Nicht-technische Aspekte der IT-Sicherheit

Fraunhofer Institut
Naturwissenschaftlich-
Technische Trendanalysen

Dipl.-Math. Wilfried Gericke

Vortrag für das Rheinlandtreffen 2006 (07.-08.11.2006)

Motivation

Fraunhofer Institut
Naturwissenschaftlich-
Technische Trendanalysen

Inhalt:

- IT-Sicherheit als Teil der Unternehmensführung
- Gesetzliche Vorgaben und Haftungsrisiken
- IT-Sicherheitsrichtlinie
- Information Security Management System (ISMS)
- EDV-spezifische Straftatbestände
- weitere gesetzliche Regelungen

IT-Sicherheit als Teil der Unternehmensführung

- Corporate Governance (bezeichnet eine gute Unternehmensführung und -kontrolle)
  - ISO9000QM
  - Corporate Risk Management
  - Sarbanes-Oxley Act
  - KonTraG
  - Basel II

IT-Sicherheit als Teil der Unternehmensführung

- IT-Governance (regelt die Steuerung der unternehmenskritischen IT)
  - ITIL (ISO20000)
  - Audit: COBIT,. ..
  - Risikomanagement: FIRM

- IT-Security
  - ISMS: ISO2700 (ehemals BS7799)
  - Risikomanagement
  - Maßnahmen: GSHB
  - technisch: TCSEC (*Trusted Computer System Evaluation Criteria*; im Allgemeinen als ***Orange Book*** bezeichnet),

IT-Sicherheit als Teil der Unternehmensführung

„Sicherheit ist kein Produkt; sie ist ein Prozess. Sie hat mit vorbeugenden Technologien, aber auch mit Erkennungs- und Reaktionsprozessen zu tun.“

(BRUCE SCHNEIER)

Gesetzliche Vorgaben und Haftungsrisiken

- GmbH G§43 verpflichtet den Geschäftsführer die Sorgfalt des ordentlichen Geschäftsmannes anzuwenden
  - Geschäftsführer haften, wenn sie ihre Obliegenheiten verletzen
- BGB §831 verpflichtet den Unternehmer, die Organisationsverantwortung zu übernehmen
  - Kontrollpflicht: Überwachung der Durchführung
  - Auswahlpflicht: geeignetes Personal zur Durchführung auswählen
  - Anweisungspflicht: Vorgaben zur Durchführung der Unternehmenszwecke festlegen

Bei Nichtbeachten droht persönliche Haftung wegen Organisationsverschulden

Gesetzliche Vorgaben und Haftungsrisiken

Haftung (Geschäftsleitung)

Die Verantwortung für die IT-Sicherheit trägt immer die Unternehmensleitung, sie kann auch nicht an andere delegiert werden.

Gesetzliche Vorgaben und Haftungsrisiken

Haftung (IT-Administratoren)

- allgemeine Haftung von Mitarbeitern
  * Schlechterfüllung arbeitsvertraglicher Pflichten (BGB §280)
  * Verletzung von Schutz-, Mitwirkungs- und Aufklärungspflichten
- Wie kann man sich dagegen schützen ?
  * Übertragene Aufgaben gewissenhaft ausführen
  * Unternehmensleitung über mögliche Risiken informieren
  * Vorschläge für die Beseitigung von Sicherheitsrisiken erstellen

Gesetzliche Vorgaben und Haftungsrisiken

Urheberrechtsverletzung

Die Unternehmensleitung verletzt die Organisationspflicht und verstößt gegen §106 UrhG, wenn sie

- das Herunterladen und Verbreiten kopiergeschützter Musik und Filme
- den Einsatz nicht-lizensierter Software

duldet und keine Maßnahmen ergreift, dies zu unterbinden

Gesetzliche Vorgaben und Haftungsrisiken

E-Mails und Fernmeldegeheimnis

-E-Mails unterliegen dem Fernmeldegeheimnis (§206 StGB)

> Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekannt geworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit einer Freiheitsstrafe bis zu 5 Jahren oder mit Geldstrafe bestraft.

-Erbringung „geschäftsmäßiger Telekommunikationsdienste“ gilt auch für Unternehmen, die Mitarbeitern die private Nutzung des Internet erlauben oder dies dulden.

> Strafbestand ist beim Überprüfen des E-Mail-Verkehrs aber auch beim ungenehmigten Löschen von Spam-Mails erfüllt.

Gesetzliche Vorgaben und Haftungsrisiken

E-Mails und Fernmeldegeheimnis

-Zusätzlich verbietet §303a StGB das Unterdrücken von Spam-Mails

> Wer rechtswidrig Daten (§202a Abs.2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu 2 Jahren oder einer Geldstrafe bestraft.

-Lösung: Erstellung einer BV oder einer Sicherheitsleitlinie, die private E-Mail-Nutzung sowie Mail-Filterung regelt.

Gesetzliche Vorgaben und Haftungsrisiken

Archivierungspflichten für E-Mails

- E-Mails als Handelsbriefe gem. §257 HGB:
  * Sämtliche Schriftstücke, die zur Vorbereitung, Durchführung und dem Abschluss oder der Rückgängigmachung eines Geschäftes dienen
  * keine Unterscheidung zwischen Brief, Fax oder E-Mail (nur mit Signatur ?)
  * Archivierungsdauer 10 Jahre
- E-Mails nach §147 AO (Abgabenordnung):
  * Unterlagen, die für die Besteuerung von Bedeutung sind
  * Archivdauer 6 Jahre

- Lösung: Die Unternehmensleitung muss die Archivierung der Mails organisieren.

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Gesetzliche Vorgaben und Haftungsrisiken

Datenschutz – Grundsätze

- Beschränkung der Zweckbestimmung

  Daten sind für einen spezifischen Zweck zu verarbeiten und auch nur zu verwenden oder weiter zu übermitteln, als dies mit dem Zweck nicht unvereinbar ist.

- Datenqualität und –verhältnismäßigkeit

  Daten müssen sachlich richtig und auf dem neuesten Stand sein. Sie sollten angemessen, relevant und nicht exzessiv sein.

- Sicherheit

  Es sind geeignete technische und organisatorische Sicherheitsmassnahmen für die Risiken der Verarbeitung zu treffen.

Fraunhofer Institut Naturwissenschaftlich-Technische Trendanalysen

Gesetzliche Vorgaben und Haftungsrisiken

Bundesdatenschutzgesetz (BDSG)

- Verantwortlich für die Einhaltung der Vorschriften zum Datenschutz ist das jeweilige Unternehmen.
  * Die Unternehmensleitung trägt grundsätzlich die Gesamtverantwortung nach innen und nach außen.
  * Jeder im Unternehmen, der ungesetzlich mit personenbezogenen Daten umgeht, kann dafür auch persönlich zur Rechenschaft gezogen werden.
- Datenschutzbeauftragter
  * Notwendig, wenn mindestens 5 Arbeitnehmer mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind.

Gesetzliche Vorgaben und Haftungsrisiken

- Basel II

  fordert ein Information Risk Management (IRM)
- Sarbanes-Oxley Act (SoX)

  fordert ein internes Kontrollsystem (IKS)
- KonTraG

  fordert ein Information Security Management System (ISMS)

IT-Sicherheitsrichtlinie – Security Policy

- Positionierung der Geschäftsleitung zum Stellenwert der IT-Sicherheit und zum angestrebten Sicherheitsniveau
- Verbindliche Anweisungen der Unternehmensführung zur angestrebten IT-Sicherheit
- Ein Dokument mit generellen Anweisungen der Unternehmensleitung zur Rolle der Sicherheit.

Ohne eine definierte Sicherheitslinie ist keine IT-Sicherheit möglich !

IT-Sicherheitsrichtlinie – Security Policy

Lösungsansatz in der FhG:

IT-Sicherheitspolicy

IT-Rahmenplan

IT-Sicherheitshandbuch

IT-Benutzerordnung

IT-Gesamtbetriebsvereinbarungen

IT-Sicherheitsrichtlinie – Security Policy

Weitere Dokumente

- Standard (Normen)
- Baseline (Mindestanforderung)
- Guidelines (Leitlinien, „Best Practices“)
- Procedures (Verfahren, detaillierte, schriftliche Anleitungen)

Information Security Management System (ISMS)

Aufbau eines ISMS

- Festlegung der Sicherheitsziele und des zu schützenden Bereichs
  was soll geschützt werden
- Ermitteln des Schutzbedarfs
  wie wirksam soll geschützt werden
- Analyse der Bedrohungen und Risiken
  was sind die Risiken
- Festlegen und Implementieren der Sicherheitsmaßnahmen
  wie soll geschützt werden
- Prüfen der Wirksamkeit der Maßnahmen
  bieten die Maßnahmen genügend Schutz

Information Security Management System (ISMS)

ISO27001 / BS7799-2

- Geschäfts- und Prozessorientierter Top-Down Ansatz
  * keine detaillierten Maßnahmen
  * beschreibt nur die Anforderungen an ein solches System
- Maßnahmen zur Umsetzung des ISMS
  * ISO17799 / BS7799-1
  * BSI Grundschutzhandbuch

Information Security Management System (ISMS)

ISO17799 / BS7799 – Code of Practice

Besteht aus ca 130 Kapitel, die so genannten controls;

Implementation Guidance

Information Security Management System (ISMS)

BSI Grundschutzhandbuch

Technik-orientierter Bottom-Up Ansatz, kein Management-Standard

* Kataloge möglicher Gefährdungen
* Empfohlene Standard-Sicherheitsmaßnahmen
* Einschätzungshilfen zum Schutzbedarf

Erspart für IT-Bereiche mit geringem oder mittleren Schutzbedarf aufwändige Risiko-analysen

EDV-spezifische Straftatbestände

Verletzung des persönlichen Lebens- und Geheimbereiche

Verletzung des Briefgeheimnisses §202

Ausspähen von Daten §202a

Verletzung von Privatgeheimnissen §203

Verwendung fremder Geheimnisse §204

Verletzung des Post- und Fernmeldegeheimnisses §206

EDV-spezifische Straftatbestände

- Betrug und Untreue
  - Computerbetrug §263a
  - Erschleichung von Leistungen §265a
- Urkundenfälschung
  - Fälschung technischer Aufzeichnungen §268
  - Fälschung beweiserheblicher Daten §269
  - Täuschung im Rechtsverkehr bei Datenverarbeitung §270
  - Urkundenunterdrückung §274

EDV-spezifische Straftatbestände

- Datenveränderung §303a
- Computersabotage §303b

EDV-spezifische Straftatbestände

unlauterer Wettbewerb

Verrat von Geschäfts- und Betriebsgeheimnissen §17 UWG

Verwertung von Vorlagen §18 UWG

Außenwirtschaftsgesetz

Technologietransfer (Dual Use ?)

weitere gesetzliche Regelungen:

TDDSG Gesetz zum Datenschutz bei Telediensten

TDG Gesetz zur Nutzung von Telediensten

TKG Telekommunikationsgesetz

Fernmeldegeheimnis §88

Fragen ?

Fraunhofer Institut
Naturwissenschaftlich-
Technische Trendanalysen