

IT Security ist Chefsache

Rechtliche Aspekte im Umfeld von IT Security

RA Wilfried Reiners, MBA

Agenda

- **Einführung in das Thema**
- **Anspruchsgrundlagen**
- **Haftungsrisiken**
- **Fallbeispiele für Viren, Würmer, Lücken und Attacken**
 - **Fremder Angriff**
 - **Eigener Angriff**
 - **Eigene Sorglosigkeit**
- **Rechtsfolgen für Schädiger + Geschädigte**
- **Todo-Liste**

IT-Sicherheits-Umgebungen

Arbeiten mit E-Mail und Internet

Firmen-Präsenz im Netz

Lokale Firmennetze

Datenaustausch mit Kunden, Filialen und Lieferanten

Mobiles Arbeiten

Offene Türen

Wer ist schuld, wenn der Dieb bei Ihnen offene Türen vorfindet?

Sie sagen: **Der Dieb**

Ihre Versicherung sagt: **Sie!**

Grundsatz:

Sie müssen für Ihre Sicherheit selbst sorgen

Wichtiger noch: **Sie müssen dafür sorgen!**

Gesetze schützen nicht

Gibt es keine Mörder, nur weil Mord strafbar ist?

§ 303a StGB Datenveränderung

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

(2) Der Versuch ist strafbar.

Existierende Regelungen

§ 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, daß er

- 1. eine Tat nach § 303a Abs. 1 begeht oder*
- 2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,*

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

www.hacker-software.de

Hacker-Software.de
The best Hackersite on net!

Ihr wollt Passwörter herausbekommen? Dann benötigt ihr einen Brudeforcecracker!

Ihr wollt Kontrolle über andere PC's, dann braucht ihr einen Trojaner

Ihr wollt jemand einen Virus schicken? Dann braucht ihr einen Virengenerator

Hacker benutzen viele Programme hier wollen wir euch einmal ein paar vorstellen!

- Ihr wollt **Passwörter herausbekommen**? Evtl. mit **Bruce Force**? Dann benötigt ihr einen Bruceforcecracker!
- Ihr **wollt die Kontrolle über andere PC's** dann braucht ihr einen Trojaner.
- Wollt jemanden einmal einen Virus schicken? Dann braucht ihr ein Virengenerator
- ...

Hacker benutzen aber auch andere Programme wie z.B.

- Trojaner
- Sniffer
- Portscanner
- Spoofer
- Hex-Editor

Vertrauen auf Lösungen

Es gibt keine 100% Sicherheit.

Wenn Sie Ihrer Schließanlage vertrauen, dann können Sie auch professioneller IT Sicherheit vertrauen.

In beiden Fällen gibt es gute und schlechte, teure und günstige Lösungen.

„**Ignorieren**“ ist keine Lösung. Sie haben nicht mal das Recht dazu!

Sorgfaltspflichten

Das offensichtliche Vorhandensein von Angreifern und Angriffsmöglichkeiten, fordert von den IT Verantwortlichen die Aufgabe der Sorglosigkeit.

Wer sorglos ist, haftet!

Immer!

Schützen statt haften!



Mich gibt's
auch digital!

Anspruchsgrundlagen

Mit Einführung des Gesetzes zur Kontrolle und Transparenz im Unternehmen (KonTraG) im Mai 1998 sind Aktiengesellschaften sowie Tochterfirmen (unabhängig von ihrer Gesellschaftsform) zur Implementierung eines unternehmensweiten Früherkennungs- systems für bestandsgefährdende Risiken sowie eines entsprechenden Überwachungssystems verpflichtet. Dies betrifft auch die IT Landschaft.

Wer nicht einführt haftet **persönlich**.

Anspruchsgrundlagen

Im Aktiengesetz ist festgelegt, dass ein Vorstand persönlich haftet, wenn er Entwicklungen, die zukünftig ein Risiko für das Unternehmen darstellen könnten, nicht durch ein Risikomanagement überwacht und durch geeignete Maßnahmen vorbeugt (§ 91 Abs. 2 und § 93 Abs. 2 AktG).

Geschäftsführern einer GmbH wird im GmbH-Gesetz "die Sorgfalt eines ordentlichen Geschäftsmannes" auferlegt (§ 43 Abs. 1 GmbHG).

Anspruchsgrundlagen

Hieraus lassen sich konkrete Verpflichtungen für die Gewährleistung eines angemessenen IT-Sicherheitsniveaus im eigenen Unternehmen ableiten.

Für bestimmte Berufsgruppen gibt es darüber hinaus noch höhere Anforderungen, bis zu Regelungen im Strafgesetzbuch (§ 203). Ein fahrlässiger Umgang mit Informationstechnik kann diesen Tatbestand bereits erfüllen.

Auch Banken berücksichtigen, bei der Kreditvergabe IT-Risiken des Kreditnehmers - mit unmittelbaren Auswirkungen auf die angebotenen Konditionen (Basel II).

Fallbeispiel 1

Szenario

Sie sind Vorstand / Geschäftsführer einer Firma. Ein Hacker dringt in Ihr EDV System ein und entwendet vertrauliche Entwicklungsdaten Ihrer Kunden. Den Kunden entsteht Schaden. Diesen wollen sie von Ihrem Unternehmen ersetzt verlangen. Hilfsweise von Ihnen persönlich.

Zu Recht?

Fallbeispiel 2

Szenario

Sie sind Vorstand / Geschäftsführer einer Firma. Einer Ihrer Mitarbeiter surft in Ihrem Auftrag im Internet und fängt sich einen Virus ein. Das merkt er nicht und er überträgt den Virus an einen Ihrer Kunden. Dem Kunden entsteht ein Schaden. Diesen will er von Ihrem Unternehmen ersetzt verlangen.

Zu Recht?

Fallbeispiel 3

Szenario

Sie sind Vorstand /Geschäftsführer einer Firma. Die Firma betreibt auch einen Internetshop. Für IT-Sicherheit haben Sie sich nicht interessiert. Der Shop wird Opfer einer Attacke und kann tagelang nicht liefern, weil die Daten verloren gegangen sind. Es kommt zu großen Umsatz-Ausfällen. Ihr Gesellschafter will den Schaden von Ihnen persönlich ersetzt haben?

Zu Recht?

Alles Theorie?

Manager haften persönlich

"ARAG-Garmenbeck"-Entscheidung des BGH v. 21.04.1997

Schadensersatz bei Verbreitung eines Computervirus

- LG Hamburg, Urteil vom 18.07.2001, Az: 401 O 63/00

Schadensersatz bei Serverausfall

Amtsgericht Charlottenburg 208 C 192/01

USW.....

Bekannte Täter

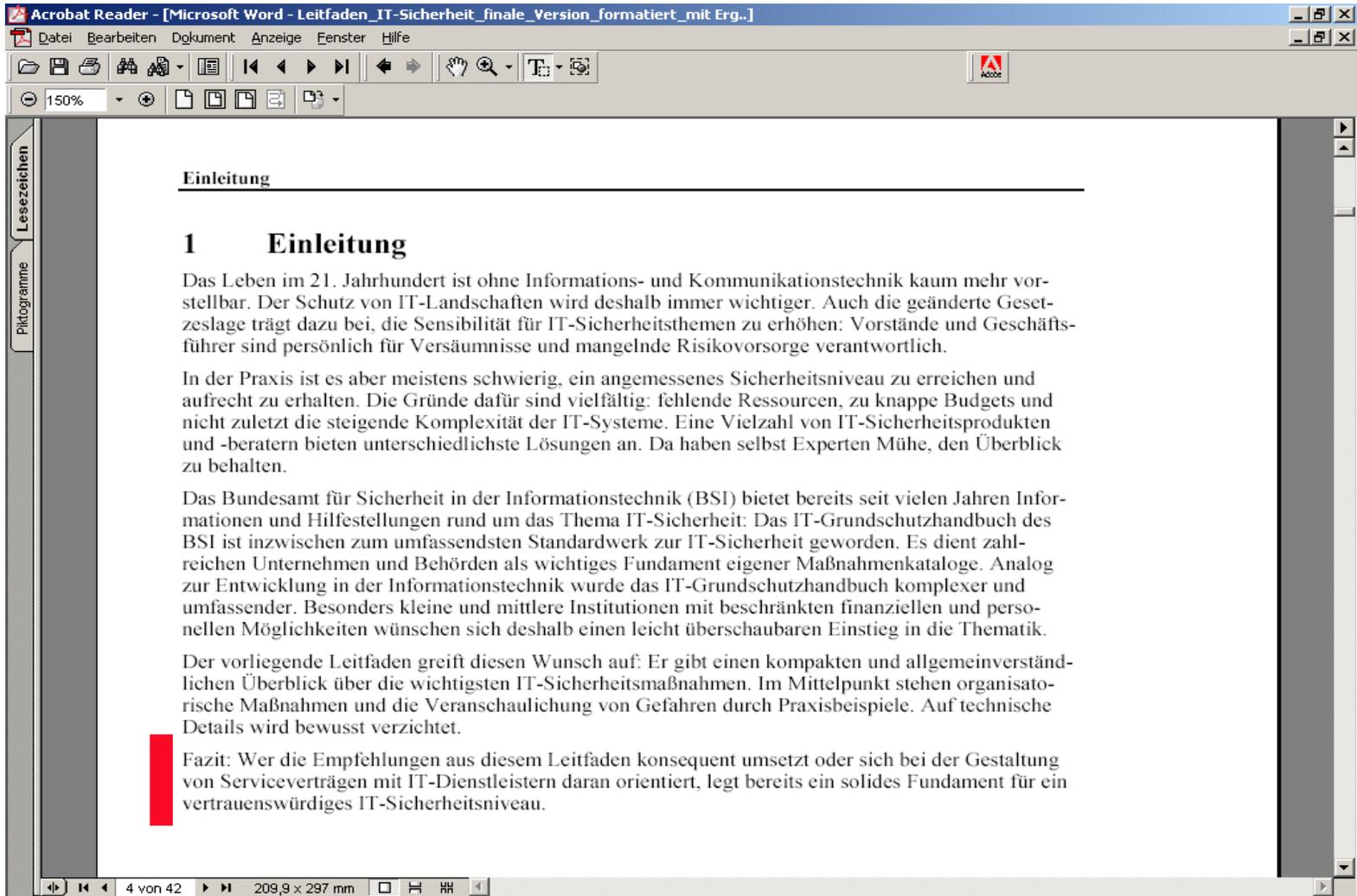
Zwei Drittel aller aktiven oder unbeabsichtigten Systemangriffe in Deutschland – so das Bundeskriminalamt – gehen auf das Konto der **eigenen Angestellten.**

(Quelle: <http://finanzen.focus.msn.de/D/DA/DAE/DAE47/dae47.htm>)

IT Security



IT Security



Acrobat Reader - [Microsoft Word - Leitfaden_IT-Sicherheit_finale_Version_formatiert_mit Erg..]

Datei Bearbeiten Dokument Anzeige Fenster Hilfe

150%

Einleitung

1 Einleitung

Das Leben im 21. Jahrhundert ist ohne Informations- und Kommunikationstechnik kaum mehr vorstellbar. Der Schutz von IT-Landschaften wird deshalb immer wichtiger. Auch die geänderte Gesetzeslage trägt dazu bei, die Sensibilität für IT-Sicherheitsthemen zu erhöhen: Vorstände und Geschäftsführer sind persönlich für Versäumnisse und mangelnde Risikovorsorge verantwortlich.

In der Praxis ist es aber meistens schwierig, ein angemessenes Sicherheitsniveau zu erreichen und aufrecht zu erhalten. Die Gründe dafür sind vielfältig: fehlende Ressourcen, zu knappe Budgets und nicht zuletzt die steigende Komplexität der IT-Systeme. Eine Vielzahl von IT-Sicherheitsprodukten und -beratern bieten unterschiedlichste Lösungen an. Da haben selbst Experten Mühe, den Überblick zu behalten.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet bereits seit vielen Jahren Informationen und Hilfestellungen rund um das Thema IT-Sicherheit: Das IT-Grundschutzhandbuch des BSI ist inzwischen zum umfassendsten Standardwerk zur IT-Sicherheit geworden. Es dient zahlreichen Unternehmen und Behörden als wichtiges Fundament eigener Maßnahmenkataloge. Analog zur Entwicklung in der Informationstechnik wurde das IT-Grundschutzhandbuch komplexer und umfassender. Besonders kleine und mittlere Institutionen mit beschränkten finanziellen und personellen Möglichkeiten wünschen sich deshalb einen leicht überschaubaren Einstieg in die Thematik.

Der vorliegende Leitfaden greift diesen Wunsch auf: Er gibt einen kompakten und allgemeinverständlichen Überblick über die wichtigsten IT-Sicherheitsmaßnahmen. Im Mittelpunkt stehen organisatorische Maßnahmen und die Veranschaulichung von Gefahren durch Praxisbeispiele. Auf technische Details wird bewusst verzichtet.

Fazit: Wer die Empfehlungen aus diesem Leitfaden konsequent umsetzt oder sich bei der Gestaltung von Serviceverträgen mit IT-Dienstleistern daran orientiert, legt bereits ein solides Fundament für ein vertrauenswürdiges IT-Sicherheitsniveau.

4 von 42 209,9 x 297 mm

Jobsicherungsinteresse

**Vertrauen ist gut,
Kontrolle ist besser.**

(Lenin)

**Was muss kontrolliert werden?
Was darf kontrolliert werden?**

Todo-Liste

- Machen Sie IT Sicherheit zur Chefsache
- Bestellen Sie einen Verantwortlichen für die IT Sicherheit
- Holen Sie sich professionelle Beratung ins Haus
- Befreien Sie sich von der Durchgriffshaftung
- Erstellen Sie eine betriebsinterne Richtlinie / Betriebsanweisung für den Umgang mit E-Mails und die Nutzung des Internet
- Schulen Sie die Mitarbeiter zum Thema IT Sicherheit
- Erstellen Sie einen Notfallplan für den Ausfall verschiedener Komponenten, z.B. der Firewall, einem Virus Angriff, einem Angriff durch einen Hacker, etc.

Kontakt

PRW Rechtsanwälte

RA Wilfried Reiners, MBA

Steinsdorfstr. 14

80538 München

Tel: +49-89-2109770

E-mail: office@prw.de

Internet: www.prw.info