

DNS & WatchGuard X Days



Rechtliche Aspekte im Umfeld von IT Security

RA Wilfried Reiners, MBA

Vorstellung

- **Seit 15 Jahren Spezialkanzlei im IT Umfeld.**
- **Kunden: SW-, HW Hersteller, IT-Dienstleister.**

47 %

aller Einführungen von Unternehmenssoftware scheitern

84 %

überschreiten Zeit- und Kostenvorgaben

(Standish Group, 2001)

Wer hat den Hut auf?

IT Dienstleister

- Sales / Beratung
- GL

Kunde

- IT Leiter / Einkauf
- GL

Fakten zur IT Security

- 2002: 25 Mrd. \$ Schäden durch Viren
- 2003: 55 Mrd. \$ Schäden durch Viren
- Opfer schweigen
- Jährlich interessiert nicht die
Sicherheit der
Geschäftsführung
- 80% der Unternehmen mit
Netzwerke, ca. ¼ der Betriebe bis 350
HR hat keine Regelung für den Ernstfall
getroffen.

Vertriebsansätze für IT Security

„Die Fachleute sind alarmiert, aber bei den Geschäftsführern fehlt die Sensibilität für das Thema“.

Katrin Sobania, DIHT in DER TAGESSPIEGEL, 5. Mai 2004

Vertriebsansätze für IT Security

Angst verkauft!

Es ist die Angst der Spitze, dass es sie trifft, sie persönlich. Und sie kann nur eines dagegen tun, sich nachweislich IT-Sicherheit einkaufen.

IT Security

End-Kundenvortrag

Adressaten:

GL / Vorstand und IT-Einkauf

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!**

Die 3 Chef-Taugenichtse

Der Sorglose

Es ist noch immer gut gegangen.

Der Glückspilz

Das hätte auch richtig schief gehen können.

Der Ungläubige

Das hätte ich nie gedacht.

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

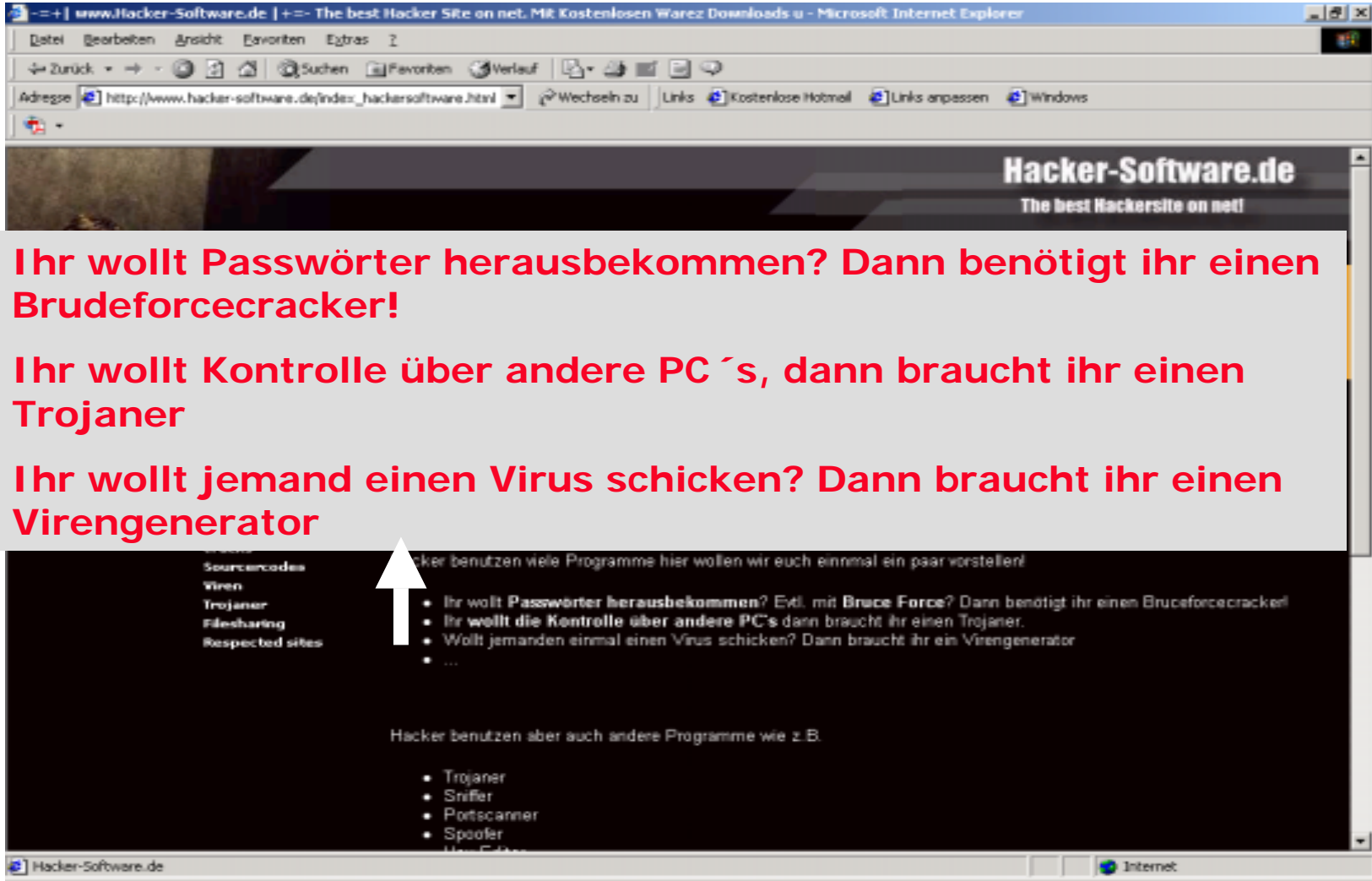
(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, daß er

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

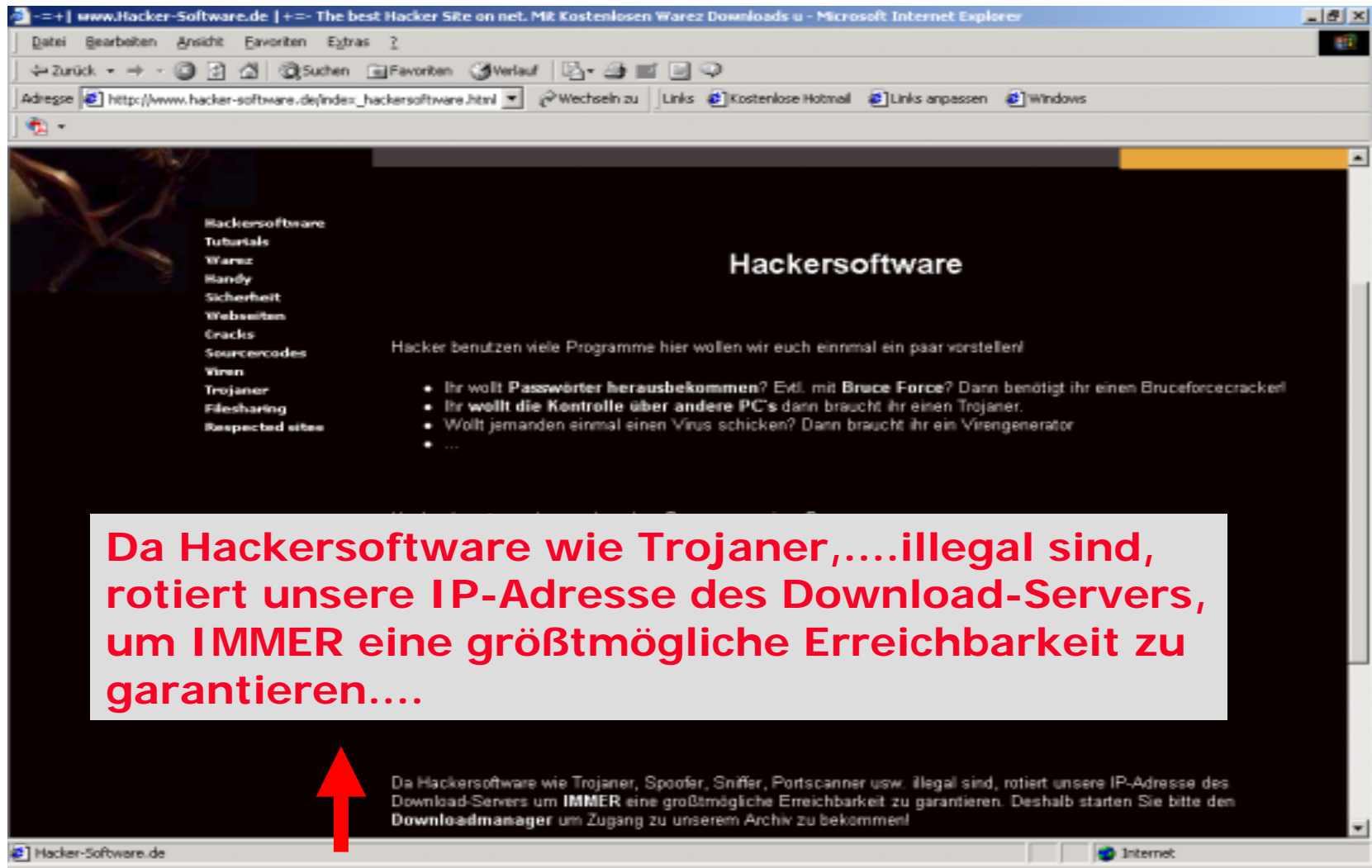
wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

www.hacker-software.de



www.hacker-software.de



Da Hackersoftware wie Trojaner,....illegal sind, rotiert unsere IP-Adresse des Download-Servers, um IMMER eine größtmögliche Erreichbarkeit zu garantieren....



Da Hackersoftware wie Trojaner, Spoofer, Sniffer, Portscanner usw. illegal sind, rotiert unsere IP-Adresse des Download-Servers um IMMER eine größtmögliche Erreichbarkeit zu garantieren. Deshalb starten Sie bitte den Downloadmanager um Zugang zu unserem Archiv zu bekommen!

www.hacking.de

The screenshot shows a Microsoft Internet Explorer browser window displaying the website <http://www.hacking.de/>. The browser's address bar shows the URL, and the page title is "hacking.de - security, information, community". The website has a dark blue and black theme. At the top, there is a navigation bar with links for "Start", "Download", "WebTester", and "Impressum". Below this is a large banner image with the text "PIRATOS.de" in white. A search bar is located on the right side of the banner. The main content area is divided into several columns, each with a category title and a list of sub-items:

- Sicherheit**
 - Firewall
 - Virenschanner
 - Ports
 - Crypten
 - DOS Attacks
- Hackersoftware**
 - Toolz
 - Virengenerator
 - Trojaner
 - Iceqtoolz
 - Keygenerator
- Anonymität**
 - Proxies
 - Public Server
- Warez**
 - Appz
 - Cracks
 - Serials
 - Autokommandos
- Hackersoftware**
 - DOS Tools, Toolz, Virengenerator, Trojaner, ICQ-Toolz, Keygenerator, Nuketoolz, Mailbomber, HEX-Editor
- Sex**
 - Passwörter, Backdoors, Geld verdienen, Links, Sexseiten, Hacken, Kostenlose Sexseiten, HardCore, Private Girls
- Webseiten**
 - FTP Passwörter, CGI-Backdoors, PHP-Server übernehmen, Strategien, Passwort listen, Tutorials, Tools, Insider Tipps, Bilder
- Warez**
 - Esel, Appz, Downloads, Testberichte, Vorschau, Speedtools, Serials, Suchmaschinen, Tipps
- Multimedia**
 - DnK, Mp3, SVCD, Charts, Software, Movies, Brennen, Kopierschutz, Links
- Games**
 - Cheats, Cracks, Tipps, Brennen, Kopierschutz knacken, Tunen, Download, Classics, Konsolen
- Handy**
 - Bildmitteilungen, Klingeltöne, SMS Sprüche, ASCII Bilder, Handylogos, Codes, SMS Bomber, Charts, Secrets
- Tutorials**
 - Anonyme Emails Senden, Hacken, Cracken, Sniffing, BruteForce, Spoofing, Keylogger, Phreaking, Naker
- Sicherheit**
 - Firewalls, Virenschanner, Sicherheitsereinstellungen, DOS Attacks, TCP IP, Cookies, ActiveX, Ports, Crypten
- Trojanische Pferde**
 - Mit "Trojanischen Pferden" ist es für einen Hacker möglich, wie mit ihren Vorbildern aus der Geschichte unbemerkt in fremde Systeme
- Passwortknacker**
 - Mit dem richtigen Passwort gelangen Hacker auch an sensibelste Daten. Finden Sie mit diesem Programm heraus, wie sicher Ihre

The browser's taskbar at the bottom shows the Start button, several application icons, and the system tray with the date and time (09:43).

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 für Datenverlust 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.....

Jobsicherungsinteresse

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

(Lenin)

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

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>)

Todo-Liste Endkunde

- 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.

IT Security

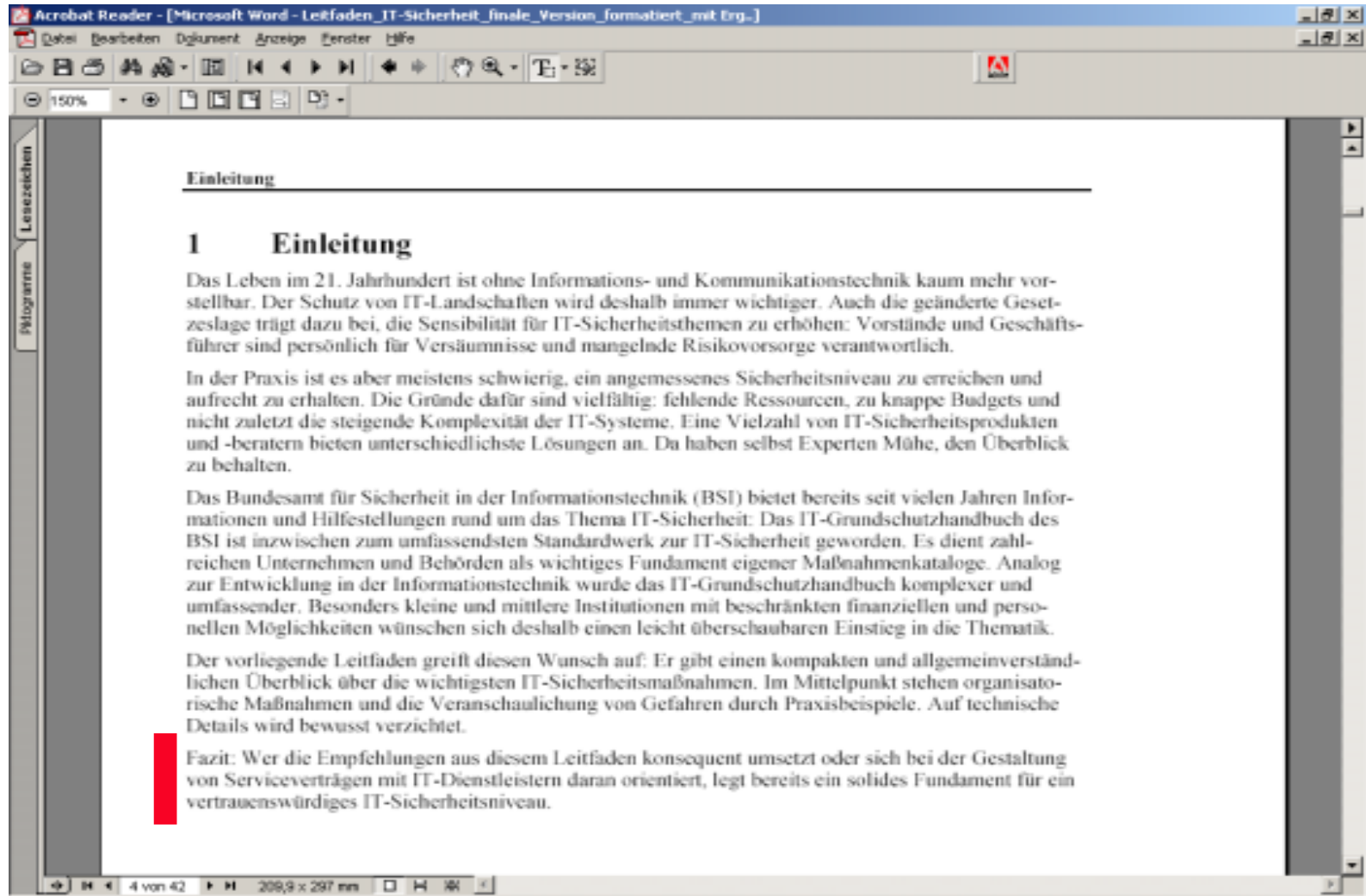
Zurück zu Ihnen...

Haftung des Resellers für nicht abgeschlossene Deals?

IT Security



IT Security



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

Übri Bearbeiten Dokument Anzeige Fenster Hilfe

150%

Leseseiten
Miniatur

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 Risikoversorge 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

Todo-Liste Reseller

- Interne Vorkehrungen treffen als IT **Security** Dienstleister
- Spezielle Kundenverträge vorbereiten (Haftung!)
- IT Security als „Rund um Sorglos“ Packet anbieten
- IT Security als Dauerdienstleistung verstehen
- Kundenbeziehung vom Push zum Pull drehen

Vielen Dank und guten Umsatz.

Kontakt

PRW Rechtsanwälte
RA Wilfried Reiners, MBA
Steinsdorfstr. 14
80538 München
Tel: +49-89-2109770
E-mail: office@prw.de
Internet: www.prw.info