nach Abrechnung
  - Einzelnachweis max. 6 Monate
  - Sanktion: Bußgeld bis 50T€
    TKG bis 300 T€
- **BDSG, personenbezogene Daten:**
  - Grundsatz der Datenvermeidung/-sparsamkeit
  - Löschungsanspruch
  - Sanktion: Bußgeld 25 - 250 T€,
    Freiheitsstrafe (Bereicherungsabsicht)

Bundesdatenschutzgesetz

- Personenbezogene Daten, § 3 Abs. 1 BDSG:
  - Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person
  - Besondere (zweckgebundene) Daten
- IP-Adresse personenbezogen?
  - absolute vs. relative Bestimmbarkeit
  - Bundesjustizministerium - AG Berlin
  - Bundeskriminalamt - Honeypot
  - Bewegungs-/Nutzerprofile mit Zusatzwissen (Google Analytics))
    - wenn IP nicht personenbezogen ist:
    - § 15 Abs. 3 TMG: pseudonym, Belehrung über Widerspruchsrecht, keine Zusammenführung, für Werbung, Marktforschung,Angebotsgestaltung
    - Grundrecht auf Integrität und Vertraulichkeit von IT-Systemen

Datenschutz

- **Handel mit Kundendaten**
  - Nur mit Einwilligung, § 4 BDSG
  - oder Ausnahmeerlaubnis, § 28 BDSG
  - wenn im Inland zulässig, dann im Ausland:
    - EU-weit und in sichere Drittstaaten
    - bei bestimmten vertraglichen Vereinbarungen
    - oder safe harbour principles (USA)
- **Datengeheimnis, vorherige Verpflichtung, § 5 BDSG**
- **Auftragsdatenverarbeitung, § 11 BDSG**
  - Verantwortliche Stelle - Verarbeitende Stelle
- **Sanktionen: Bußgeld bis 25 T€, bis 250 T€, Freiheitsstrafe bis 2 Jahre**

Fernmeldegeheimnis

- Art. 10 GG, § 88 TKG
  - Inhalt und nähere Umstände
  - Beteiligung
  - erfolglose Verbindungsversuche
- § 206 StGB
  - Mitteilung an Dritte
  - Öffnen oder Kenntnis vom Inhalt verschaffen (körperliche Sendungen)
  - Unterdrücken, wenn zur Sendung anvertraut (auch eMail)
  - Unbefugt: Erlaubnis nur durch Gesetz (vgl. § 88 III TKG)
- Sanktion: Freiheitsstrafe bis zu 5 Jahre / Geldstrafe

Betriebliche Nutzung

- TKG: Arbeitnehmer <> Dritter
- TMD: ausdrücklich ausgenommen § 11 Abs. 1 Nr. 1 TMD
- BDSG: im allgemeinen arbeitsrechtlichen Rahmen

Private Nutzung

- TKG: AG = Dienstleister, AN = Dritter
  - => Fernmeldegeheimnis ist zu beachten § 88 TKG, § 206 StGB
  - => technische Vorkehrungen, angemessene Schutzmaßnahmen, § 109 TKG
  - => Zugriff nur zur Störungsbeseitigung, Verhinderung rechtswidriger Nutzung letzteres aber nur bei bestehendem Anfangsverdacht, § 100 Abs. 3 TKG
- TMG: AG = Diensteanbieter, AN = Nutzer
  - => Datenerfassung nur, soweit erforderlich
  - => Löschung nach Ende der Nutzung
- Gesamte eMail gilt als privat

Handlungsoptionen bei Mischnutzung

- Datenströme logisch und physisch trennen
- Separate Namensräume schaffen
  - Karin.Mustermann.privat@firma.com
- Detaillierte Regelungen über Nutzung
  - durch arbeitsvertragliche Vereinbarung
  - durch Betriebsvereinbarung
- Zustimmung zu bestimmten Handlungen
  - z.B. Spamfilterung, Logging
  - Löschung nach Ende des Arbeitsverhältnisses
  - Hohe Anforderungen an Zustimmung!
    keine Rückwirkung, Schriftform, vorherige Information
- Einhaltung der Regeln überwachen

Form

- **Formmangel => Nichtigkeit, Beweisproblem**

- **Gesetzliche Schriftform**
  - eigenhändige Unterschrift auf Urkunde
  - bei Vertrag auf derselben Urkunde
- **Gesetzliche Textform**
  - Urkunde oder
  - zur dauerhaften Wiedergabe in Schriftzeichen geeignet
    - d.h. Papier, Datei auf Datenträger, eMail, Fax
  - Person des Erklärenden
  - Abschluss der Erklärung
- **Gesetzliche Elektronische Form**
  - ersetzt die gesetzliche Schriftform
  - erfordert qualifizierte elektr. Signatur nach dem SigG

Vereinbarte Form

- **im Zweifel wie gesetzlich, aber Erleichterungen**
- **Schriftform**
  - telekommunikative Übermittlung reicht, wenn nicht ausgeschlossen
    - Telefax, eMail, Telegramm (wie Textform)
    - keine Unterschrift erforderlich
    - aber Erklärender muss erkennbar sein
    - dauerhafte Aufbewahrung bzw. Druck
  - Vertrag durch Schriftwechsel
  - Anspruch auf nachträgliche Beurkundung
- **Elektronische Form**
  - "andere elektronische Signatur"
  - d.h. einfache oder fortgeschrittene Signatur nach SigG

Open Source Software

- **OSS -> FOSS -> FLOSS**
- **Verschiedene Lizenzen**
  - BSD, Mozilla, MySQL, GPL
  - Dual Licensing
- **GPL, LGPL**
  - Copyleft - virale Verbreitung der Lizenz
  - Weitergabe der Sourcen
- **Vier Freiheiten:**
  - Nutzung ohne Einschränkung
  - beliebige Weitergabe mit Sourcen + gleicher Lizenz
  - Bearbeitung erlaubt
  - Weitergabe von Bearbeitungen mit Sourcen + gleicher Lizenz

Neues in GPL v. 3 von 2007:

- Keine Unterstützung für technischen Kopierschutz + DRM-Maßnahmen
- kostenfreie Patentnutzung
- LGPL ebenfalls in angepasster Version 3
- Kompatibilität mit Afero GPL (Interaktionen in Netzen, Web Services)
- Neue Begrifflichkeiten:
  - Propagation - Kopieren, Verbreiten, Veröffentlichen
  - Conveying - mit Kopien verbundenes propagating
  - Making available to the public / distribution
- Kommerzielle Lizenz: any price or no price
- Damit auch: Vermieten, Verleasen, ASP
- Aber: Immer originäres einfaches Nutzungsrecht vom Rechtsinhaber
- d.h. direktes Lizenzverhältnis zwischen Anwender und original licensor

Open Source Software

- **Inkompatibilitäten:**
- **Vollständiger Gewährleistungsausschluss ("as is")**
  - bei entgeltlicher Überlassung unwirksam, § 309 Nr.8b aa) BGB
  - daraus folgt Überlassungssperre gem. GPLv3 Nr. 12 Satz 2
  - Lösung: Garantieversprechen in Zusatzvertrag
- **Umfassender Haftungsausschluss**
  - würde selbst für Vorsatz und grobe Fahrlässigkeit gelten
  - unwirksam nach §§ 276 Abs. 2, 305 Nr. 7,8 BGB
- **Salvatorische Klauseln (".. applicable law"):** unwirksam
- **Viraler Effekt auch zwischen v2 und v3 der GPL**

FOSS Compliance Guide

- SW-Import kontrollieren
- Einschlägige Lizenz ermitteln
- Bearbeitung kontrollieren (revision control)
- Definierter Build Process (no Guru, please)
- Quelle: www.softwarefreedom.org
- Entscheidungsverantwortlichkeit

Gebrauchte Software

- **Urheberrecht:**
  - Vervielfältigung, Verbreitung nur mit Erlaubnis
- **Erschöpfungsgrundsatz**
  - Datenträger
  - Fungibilität
- **Vertriebsformen:**
  - Einzelstück auf Datenträger
  - Vorinstalliert auf Maschine (Bundling)
  - Kopier-/Volumenlizenz
  - On-Line ohne Datenträger
  - Terminallizenz (Userlizenz)
- **Lösungsansätze**
  - Analogie, Handelbarer Datenbestand (LG Düsseldorf)

Referent

Ernst Dieter Naber
Rechtsanwalt
Fachanwalt für Informationstechnologierecht

Rechtsanwälte
Kühn Jäger Naber
Theodor-Heuss-Ring 28
50668 Köln

www.kjn-law.de
naber@kjn-law.de