

02
Anschrift

e-Networkers GmbH
Am Planetarium 8
D-07743 Jena

03
Kontakt

Tel. +49 (3641) 479560
Fax +49 (3641) 479341
info@e-networkers.de

04
Leistungen

Consulting
Systembetreuung
Systemsicherheit

05
Leistungen

Netzwerke
Analysen
Webanwendungen



IT SICHERHEIT IM KOMMUNIKATIONS- UND ZÄHLUNGSVERKEHR

BVMW-Unternehmertreff
am
29. August 2006 in Hermsdorf

HANS ELSTNER
GESCHÄFTSFÜHRER DER E-NETWORKERS GMBH



AGENDA

INHALT UND GLIEDERUNG

- | | |
|--|---|
| 1. EINFÜHRUNG
IT Sicherheit im Mittelstand | 3 |
| 2. HAFTBARKEIT
Haftung von Geschäftsführern und Vorständen | 4 |
| 3. IT GRUNDSCHUTZ
Wichtige Grundlagen für einen Mindestschutz | 5 |
| 4. E-MAIL VERSCHLÜSSELUNG
eine Notwendigkeit im Kommunikationsverkehr | 6 |
| 5. PHISHING
Risiken und Abwehrmaßnahmen | 7 |



EINFÜHRUNG IT SICHERHEIT IM MITTELSTAND

Die Informationstechnik ist aus dem heutigen Unternehmensalltag nicht mehr wegzudenken.

Sie ist zentrales Element vieler Unternehmensprozesse:

- Kommunikation
- Geschäftsanbahnung
- Vertragsabschluß
- Datenspeicherung
- Zahlungsverkehr
-

Der Schutz der IT ist deshalb ein entscheidender und existenzieller Faktor für das Unternehmen!

Dennoch wird die IT als Risikofaktor oftmals vernachlässigt und stiefmütterlich behandelt.

Fragen Sie sich selbst: „*Welche Maßnahmen haben wir ergriffen?*“

Weitverbreitete Fehleinschätzungen:

- "Bei uns ist noch nie etwas passiert."
- "Was soll bei uns schon zu holen sein, so geheim sind unsere Daten nicht."
- "Unser Netz ist sicher."
- "Unsere Mitarbeiter sind vertrauenswürdig."

Kostenfaktor:

IT-Sicherheitsmaßnahmen sind nicht zwangsläufig mit hohen Investitionen verbunden. Schon vergleichsweise geringe Investitionen können die IT Sicherheit erheblich erhöhen. Schulung der Mitarbeiter im Umgang mit dem System sind darüber hinaus äußerst sinnvoll und erweisen sich ebenfalls als essentielle und kosteneffiziente Vorkehrung.

Die Kosten beim Ausfall der IT sind oft um ein Vielfaches höher, als die für einen angemessenen Schutz der IT.

02
Anschrift

e-Networkers GmbH
Am Planetarium 8
D-07743 Jena

03
Kontakt

Tel. +49 (3641) 479560
Fax +49 (3641) 479341
info@e-networkers.de

04
Leistungen

Consulting
Systembetreuung
Systemsicherheit

05
Leistungen

Netzwerke
Analysen
Webanwendungen



HAFTBARKEIT

HAFTUNG VON GESCHÄFTSFÜHRERN UND VORSTÄNDEN

Pflicht eines jeden Geschäftsmannes ist es drohende wirtschaftliche Schäden abzuwenden. Der Ausfall der IT oder das abfließen von Informationen an Dritte kann enorme wirtschaftliche Schäden nach sich ziehen.

→ Damit wird IT-Sicherheitsmanagement zur Chefsache

Der Gesetzgeber hat dieser Tatsache Rechnung getragen. Verschiedene Gesetze und Regelungen belegen die persönliche Haftung von Geschäftsführern und Vorständen

Im Folgenden seien einige Beispiele genannt:

- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) [Artikelgesetz, ergänzt bzw. ändert verschiedene Gesetze]
- Im Aktiengesetz wird 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).
- Dem Geschäftsführern einer GmbH wird im GmbH-Gesetz „die Sorgfalt eines ordentlichen Geschäftsmannes“ auferlegt (§ 43 Abs. 1 GmbHG).
- Strafgesetzbuch (z.Bsp. §203StGB, Veröffentlichung vertraulicher Daten)
- Telekommunikationsgesetz, Gesetz zur Nutzung von Telediensten,...



IT GRUNDSCHUTZ

WICHTIGE GRUNDLAGEN FÜR EINEN MINDESTSCHUTZ

nur ein **kontinuierliches IT-Sicherheitsmanagement** kann den reibungslosen Unternehmensablauf gewährleisten.

Unabdingbar sind unter anderem

- ein durchdachter Serverstandort (Infrastruktur) und ausreichender Schutz der Hardware vor physikalischen Einflüssen (Feuer, Wasser, Vandalismus)
- eine regelmäßige Datensicherung, die Kontrolle der Backups und deren Auslagerung (Beispielsweise zum Geschäftsführer nachhause oder zu einem externen Dienstleister)
- Schutz vor Schadsoftware (Viren, Würmer, Spyware)
- Schutz vor unerlaubten Zugriffen (Firewall, durchdachte Rechtevergabe)
- Anlegen einer ausführlichen Dokumentation (System- und Netzwerkdaten, Zugangsdaten)

Nehmen Sie sich etwas Zeit und überlegen Sie besonnen ob Ihre IT wirklich ausreichend geschützt ist.

Stellen Sie Ihr Tagesgeschäft einen Augenblick hinten an.

Machen Sie sich klar welche Kosten und welche Haftungsfolgen im Falle eines Systemausfalls auf Ihr Unternehmen zu kommen.

Vertrauen Sie nicht blind Ihrem IT Systemhaus. Hinterfragen Sie kritisch ob alle wichtigen Vorkehrungen getroffen wurden.



E-MAIL VERSCHLÜSSELUNG

EINE NOTWENDIGKEIT IM KOMMUNIKATIONSVERKEHR

Für das Versenden von E-Mails wird üblicherweise das weit verbreitet SMTP Protokoll genutzt. Allerdings ist es veraltet und weist eine Reihe von Schwächen auf.

Besonders die folgenden Kriterien für eine verbindliche und verlässliche Kommunikation sind bei E-Mails nicht gegeben:

- Vertraulichkeit (*Inhalt einer Nachricht muss vor Dritten geheim bleiben*)
- Authentizität (*Urheber einer Nachricht muss zweifelsfrei feststellbar sein*)

E-Mail Verschlüsselung als Ausweg

- Vertraulichkeit (*E-Mail können nur noch vom adressierte Empfänger gelesen werden*)
- Authentizität (*E-Mails werden vom Absender signiert und sind so eindeutig dem Urheber zuzuordnen*)

Es empfiehlt sich die Verwendung der asymmetrischen Verschlüsselungs-software PGP (bis Version 6.5.8 kostenlos) oder GnuPG (kostenlos).

Die Software kann sowohl in vorhandene E-Mail Programme integriert, aber auch unabhängig von ihnen verwendet werden.

E-Mail Verschlüsselung per PGP (Pretty Good Privacy)

Es gibt ein eindeutig zugeordnetes Schlüsselpaar: Einen öffentlichen, mit dem jeder die Daten für den Empfänger verschlüsseln kann (*Schloss*), und einen geheimen privaten Schlüssel, den nur der Empfänger besitzt und der durch einen Kennwortsatz geschützt ist.

Verschlüsselte Nachrichten können nur vom Empfänger mit dem passenden privaten Schlüssel entschlüsselt werden.

Das Signieren, also eindeutige digitale Unterschriften von Nachrichten, ist hingegen nur mit privaten Schlüssel möglich. Die Nachricht wird dadurch eindeutig zuordenbar.

Anleitungen PGP und GnuPG

<http://kai.iks-jena.de/pgp/>

PGP Tray 6.5.8 und andere nützliche Software

<http://www.e-networkers.de/eNetworkers-jena-it-downloads.html>



PHISHING

RISIKEN UND ABWEHRMAßNAHMEN

Trend geht stark zum Online – Banking. Inzwischen ist jeder vierte Deutsche „Online-Banker“

Phishing nimmt immer stärker zu.

Schaden durch Phishing in Deutschland laut BKA: 4.500.000 €

Begriffsklärung Phishing

- Internetgestützte Form des Trickbetruges
- meist mittels gefälschter E-Mails (Spamartig versendet)
- Ziel: Vermögensvorteile zu erlangen
- dazu werden Zugangsdaten von Internetnutzern benötigt (z.Bsp. PIN / TAN)

Mittel zur Täuschung

- Fälschen der E-Mail Adresse
 - Absender der E-Mail fälscht seine E-Mail Adresse
 - wird ermöglicht durch fehlenden Identitätsschutz im SMTP Protokoll
- Vortäuschen der Echtheit mittels Darstellung
 - Inhaltlich überzeugende Darstellung
 - Graphisch dem Internetauftritt der Bank angepasst
- Täuschen mittels URL
 - Bspw. statt <http://www.volkbank.de> verwenden von <http://www.volksbank.de.url.ster.st>

→ Phishing ist gerade durch die Kombination von technischen und psychologischen Methoden erfolgreich.

02
Anschrift

e-Networkers GmbH
Am Planetarium 8
D-07743 Jena

03
Kontakt

Tel. +49 (3641) 479560
Fax +49 (3641) 479341
info@e-networkers.de

04
Leistungen

Consulting
Systembetreuung
Systemsicherheit

05
Leistungen

Netzwerke
Analysen
Webanwendungen



Risiken aus Kundensicht:

- Vermögensschaden
- Vertrauensverlust, pot. Abkehr vom Online – Banking
- Bei Abkehr vom Online – Banking höherer Aufwand

Risiken aus Bankensicht

- Imageschäden
- Abkehr der Kunden vom Online – Banking
- Zusätzliche Kosten durch Notwendigkeit neue Sicherheitssysteme

Abwehrmaßnahmen aus Sicht der Kunden

- Misstrauen gegenüber E-Mails von Banken
- Kontrolle der URL im Browser (Internet Explorer, Firefox) auf Richtigkeit
- Verwendung von Internetschutzsoftware (Firewall, Antivirensoftware, Antispyware)
- Ständige Aktualisierung des Computers und der Schutzsoftware

Abwehrmaßnahmen aus Sicht der Banken

- Öffentliche Aufklärung
- Kundenbetreuung
- Technische Maßnahmen

Technische Maßnahmen

- Transaktionsüberwachungssysteme (Kontenüberwachung)
- Verbesserte TAN Verfahren: iTAN, mTAN
- Kartenbasierte Verfahren - HBCI

02
Anschrift

e-Networkers GmbH
Am Planetarium 8
D-07743 Jena

03
Kontakt

Tel. +49 (3641) 479560
Fax +49 (3641) 479341
info@e-networkers.de

04
Leistungen

Consulting
Systembetreuung
Systemsicherheit

05
Leistungen

Netzwerke
Analysen
Webanwendungen



iTAN = indizierte Transaktionsnummer

Alle TANs sind fortlaufend nummeriert. Für eine Überweisung wird eine bestimmte TAN abgefragt.

Vorteile: *Einfaches und kostengünstiges Verfahren*
Nachteile: *kann durch Echtzeitangriffe überlistet werden
(Zum Beispiel durch Trojaner, Backdoors)*

mTAN = m(obile)TAN

TAN + Überweisungsdaten werden via SMS an Nutzer übermittelt.

Vorteile: *Das Verfahren ist einfach, relativ günstig und sicher vor Phishing.*
Nachteile: *Das Handy wird immer benötigt und es entstehen dem Kunden Kosten
(gering).*

HBCI - Kartenbasiertes Verfahren

Kartenlesegerät wird direkt am PC angeschlossen. Es werden keine TANs eingegeben. Die Buchung wird mittels Karte verifiziert.

Vorteile: *Bisher nicht überlistet → sehr sicher*
Nachteile: *Installationsaufwand
HBS und Kartenleser benötigt → schlecht portabel
Anschaffungs-+ laufende Kosten → nicht so kostengünstig
(dennoch lohnenswert)*

Fazit und Ausblick

Phishing wird zwar zunehmend professioneller, dennoch gibt es keinen Grund sich vom Onlinebanking abzuwenden.

Obgleich trotz aller Vorkehrung eine 100 % Sicherheit nicht möglich ist, kann durch die Wahl eines sichereren Verfahrens und unter gebotener Vorsicht, Onlinebanking durchaus sicher sein.