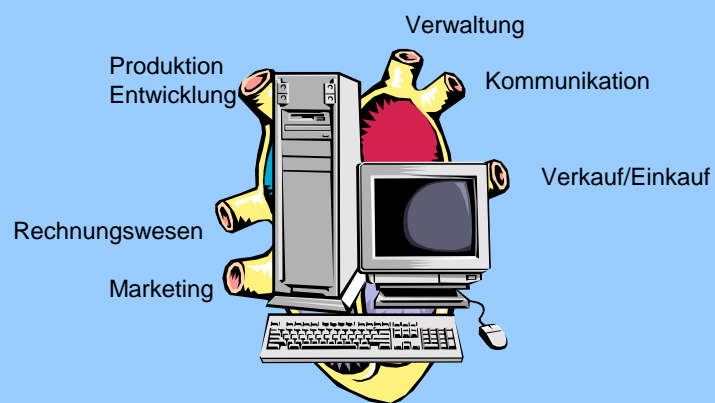


IT-Grundschutz im Unternehmen

Chefsache

IT-Grundschutz im Unternehmen

IT wird zunehmend das Herz des Unternehmens

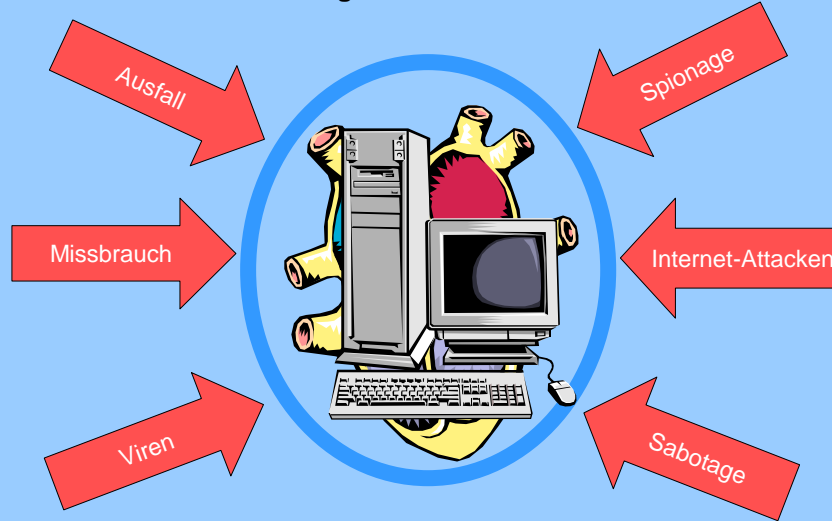


18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 2

Das Herz – beliebtes Angriffsziel



18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 3

Die drei Aspekte der IT-Sicherheit



1. Verfügbarkeit der Daten

2. Schutz der Vertraulichkeit von Daten

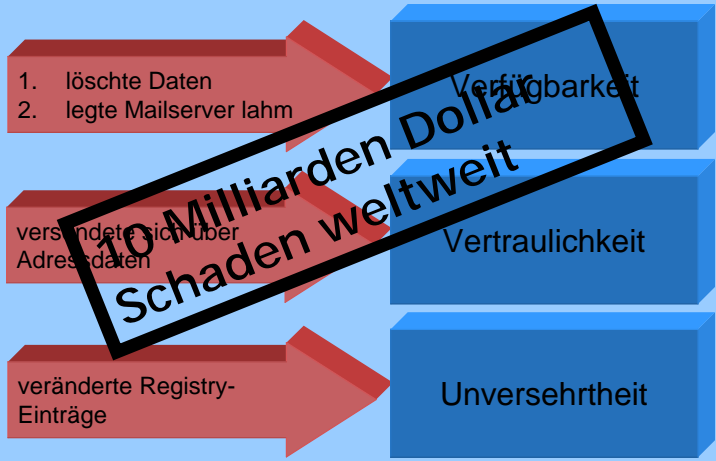
3. Unverletzlichkeit (Integrität) der Daten

18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 4

LoveLetter (4.Mai 2000)



10 Milliarden Dollar Schaden weltweit

- infizierte 45 Millionen PCs

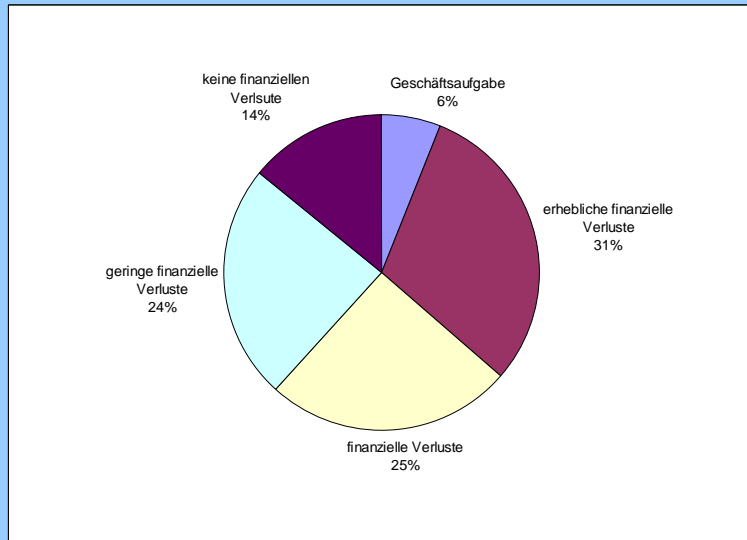
Ein Jahr später...

2001: 10 Milliarden EURO Schäden ALLEIN IN DEUTSCHLAND durch

- illegale Datenbeschaffung
- Datenmanipulation

(Quelle: Mummert + Partner)

Finanzieller Verluste durch Datenverlust



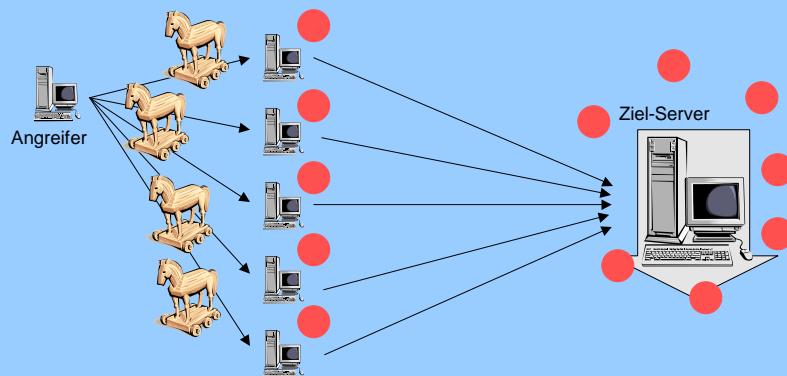
18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 7

Angriffe auf Server

August 2003 à Microsoft-Download-Server (LoveSAN)



Distributed Denial of Service-Attacke (DDoS)

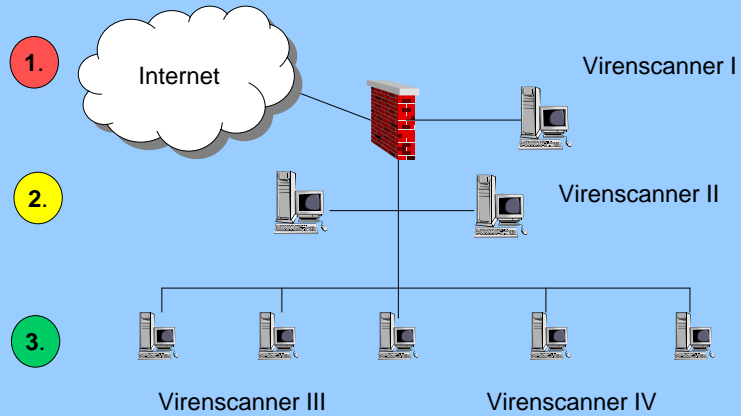
18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 8

Was tun gegen Viren?

Mehrstufiges Antiviren-Konzept



18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 9

Was tun Nutzer gegen Viren?

Sensibilisierung + Vorschriften



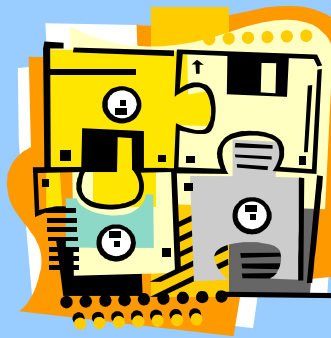
- Skepsis bei Mails unbekannter Herkunft (Anhang) → Löschen!
- Makroviren-Schutz aktivieren
- Sicherheit des Browsers auf höchste Stufe
- Passt Text zu Absender? (deutsch/englisch/I love you)
- keine Programme versenden/öffnen nach tel. Konsultation
- Hoaxes nicht weiterleiten (Merkmal: „Weitersenden...!“).

18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 10

Daten-Sicherung



Datensicherungs-Konzept

ABC
GmbH
Erfurt

- MA speichern auf Server (Netz-LW)
- Art der Datensicherung des Servers
- Häufigkeit + Zeitpunkt
- Anzahl der Generationen
- Vorgehensweise + Speichermedium
- Aufbewahrungsort
- Transport
- Sicherungsplan
- schriftl. dokumentieren (à Nachweis!)
- Kontrollen!
- Wiederherstellungsproben

Die drei Aspekte der IT-Sicherheit

P

1. Verfügbarkeit der Daten

2. Schutz der Vertraulichkeit von Daten

3. Unverletzlichkeit (Integrität) der Daten

Missbrauch - Industriespionage – Sabotage - Unfälle



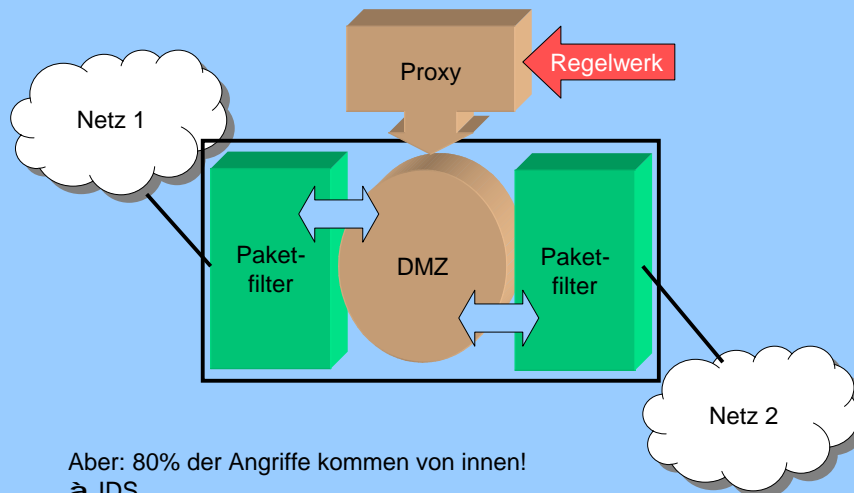
- Persönliche Daten → Profile, Handel
- Produktentwicklung
- Konkurrenz: Preise?
- offizieller CIA-Auftrag

18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 13

Was ist eine Firewall?



Aber: 80% der Angriffe kommen von innen!
→ IDS

18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 14

Öffentliche Briefe?

- statt Kuvert bei SMTP: **nichts!**
 1. → • keine Vertraulichkeit
 2. → • Manipulation möglich
- Nutzung im Geschäftsverkehr eingeschränkt
- mit IT: nicht nur mitlesen, auch Millionen auswerten (Stichwort-Suche, Datenbanken)



Verschlüsselung!

18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 15

Emails verschlüsseln

1. Nutzer erzeugt Schlüsselpaar: öffentlichen und privaten
2. A sendet B ihren *öffentlichen* Schlüssel



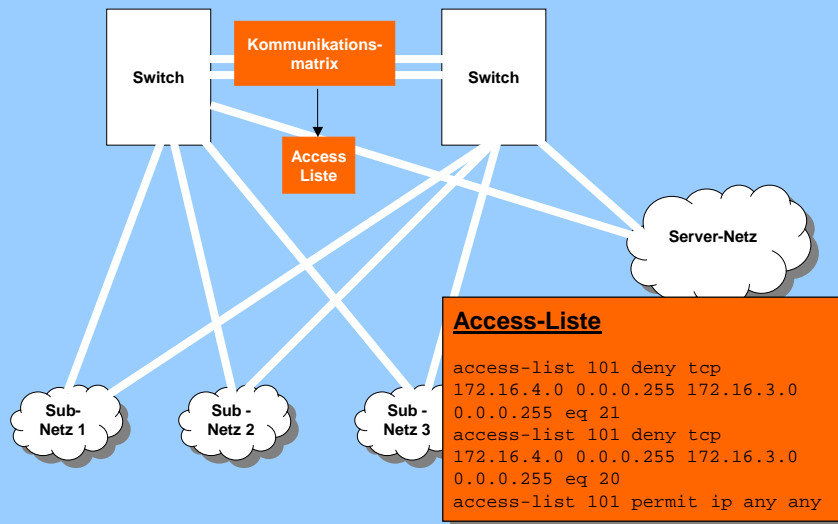
3. B verschlüsselt damit seine Email und sendet sie A
4. A entschlüsselt die Email mit ihrem *privaten* Schlüssel

18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 16

Kernnetz und Sub-Netze



18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 17

Hacking ohne Computer?

= Social Engineering à „Wetware“

- Konkurrenten im gleichen Marktsegment
- Überzeugungskraft - Täuschung - Druck
- à Sekretärinnen!
- „Dumpster Diving“: Untersuchen vom Müll
- Trick: Reportage über „große“ Firma
- Blaumann-Trick
- Telefon-Trick



Verantwortung jedes Einzelnen!

Sicherheit = Prozess!

18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 18

Die drei Aspekte der IT-Sicherheit

P

1. Verfügbarkeit der Daten

P

2. Schutz der Vertraulichkeit von Daten

3. Unverletzlichkeit (Integrität) der Daten

Wie schütze ich meinen PC?

- Passwort! à Satz „lbdMdi200EiMmvs“
- BIOS-Passwort
- Standard-Programme definieren
- keine eigenen Installationen erlauben
- Speziallösungen nur in Absprache mit IT
- keine Funktastaturen
- Schutz vor Manipulationen (z. B. Key Ghost)

Verpflichtungserklärung nach § 5 des Bundesdatenschutzgesetzes (BDSG) zur Wahrung des Datengeheimnisses

Angebildeter Name (Stempel)

Gemäß § 5 des Bundesdatenschutzgesetzes (BDSG) muss jedes Unternehmen alle Mitarbeiter, die personenbezogene Daten verarbeiten, zur Wahrung des Datengeheimnisses verpflichten.

Auf Grund des § 5 BDSG (siehe unten) ist Ihnen unter sagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen.

Ihre Verpflichtung bleibt auch im Falle einer Versetzung oder nach Beendigung des Arbeitsverhältnisses bestehen.

Verstöße gegen die Datenschutzrichtlinien können nach §§ 43 Absatz 2, 44 BDSG (siehe unten) und ggf. nach anderen Vorschriften bestraft werden. In der Tatbestandsfolge des Strafgesetzbuches können zugleich die Rückabwicklung sowie strafrechtliche Verpflichtung gegen die Gewerkschaften bis zur Endlösung entstanden werden.

Hiermit bestätige ich, über meine Verpflichtung zur Wahrung des Datengeheimnisses unterrichtet zu sein. Die Texte der §§ 5 BDSG, 43 Absatz 2 BDSG und 44 BDSG habe ich erhalten.

Vorname	Nachname	Geburtsdatum
Friedrich	Müller	12.03.1978

Was Unterzeichnung bescheinigt:

§ 5 BDSG
 Das mit der Datenverarbeitung beauftragte Personal ist zu jeder Zeit personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Unternehmensdaten, Daten Dritter und sonstigen Daten).
 Die Mitarbeiter sind verpflichtet, die Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen zu verhindern. Die Mitarbeiter sind verpflichtet, die Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen zu verhindern.

§ 43 Absatz 2 BDSG
 Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig:
 1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet;
 2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, weitergibt oder

§ 44 BDSG
 1. Die Verletzung von datenschutzrechtlichen Vorschriften durch einen Mitarbeiter ist strafbar, wenn die Verletzung zu einem Schaden führt, der die Interessen der betroffenen Person erheblich beeinträchtigt.
 2. Die Verletzung von datenschutzrechtlichen Vorschriften durch einen Mitarbeiter ist strafbar, wenn die Verletzung zu einem Schaden führt, der die Interessen der betroffenen Person erheblich beeinträchtigt.

§ 19 Abs. 2 Satz 1 bis 3 BDSG
 1. Die Verletzung von datenschutzrechtlichen Vorschriften durch einen Mitarbeiter ist strafbar, wenn die Verletzung zu einem Schaden führt, der die Interessen der betroffenen Person erheblich beeinträchtigt.
 2. Die Verletzung von datenschutzrechtlichen Vorschriften durch einen Mitarbeiter ist strafbar, wenn die Verletzung zu einem Schaden führt, der die Interessen der betroffenen Person erheblich beeinträchtigt.

18.09.2003

Fuchs, Jenoptik

Bild 21

Belehrungen

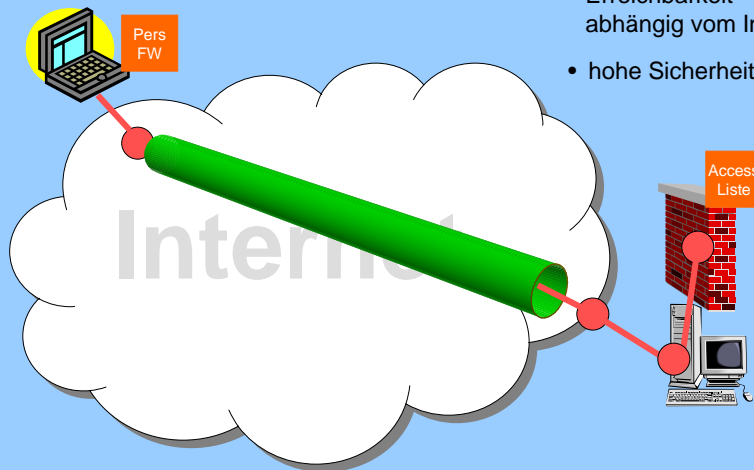
- §§ 43, 44 Bundesdatenschutzgesetz (BDSG)
- § 43 Thüringer Datenschutzgesetz – Verstöße gegen den Datenschutz
- StGB
- § 86 – Verbreitung von Propagandamitteln verfassungsfeindlicher Organisationen
- § 95 – Offenbaren von Staatsgeheimnissen
- § 184 – Verbreitung pornographischer Schriften
- § 202a – Ausspähen von Daten
- § 203 – Verletzung von Privatgeheimnissen
- § 263a – Computerbetrug
- § 266b – Missbrauch von Scheck- und Kreditkarten
- § 268 – Fälschung technischer Aufzeichnungen
- § 269 – Fälschung beweiserheblicher Daten
- § 270 – Täuschung im Rechtsverkehr bei Datenverarbeitung
- § 303a – Datenveränderung
- § 303b – Computersabotage
- § 94 TKG – Unerlaubter Betrieb/Besitz von Sendeanlagen
- § 95 TKG – Unberechtigtes Abhören von Nachrichten
- §§ 106 – 111 Urhebergesetz (verschiedene Verstöße gegen Urheberrecht).

18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 22

Wenn Fernzugriff, dann VPN



- Tunnel im Internet (VPN)
- Erreichbarkeit abhängig vom Internet
- hohe Sicherheit

18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 23

Die drei Aspekte der IT-Sicherheit

- P** 1. Verfügbarkeit der Daten
- P** 2. Schutz der Vertraulichkeit von Daten
- P** 3. Unverletzlichkeit (Integrität) der Daten

PRAXIS-TIPPS

18.09.2003

Dr. W. Fuchs, Jenoptik

Bild 24

Projekt IT-Sicherheit

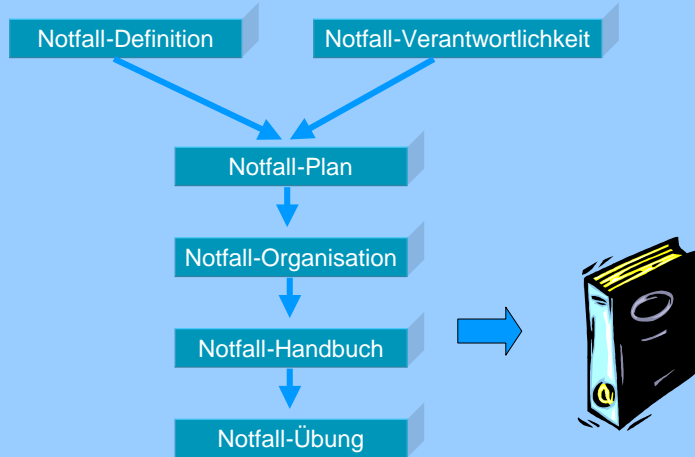
- 1 Leitlinien für IT-Sicherheit
- ↓
- 2 Notfall-Vorsorge
- ↓
- 3 Festlegungen
- ↓
- 4 Vermittlung zum Nutzer

Wo anfangen?

IT-Grundschutz-Handbuch – Leitlinie



Notfall vorbeugen!



Wie sag ich's meinem Nutzer?

Merkmale von Merkblättern:

- 1. Sie sind für Mitarbeiter, die kein IT-Verständnis haben, leicht verständlich.
- 2. Sie sind für alle Mitarbeiter, die mit dem IT-System arbeiten, verfügbar.
- 3. Sie sind für alle Mitarbeiter, die mit dem IT-System arbeiten, leicht verständlich.

Merkmale von Merkblättern:

- 1. Sie sind für Mitarbeiter, die kein IT-Verständnis haben, leicht verständlich.
- 2. Sie sind für alle Mitarbeiter, die mit dem IT-System arbeiten, verfügbar.
- 3. Sie sind für alle Mitarbeiter, die mit dem IT-System arbeiten, leicht verständlich.

- Merkmale**
- Praxis-bezogen
 - kurz
 - verständlich

