

## IT-Sicherheit 2009: Nur Profis leben ohne Risiko!

Robert Niedermeier  
Rechtsanwalt

# Ausgangslage

Mitarbeiter

Vertrieb

Kunden

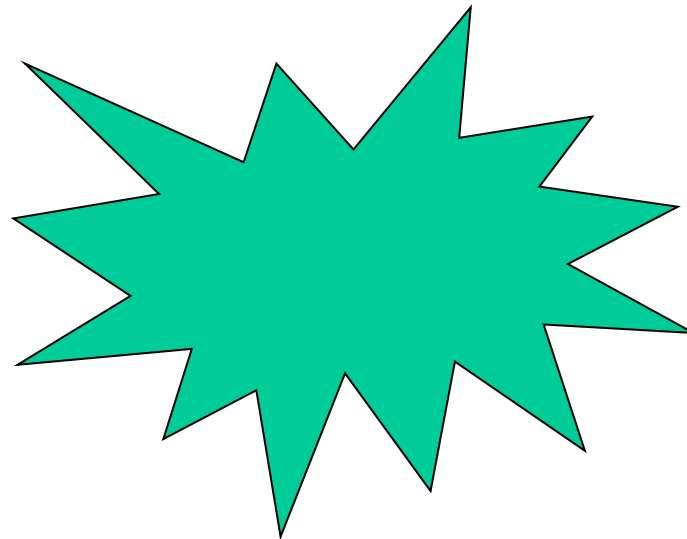
Finanzen

B2B

Marketing

Partner

Logistik



**EDV- Systeme sind „gemeingefährliche Anlagen“!**

# Herausforderungen

Gesetzliche Vorschriften  
(Compliance)

Die Einhaltung gesetzlicher Vorschriften erfordern eine bessere Kontrolle und Nachvollziehbarkeit von IT-Management-Prozessen.

Effiziente Geschäfts-  
Prozesse

CIOs sind permanent gefordert, die Anwendungsproduktivität zu steigern und das Sicherheitsniveau zu erhöhen mit gleichzeitiger Reduzierung der Kosten.

Ganzheitlicher  
Sicherheitsbedarf

Trends wie Mobilität und Globalisierung bringen neue Bedrohungen für Unternehmen, öffentliche Verwaltung und Einzelpersonen.

# Compliance

- Compliance: Einhaltung von Vorschriften und Regelungen für Unternehmen
- Forderung an die IT
  - Sicherheit der IT- Systeme und –Prozesse
  - Definierte Delegation von Verantwortlichkeiten
  - Dokumentation/ Archivierung
  - Nachvollziehbarkeit/ Revisionsfähigkeit
- Grundfragen
  - Wer darf was machen?
  - Wer hat wann was gemacht?
  - Warum durfte wer was machen?
- Die Identität spielt eine zentrale Rolle
- Identity Management ist eine unverzichtbare Basis für Compliance
  - Basis für Authentifizierung und Autorisierung
  - Basis für zentrale, anwendungsübergreifende Sicherheitskonzepte
  - Basis für Auditing

**Keine Compliance ohne Identity Management!**

## Verantwortungsverteilung - Allgemein

IT-Security Risiken sind vorhersehbar und somit zurechenbar. Die Geschäftsleitung kann sich insofern nicht exkulpieren und muss alles Notwendige unternehmen um Haftungsrisiken abzuwenden. Dazu bedarf es zumindest eines Sicherheitsmanuals, dass im Ernstfall rechtlich abgesicherte Anweisungen gibt. Nur so können zivil- und strafrechtliche Risiken vom Unternehmen und der Geschäftsleitung fern gehalten werden.

## Verantwortungsverteilung - Im Besonderen

- Leitende Angestellte unterliegen einem erhöhten Sorgfaltsmaßstab, der mit der Position im Unternehmen steigt.
- Der IT- Entscheider haftet als Privatperson gegebenenfalls mit dem eigenen Vermögen

# Hauptproblem: Haftung

Nach dem Urteil des Landgerichts Nürnberg-Fürth (Urteil vom 10.04.2002, AZ: 10 O 8034/01) ist eine im Online-Bereich tätige Bank verpflichtet, geeignete technische und organisatorische Vorkehrungen zu treffen, die sicherstellen, dass im Internet erteilte unplausible und offensichtlich irrtümliche Aufträge als solche erkannt werden.

# Hauptproblem: Haftung

Hat eine Bank die notwendige Sicherung bei der Auftragserteilung nicht eingebaut, ist sie dem Kunden zum Ersatz des hieraus entstandenen Schadens verpflichtet.

## Technische Risiken

Überlastung des Netzwerkes

Daten- und  
Anwendungssicherheit

Vertraulichkeit, Integrität

## Finanzielle Risiken

Produktivitätsverluste

Kostensteigerungen

verlorene Arbeitszeit

# Regel

- IT-Sicherheit ist Chefsache!
- Denn:
  - Zivil- und arbeitsrechtliche Haftung im Außenverhältnis setzt idR Verschulden voraus → Organisationsverschulden der Unternehmensführung
  - → führt zu Haftung der Unternehmensführung im Innenverhältnis

# Folge

- Verpflichtung, „angemessenes“ IT-Sicherheitsniveau zu garantieren
- → Problem: Was heißt „angemessen“?
- Kriterien: Branchenüblichkeit, Audits, Codes of Conduct, etc.

Organisations-  
Verpflichtung

Art 4 EKDSRL

SOX / Basel II / KontraG

T

O

S

R

# Organisationsverpflichtung

Ein Unternehmen ist nach den Vorschriften der Gewerbeordnung gehalten, seine Applications entsprechend Art und Umfang des Geschäfts so auszugestalten, wie dies für eine ordentliche Durchführung des Geschäfts erforderlich ist.

## Organisationsverpflichtung- Im Einzelnen

Hierzu zählen über die notwendigen Sicherheitsmaßnahmen hinaus verschiedene Organisationspflichten, die die einwandfreie Abwicklung eines IT- Betriebs ermöglichen und sicherstellen.

## Art 4 Abs. 1 EKDSRL

Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveaugewährleisten, das angesichts des bestehenden Risikos angemessen ist.

## Art 4 Abs. 2 EKDSRL

Besteht ein besonderes Risiko der Verletzung der Netzsicherheit, muss der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes die Teilnehmer über dieses Risiko und — wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt — über mögliche Abhilfen, einschließlich der voraussichtlich entstehenden Kosten, unterrichten.

## Art. 4 EKDSRL

- Neue Anforderungen hinsichtlich der Betriebssicherheit
- Die Maßnahmen nach Art. 4 Abs. 1 EKDSRL müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.

# § 9 BDSG

## Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, [...] haben die technischen und organisatorischen Maßnahmen zu treffen, die ***erforderlich*** sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem ***angemessenen Verhältnis zu dem angestrebten Schutzzweck*** steht.

# Anlage zu § 9 BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

# Sarbanes-Oxley-Act (SOX)

- Vorstandsvorsitzende und Finanzvorstände (CEO und CFO) haften persönlich!
- Betrifft deutsche Unternehmen, die in den USA auftreten
- Ziel des Gesetzes: Wiederherstellung des Vertrauens der Anleger in die Richtigkeit der öffentlichen Finanzdaten von Unternehmen, die den amerikanischen Rechtsvorschriften unterliegen.

# Wichtige Bestandteile des SOX

- Strafrechtliche und zivilrechtliche Strafen für Sicherheitsverstöße
- Unabhängigkeit der internen und externen Unternehmensprüfungen
- Erhöhte Mitteilungspflicht über Gehälter der Unternehmensleitung und zu veröffentlichender Unternehmensinformationen

# Basel II

Einrichtung von Unternehmensprozessen zur Kontrolle und zum Management von Risiken und Anlagewerten eines Unternehmens.

# Forderungen von Basel II

- Ein aussagekräftiges und jederzeit aktuelles IT-Asset- und Lizenzmanagement als Beitrag zum Bestandsmanagement des Unternehmens
- Ein geeignetes Benutzer-Management, welches insbesondere die Gefahren durch „Unangemessenheit“ oder Versagen von Prozessen, Menschen und Maschinen reduziert

# Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Keine Mindestanforderungen an die Unternehmen, sondern Definition von erweiterten Pflichten der Unternehmensleitungen bezüglich des Risikomanagements und der Risikosteuerung.

# Präzisierung § 92 Abs. 2 d AktG

„Der Vorstand hat geeignete Maßnahmen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“

# Raster IT Sicherheit

<b>T</b>	<b>O</b>	<b>S</b>	<b>R</b>

# Zur Erinnerung: Regel

- IT-Sicherheit ist Chefsache!
- Denn:
  - Zivil- und arbeitsrechtliche Haftung im Außenverhältnis setzt idR Verschulden voraus → Organisationsverschulden der Unternehmensführung
  - → führt zu Haftung der Unternehmensführung im Innenverhältnis

# ABER

- IT-Sicherheit ist auch Administratorsache
  - strafrechtliche, TKG-, arbeitsrechtliche Konsequenzen bei Problemen
- IT-Sicherheit ist auch Betriebsratssache
  - Betriebsvereinbarung als Steuerungsinstrument der IT-Nutzung durch Mitarbeiter

# Regeln

- Reden Sie mit Ihrer IT-Abteilung!
- Verantworten und verstehen Sie ein Sicherheitskonzept!
- Reden Sie mit Ihrem Betriebsrat!
- Verantworten und verstehen Sie die Grundsätze des BDSG!

# Tatort Internet

## Spielplatz der Betrüger?

Das Internet als globales Kommunikationsnetz wird nicht nur zu legalen Zwecken genutzt. Vielmehr erscheint es, dass sich das Internet zu einem Spielplatz für Nepper, Schlepper und Bauernfänger entwickelt hat. Spamming, Phishing, Port-Scanning, Backdoor-Hacking, Social-Engineering, Viren, Root Kits, Trojaner, Würmer, Spam-Bots, Key-Logger, Nigeria-Connection, DDoS, Wardriving, Snarfing, usw. sorgen für eine zunehmende Verunsicherung unter Firmen und Privatpersonen.

# Tatort Internet

## Wardriving

### Wardriving:

- Mobile Suche nach offenen WLAN / Bluetooth Verbindungen.
- Mittels Snarfing sind Man-in-the-Middle Attacken möglich.
- Hohes Risiko des Datendiebstahls und der Datenmanipulation.
- Haftung für Handlungen Dritter möglich.

# Tatort Internet

## Wardriving

### Haftung nach den Grundsätzen der Störerhaftung:

- Urteil des LG Frankfurt am Main vom 22.02.2007:LG Frankfurt/Main:  
„Der Beklagte hat für die begangene Rechtsverletzung einzustehen. Dabei kann dahinstehen, ob er selbst die Handlungen begangen hat.

Es ist nämlich nicht auszuschließen, dass die Rechtsverletzung durch andere nicht bekannte Nutzer des Anschlusses erfolgt ist, die die ungeschützte WLAN-Internetverbindung des Beklagten genutzt haben. Für diese Rechtsverletzung hat der Beklagte indes gleichfalls nach den Grundsätzen der Störerhaftung einzustehen.

**Rechtlich und tatsächlich war der Beklagte in die Lage versetzt, wirksame Maßnahmen zur Verhinderung der streitgegenständlichen Rechtsverletzung zu treffen. Es oblag ihm, sich zu informieren, welche Möglichkeiten für Rechtsverletzungen er schafft und wie er solchen Verletzungen hätten vorbeugen können.“**

### Vorschussbetrug oder die Nigeria-Connection

- Erste Fälle bereits im 16. Jahrhundert per Briefpost.
- Das System dieser Betrügerei zielt darauf ab, das Opfer zu einer Zahlung für verschiedene fiktive Kosten zu veranlassen, damit ein Geldtransfer abgeschlossen werden kann.
- Die Stadt Enningerloh zahlte im Zeitraum 1991 bis 2001 insgesamt 288.000 DM an einen Sozialhilfeempfänger. Dieser sollte über die Bank of Nigeria die Auszahlung von 30 Mio. \$ erreichen, womit der Bürgermeister den Stadthaushalt sanieren wollte. Der Bürgermeister verlor sein Amt und musste sich wegen der Veruntreuung öffentlicher Gelder vor Gericht verantworten.

# Tatort Internet Nigeria Connection

## Beispiel eines Nigeria-Connection Briefes:

„Sehr Geehrter freundlichen,  
[...]ich arbeite bei einer Finanzhaus in den Niederlanden [...]Während unseres letzten Treffens und Überprüfung der Bankkontos hat meine Abteilung ein untätiges Konto mit einer riesigen Geldsumme, US\$ 6,500,000.00 gefunden, das einem unseren gestorbenen Kunden gehört [...] Wegen unseren Finanzhaus vorschriften kann nur ein Ausländer als nächster Verwandten stehen und deshalb habe ich mich entschlossen Sie zu kontaktieren, um mit Ihnen zusammen zu arbeiten um diese untätigen Fonds zu reaktivieren [...] so dass die Fonds freigestellt und auf ihr Konto überwiesen werden können [...] Am Ende der Transaktion werden Ihnen 40% Prozent zustehen, zur Seite gelegt und 60% werden für meine Kollegen und mich sein. [...]Wir haben nicht viel Zeit diese unglückliche Situation zu ändern und ich befürchte, dass ohne Ihre Hilfe alles verloren gehen wird. Wegen der Vertraulichkeit bitte ich Sie mir auf meine privaten Email Adresse mit folgenden Angaben zu antworten:  
Vollständiger Name, Adresse, Telefon- und Faxnummer [...]“

# Tatort Internet

## Email im Unternehmen

### Beispiel: Verleumdung über Firmenverteiler

„Sehr geehrte Herren,  
Ich habe ein großes Problem, was mein Gewissen belastet. Da ich bereits im Fall XXX versucht habe die Geschäftsleitung auf Unregelmäßigkeiten aufmerksam zu machen, was jedoch ohne Erfolg war, sehe ich mich gezwungen den direkten Kontakt mit Ihnen aufzunehmen. [...]habe ich schon mehrere Fälle kennen gelernt in denen Angestellte aus dem Unternehmen entfernt wurden, nachdem sie sich kritisch der Geschäftsleitung gegenüber geäußert haben [...] Wie kann es sein, dass YYY Seine Position ausnutzt und so Mitarbeiter erniedrigt und persönlich gedemütigt werden [...] auch vor persönlicher Beleidigung schreckt YYY nicht zurück. [...] Es wäre schade, wenn der große Erfolg durch das niveaulose Verhalten des YYY verloren geht.“

# Tatort Internet

## Email im Unternehmen

Imageverlust durch unsachgemäße betriebliche Übung. Beispiel anhand privaten Emailverkehrs zweier BA-Mitarbeiterinnen aus Nürnberg.

- unbedachter Umgang schafft Gefahrenräume.
- vorsätzliches Handeln nicht notwendig.
- Gefahr der negativen Publicity.
- sehr großer Wirkungskreis.
- schnelle Verbreitung.

# Tatort Internet

## Computerviren und Hacker Tools

### Fragestellungen:

- „Experten“ tauschen Viren
- „Experten“ setzen Hackertools ein
- „Experten“ arbeiten im Bereich IT Sicherheit

# Tatort Internet

## Betrug durch Identitätstäuschung

Durch das Abfangen der Anmeldeinformationen zu einer Packstation der Deutschen Post konnte ein Betrüger Waren im Wert von mehreren tausend Euro auf fremden Namen bestellen. Die Waren kamen nie an, die Rechnungen der Lieferanten schon.

Gefahr droht jedoch auch von staatlicher Seite:

**„Entwurf zum Strafrechtsänderungsgesetz  
zur Bekämpfung der Computerkriminalität“**

### § 202c StGB

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passworte oder sonstige Sicherungscodes, die den Zugang zu Daten (§202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

*herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.*

### Der sogenannte Hackerparagraph § 202c StGB

#### Zielsetzung:

- Schließung von Strafrechtslücken im Bereich der Computerkriminalität.
- Erleichterung der Beweisführung im Rahmen von Beihilfe-Delikten.
- Strafbarkeit der Vorbereitung von Internetdelikten.
- Jedoch auch staatliche Sanktionierung der besonderen Gefährlichkeit von Hacker-Tools.

### **Die andere Seite der Medaille - Praktische Probleme des § 202c StGB:**

- Anwendungsbereich zu weit gefasst – bedingter Vorsatz reicht aus.
  - Gefahr der Überkriminalisierung.
- Rechtsunsicherheit erst durch höchstrichterliche Rechtssprechung zu beheben.
- Schädigung des Wirtschaftsstandorts Deutschland.

### Anwendungsumfang des § 202c StGB:

- IT-Security Werkzeuge, wie
  - sniffer
  - scanner
  - logger
- Entwicklung von Anti-Virensoftware
  - für die Entwicklung einer tauglichen Antvirensoftware ist die Analyse der Viren erforderlich. Hierfür müssen sich die Hersteller die Viren „beschaffen“.
- der konkrete Anwendungsumfang ist jedoch noch nicht absehbar

### **Dreh- und Angelpunkt - Der Rechtsbegriff „unbefugt“**

- § 202c soll Vorbereitungshandlungen zu § 202a und § 202b unter Strafe stellen. Für die Begehung der „Hauptstraftaten“ ist jedoch der Begriff „unbefugt“ von zentraler Bedeutung.
- Das Vorliegen dieses Merkmals wird von den Staatsanwaltschaften im Ermittlungsverfahren zu erforschen sein.

### Lösungsansatz:

- Feststellung des Bedrohungsszenarios
  - werden IT-Sicherheitstools eingesetzt?
- Schriftliche Fixierung der Berechtigung durch
  - vertragliche Regelung
  - Lizenzanpassungen im Bereich Anti-Virus

**Generell zur IT-Sicherheit ist folgendes  
festzuhalten**

# Tatort Internet

## IT-Sicherheit

- IT Sicherheit hat eine hohe Bedeutung für die Betriebskontinuität
- Defizite in der IT Sicherheit gefährden das Unternehmen
- Defizite bei der IT Sicherheit führen zur Haftung des Vorstands und der Stabsstellen
- Sofortiges Handeln ist erforderlich um den Vorwurf der Fahrlässigkeit zu entgehen
- Versicherungsschutz kann ausfallen
- Leitende Angestellte unterliegen einem erhöhtem Sorgfaltsmaßstab, der mit der Position im Unternehmen steigt.
- Der IT-Entscheider haftet als Privatperson gegebenenfalls mit dem eigenem Vermögen

### Lösungsansätze:

- Budget für IT Sicherheit explizit ausweisen
- Spielfelddefinition
- Analyse der Exponierung
- Schaffung von Strukturen der IT Sicherheit in den Bereichen Technik, Organisation, Strategie und RECHT
- Dokumentation
- Audit
- Schaffung messbarer IT Sicherheit

**Vielen Dank für Ihre Aufmerksamkeit**

**Robert Niedermeier**

Heussen Rechtsanwaltsgesellschaft mbH

Brienner Straße 9/Amiraplatz

80333 München

Tel: 089.29097-0

Fax: 089.29097-200

eMail: [Robert.Niedermeier@heussen-law.de](mailto:Robert.Niedermeier@heussen-law.de)

[www.heussen-law.de](http://www.heussen-law.de)