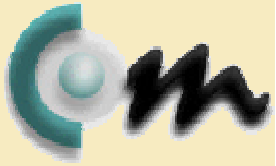
Internet – Gefahren und ihre Beherrschbarkeit

Hermann Gottschalk
Thomas Birnthaler

Firmenprofil OSTC GmbH



- OSTC = Open Source Training and Consulting: www.ostc.de
- 2 Mitarbeiter mit langjähriger IT-Erfahrung
  - **Thomas Birnthaler**, Dipl.-Informatiker, eMail: tb@ostc.de
  - **Hermann Gottschalk**, Dipl.-Physiker, eMail: hg@ostc.de
  - SCLT (SuSE Certified Linux Trainer)
- Portfolio
  - IT-Training (UNIX / Linux, Netzwerk, SW-Entwicklung)
  - IT-Sicherheits-Lösungen auf UNIX/Linux-Basis
  - IT-Consulting (Security und Open Source)
- Partnerschaften
  - SuSE Business Partner
  - GeNUA Vertriebspartner

Vortragsthemen

- Sicherheit als Management-Aufgabe!
- Wie funktioniert das Internet eigentlich?
- Welche Risiken birgt das Internet?
- Wie kann ihnen begegnet werden?
- Was für Produkte gibt es?
- Was bringt die Zukunft?
- Was ist zu tun?

Ziel des Vortrags:
Sensibilisieren + Motivieren

Inhaltsverzeichnis

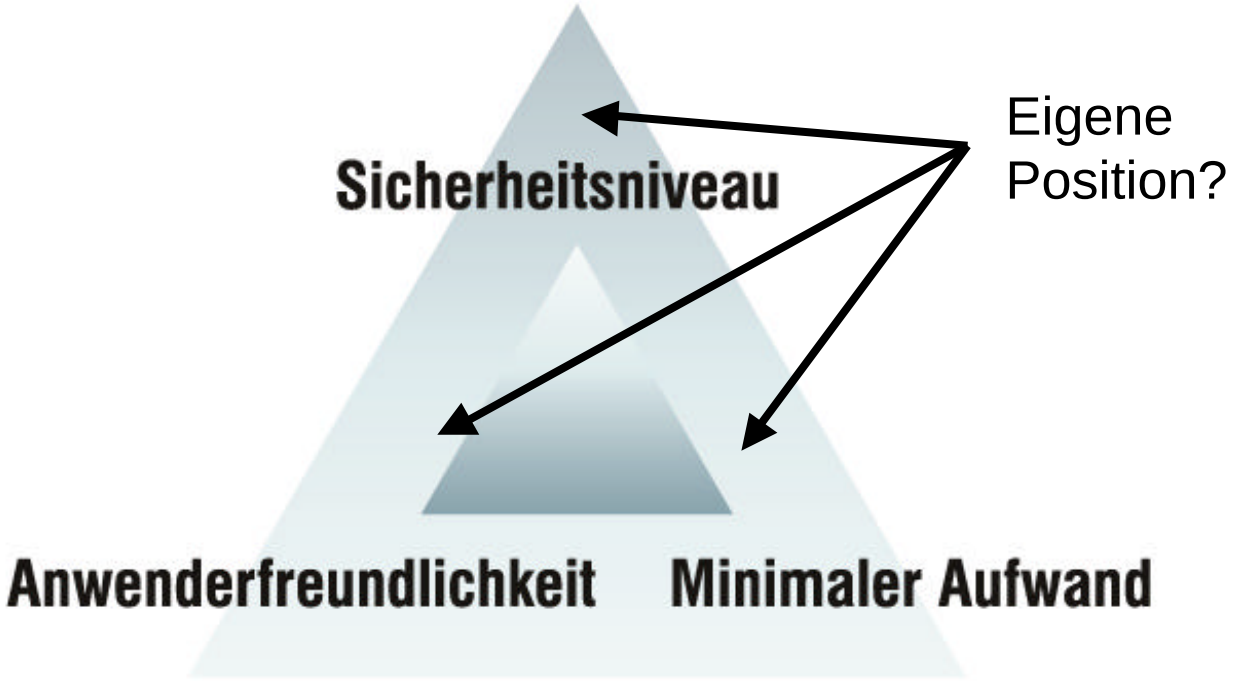
1 Sicherheit als Management-Aufgabe

- **Bewußtsein** notwendig
- Management trägt Gesamtverantwortung
  - Definieren der eigenen Sicherheits-Politik
    → "**Security Policy**"
  - Ableiten eines Sicherheits-Konzepts
  - Delegieren der (technischen) Umsetzung
  - Anpassen der Sicherheits-Politik an
    - Technische Entwicklung
    - Unternehmens-Entwicklung
- **Vorbildfunktion** (extrem wichtig!)
  - Sicherheit ist immer unbequem!

1 Sicherheit als Management-Aufgabe

- **Sicherheits-Politik ausarbeiten**
  - Schützenswerte "Güter" bestimmen
  - Gefahrenquellen analysieren
  - Schwachstellen analysieren (Ist-Zustand)
  - Risiko analysieren (Σ Schadens-Wahrscheinlichkeit $\times$ Kosten)
  - Eigene Position festlegen (Soll-Zustand)

Beziehungs-Dreieck



1 Sicherheit als Management-Aufgabe

- **Sicherheits-Konzept festlegen**
  - Physikalische Zugangsbereiche
  - Benutzergruppen / Gruppenrichtlinien
  - Virenscanner-Einsatz
  - Firewall-Einsatz
  - Getrennte Netzwerke
  - …
- **Umsetzung einleiten**
  - Verantwortliche festlegen
  - Kompetenzen definieren
  - Budget bereitstellen

1 Sicherheit als Management-Aufgabe

- **Sicherheits-Beauftragter aus dem Management**
  - Sensibilisieren
  - Sicherheitsziele vermitteln
  - Schulungen organisieren

  } → Mitarbeiter
  - Permanente Kontrolle der Umsetzung
  - Anpassung des Sicherheits-Konzepts
  - Notfall-Planung

- **Psychologische** und **organisatorische Aspekte** spielen eine sehr große Rolle
  - **Ziel**: Alle machen mit, weil sie den Sinn der Maßnahmen einsehen!

1 Sicherheit als Management-Aufgabe

Ebenen der Sicherheits-Politik

- **Management-Ebene**
  - Festlegen
  - Fortschreiben
- **Abteilungs-Ebene**
  - Details planen
  - Konkrete Maßnahmen ableiten
  - Umsetzen
  - Kontrollieren
- **Mitarbeiter-Ebene**
  - Richtlinien kennen
  - Nutzen und Bedeutung kennen
  - Anwenden ("Leben") der Maßnahmen

1 Sicherheit als Management-Aufgabe

- **Problematisches Mitarbeiter-Verhalten**
  - Unbeabsichtigt laufende ungewartete Server ("SQL-Slammer")
  - Ungeprüfte Disketten / CD-ROMs / DVDs ("Spiele")
  - Dokument-Austausch im MS-Datenformat ("aktive Inhalte")
  - USB-Sticks, portable Festplatten, Digital-Kameras, PDAs
  - Verwendung von Arbeitsplatz-Modems / ISDN-Karten
  - Nutzung von Web-Freemail-Accounts

- **Verteilung der Angriffe (Quelle: www.bsi.de)**

Aus dem Internet	48%
Über Wählverbindungen	7%
Von Innen	45%

1 Sicherheit als Management-Aufgabe

Schadensgründe

Kategorie	Reduzierbar durch
Unkenntnis	Schulung + Sicherheits-Konzept
Irrtum	Schulung + Sicherheits-Konzept
Nachlässigkeit	Schulung + Sicherheits-Konzept
Absicht	Sicherheits-Konzept

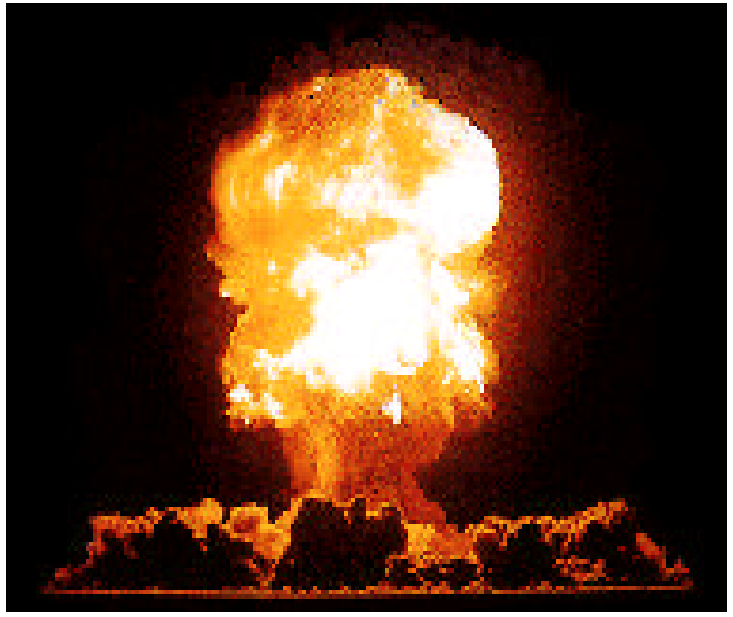
Analogie zur Datensicherung

Je länger nichts passiert,

desto leichtsinniger wird man

und

desto schlimmer kann es einen treffen.



Inhaltsverzeichnis

2.1 Internet-Anbindung – Motivation

Kaum ein Medium bietet so viele Chancen wie das Internet

- Selbstdarstellung
- Unerschöpfliches Potenzial
  - an Kommunikationsmöglichkeiten (Datenaustausch)
  - zum Knüpfen von Kontakten
  - zum Gewinnen und Verbreiten von Informationen

→ Das Internet ist heutzutage einfach **notwendig**!

2.1 Internet-Anbindung – Risiken

- **Vorsicht ist berechtigt**
  - Öffnung des internen Netzwerks
  - Risiken für **Daten**
    - Unbefugter Zugriff (Spionage)
    - Manipulation
    - Vernichtung
  - Risiken für **Systeme**
    - Missbrauch für andere Zwecke
    - Verlangsamung
    - Blockade
    - Ausfall

2.2 Internet ist mehr als WWW

- **Server bieten Dienste an**
  - Rechner ↔ Host-Name ↔ IP-Adresse
    (z.B. http://www.spiegel.de = 195.71.11.67)
  - Server und Clients kommunizieren über Router
- **Was ist ein Dienst überhaupt?**
  - Ein Stück Software
  - Spricht spezifisches Protokoll
  - Hat festen Port (z.B. Web-Server = http = 80)
  - Wartet auf Anfrage vom Client
- **TCP/IP-Protokoll**
  - Pakete
  - IP = Vermittlung und Wegewahl ("Routing")
  - TCP = Sichere Verbindung

2.2 Internet ist mehr als WWW

Dienst	Protokoll	Port
WWW	http, https	80, 443
Mail	smtp, pop, imap	25, 110, 143
Filetransfer	ftp	20/21
Remote-Login	ssh, telnet	22, 23
Namensauflösung (DNS)	domain	53
Windows Server Message Block	netbios, smb	137, 138, 139

Inhaltsverzeichnis

3.1 Gefahren aus dem Internet

Sobald ein Rechner über das Internet
erreichbar ist, können seine Dienste
für andere Zwecke **missbraucht** werden!

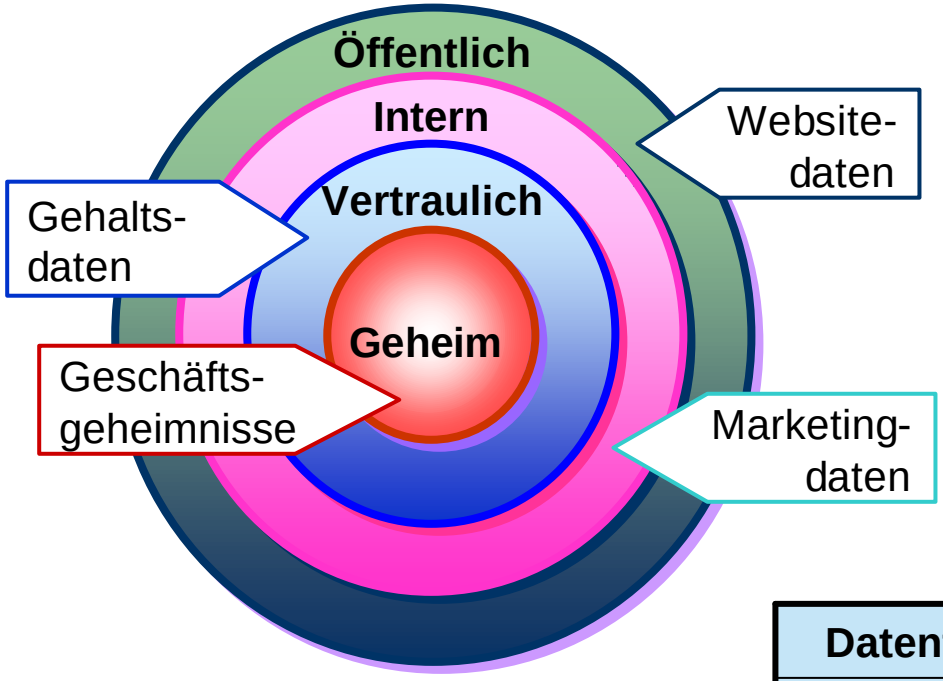
Ursache: Die eingesetzte Software (Betriebssystem, Grafikoberfläche, Browser, Server, …) hat **Entwurfs- oder Implementierungs-Fehler**, die für unvorhergesehene Zwecke ausgenützt werden können.

3.2 Was ist Gefährdet ?

- **Risiken für Daten** (Lokal / Netzwerk)
  - Unbefugter Zugriff (Spionage)
  - Manipulation
  - Vernichtung

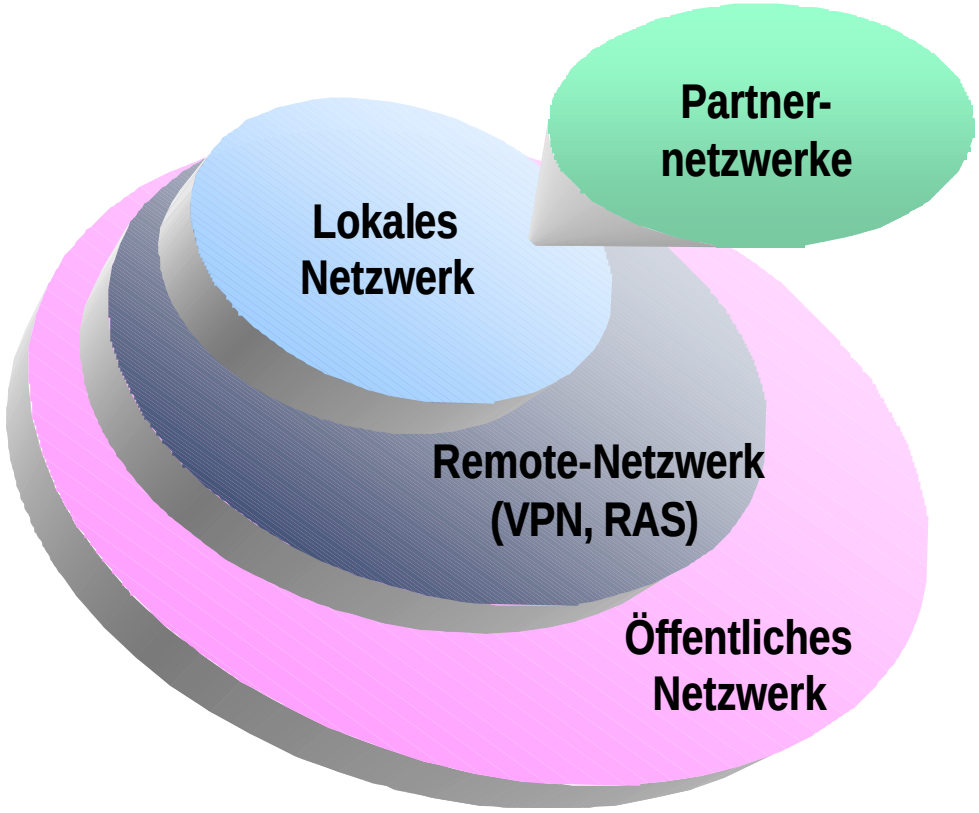
- **Risiken für Systeme** (Clients, File-, Druck-, Mail-, Web-, Datenbank-Server, Transaktions-Monitor, ...)
  - Missbrauch für andere Zwecke
  - Verlangsamung
  - Blockade des Zugriffs
  - Ausfall

3.2 Gefahren für Daten



Datentypen	Was ist gefährdet
Öffentlich	Prestige, Vertrauen, Umsatz
Intern	Abläufe, Arbeitszeit
Vertraulich	Abläufe, Internes Vertrauen
Geheim	Geistiges Eigentum

3.3 Wo lauern Gefahren ?



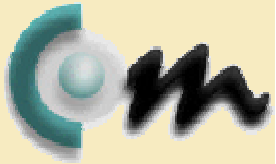
3.4 Von wem gehen Gefahren aus ?

- Admins / Rechteträger
- Mitarbeiter
- (Geschäfts)Partner
- Außenstehende
  - Provider
  - Konkurrenten
  - Hacker, Cracker, Skript-Kiddies
  - Anonyme Massenattacken

3.4 Motivation von Hackern / Crackern

- Weil‘s so einfach ist ("offene" Rechner, Tools, RootKits)
- Spiel / Spaß
- Ruhm
- Macht
- Wettbewerb
- Neugier
- Geld
- Politik / Weltanschauung
- Informationsvorsprung
- Rache (z.B. ehemalige Mitarbeiter)
- Konkurrenz
- …

3.5 Angriffsmethoden



Mit Erklärung

- Malicious Code (Viren / Würmer / Trojaner)
- Port Scanning
- (Distributed) Denial of Service Attack
- Password Cracking
- Network Monitoring
- IP-Address Spoofing
- Man in the middle
- Social Engineering

Ohne Erklärung

- Application Layer Attack
- RootKits / Backdoor
- DNS Poisoning
- E-mail Spoofing
- Session Hijacking
- Replay Attack
- Buffer Overflow (Stack)
- CGI Attack
- Cookie Exploitation

Diese Liste ist bei weitem nicht vollständig und jeden Tag werden neue Angriffsmethoden entdeckt!

3.5 Angriffsmethoden

Einschleusen von **Malicious Code** über Mail-Anhänge (Attachments) oder HTTP / FTP-Downloads

- **Virus**
  Software, die sich zu ihrer Verbreitung an ein anderes Programm hängt
- **Wurm**
  Programme, die sich selbständig ausbreiten und Computer vollautomatisch verseuchen
- **Trojaner**
  Harmlos erscheinende Programme, die beim Aufruf zusätzlich eine Schadensroutine abarbeiten

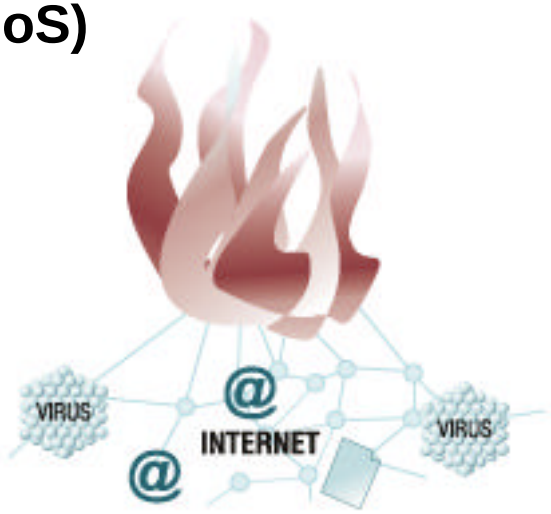
Schäden durch Computer-Viren / Würmer

Virus / Wurm	Geschätzter Schaden [Mrd. USD]
Code Red (2002)	2,62
SirCam (2002)	1,15
Nimda (2002)	0,64
I Love You (2000)	8,75
Melissa (1999)	1,10
Explorer (1999)	1,02

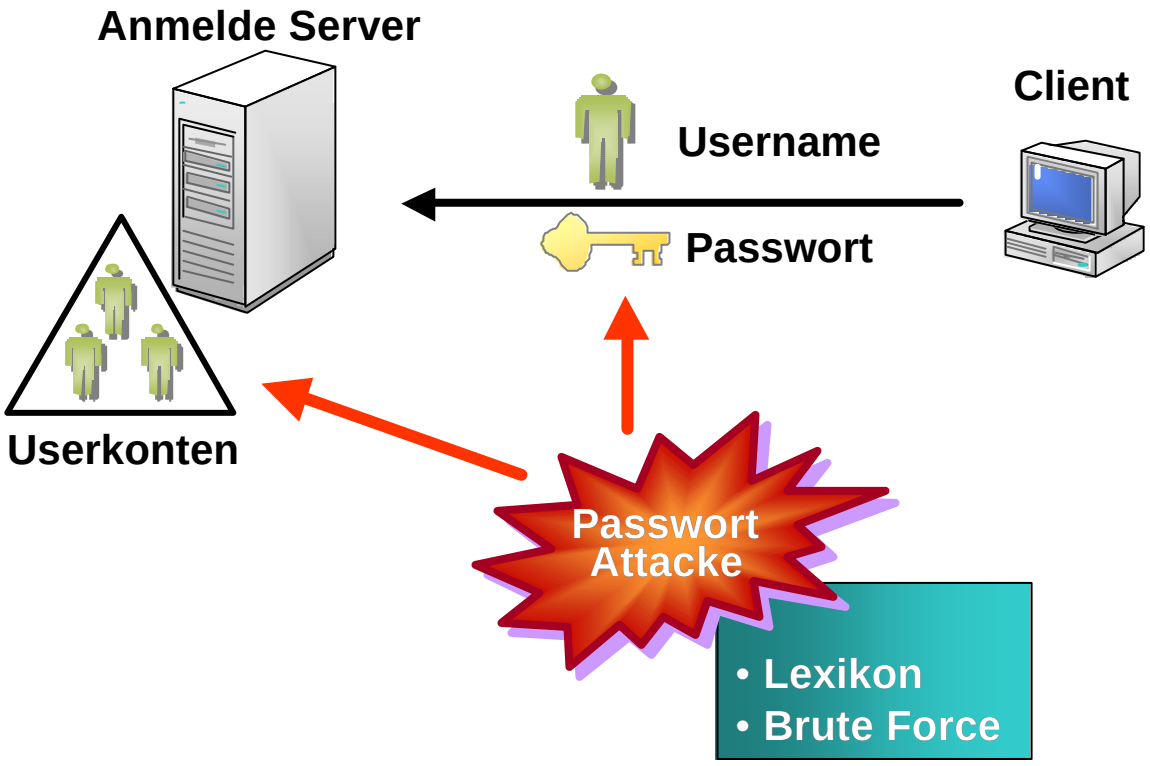
Quelle: www.computereconomics.com

3.5 Angriffsmethoden

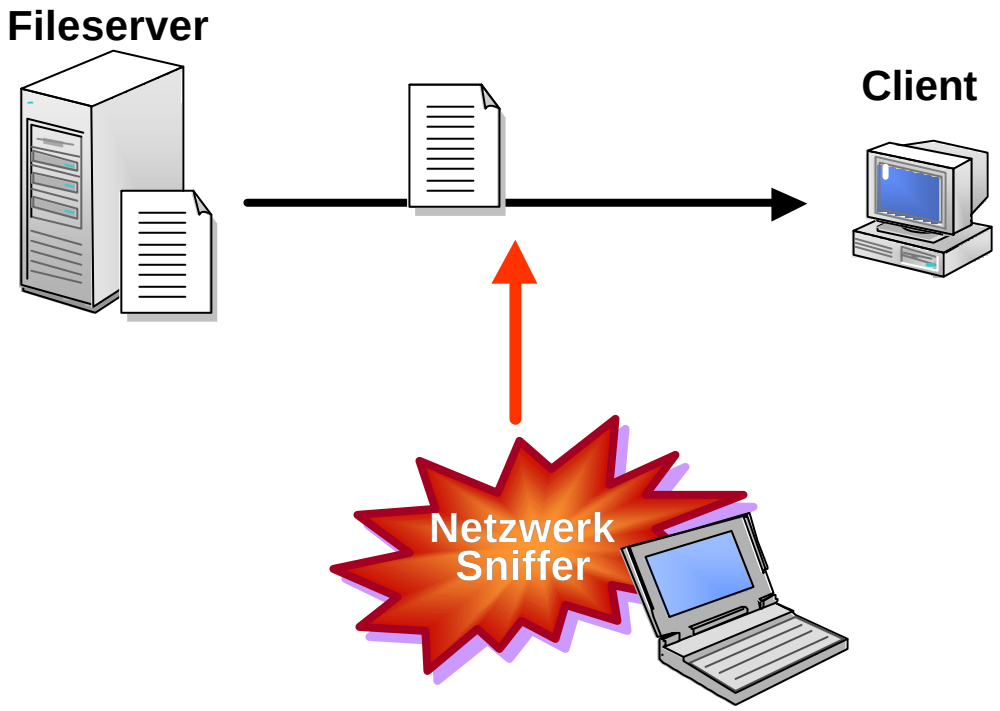
- **Port-Scanning**
  Liefern Informationen über
  fremde Netze und ihre Dienste
- **Denial-of-Service Attack (DoS)**
  Absichtliches Überfluten
  eines Rechners mit Anfragen
- **Distributed Denial-of-Service Attack (DDoS)**
  DoS zentral gesteuert über viele mit
  Würmern verseuchte Rechner
  - Nur schwer zurückverfolgbar
  - Rechner-Besitzer ahnungslos



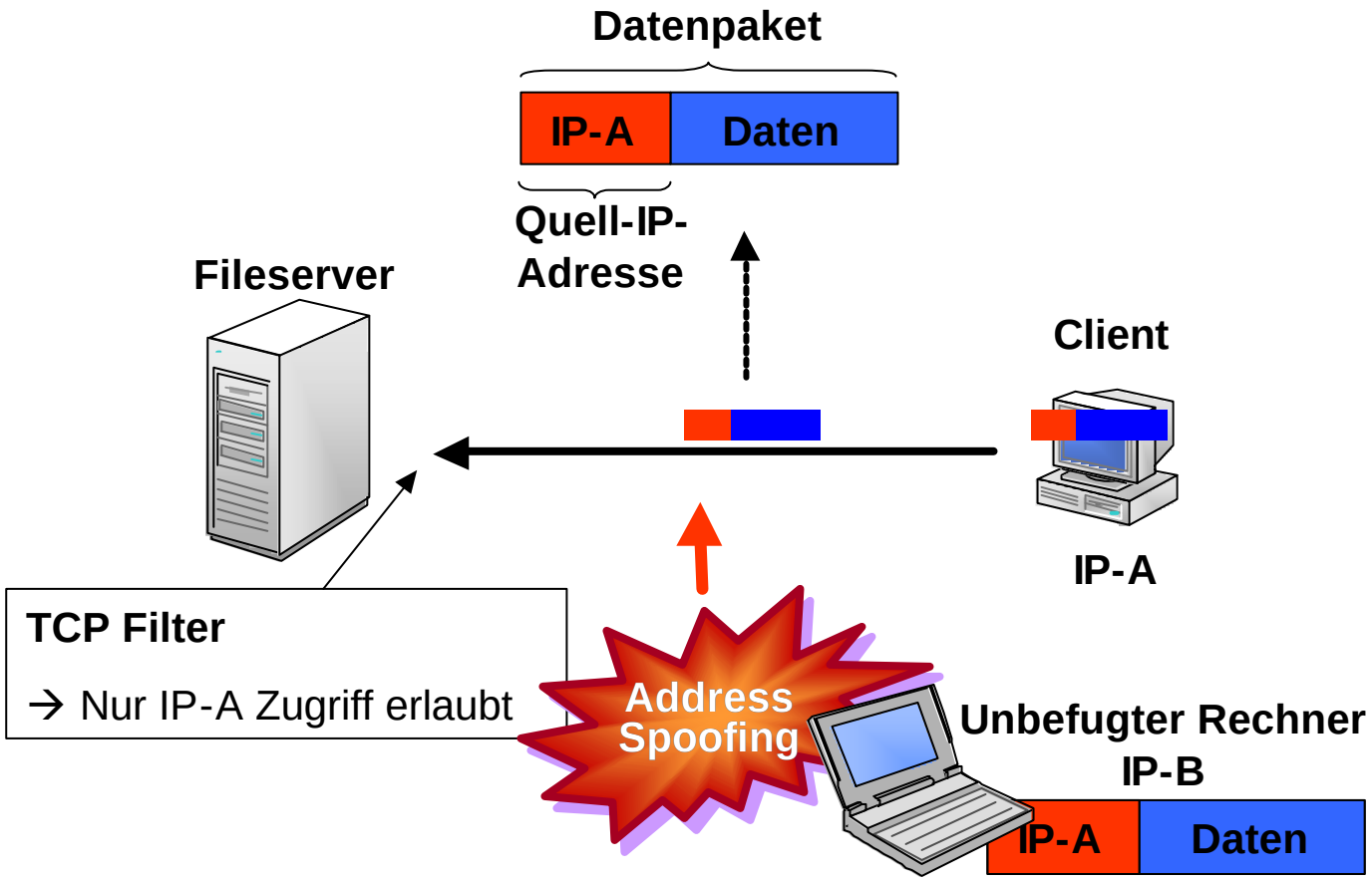
3.5 Passwort Attacke



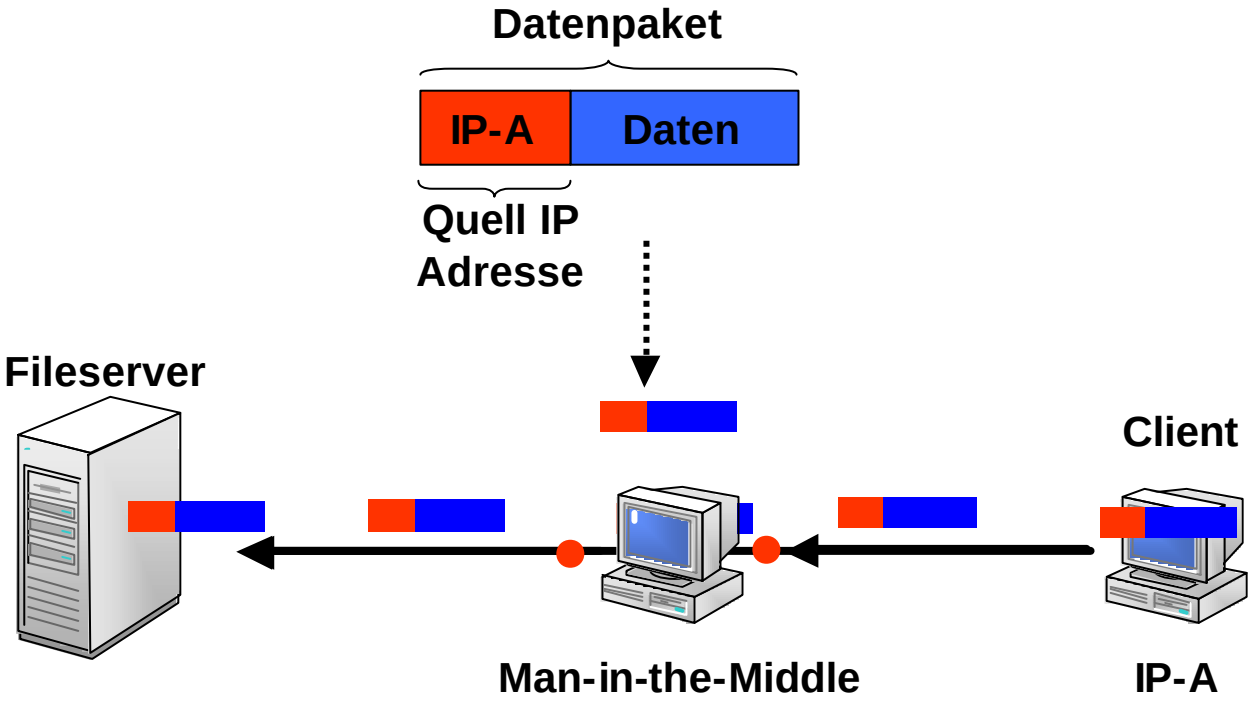
3.5 Netzwerk Monitoring



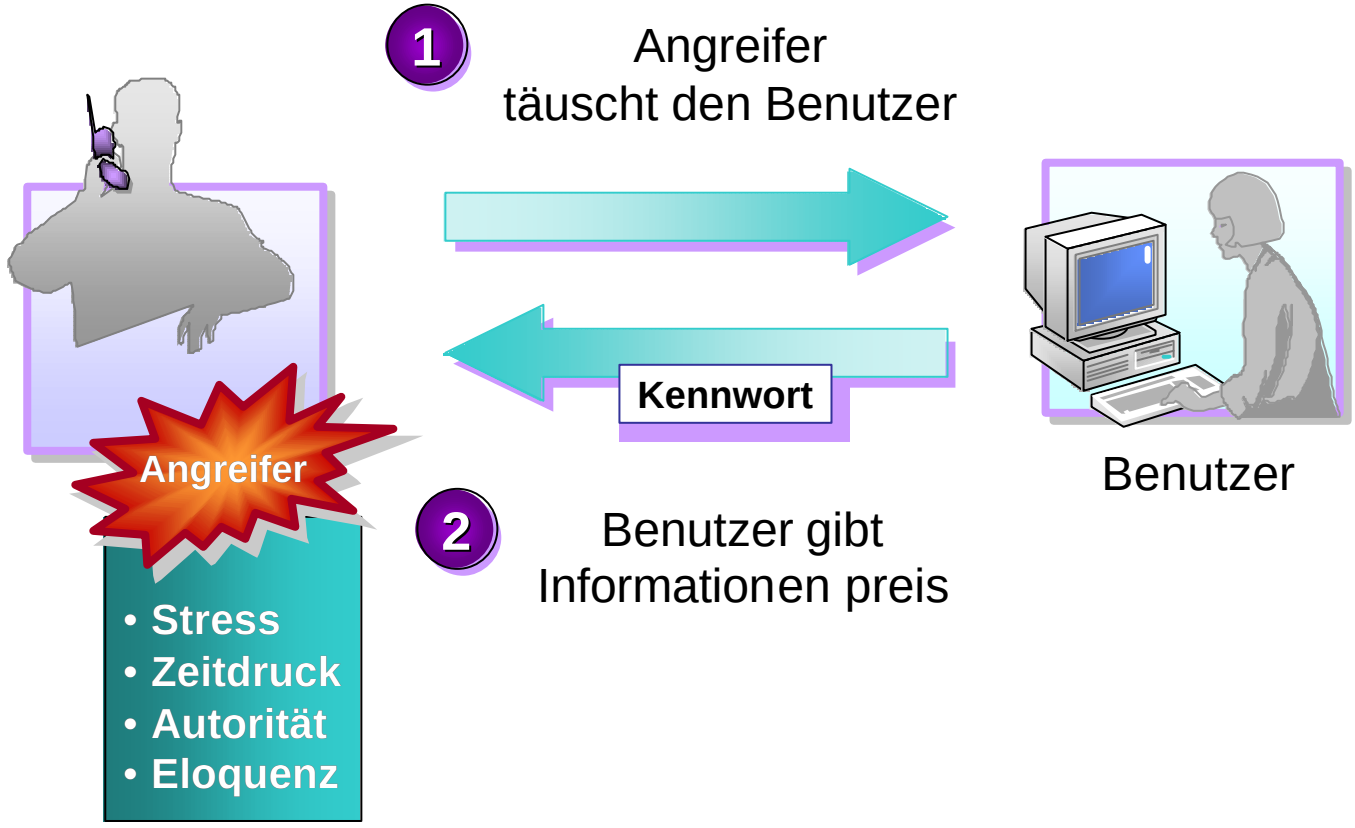
3.5 IP-Address Spoofing



3.5 Man in the Middle



3.5 Social Engineering

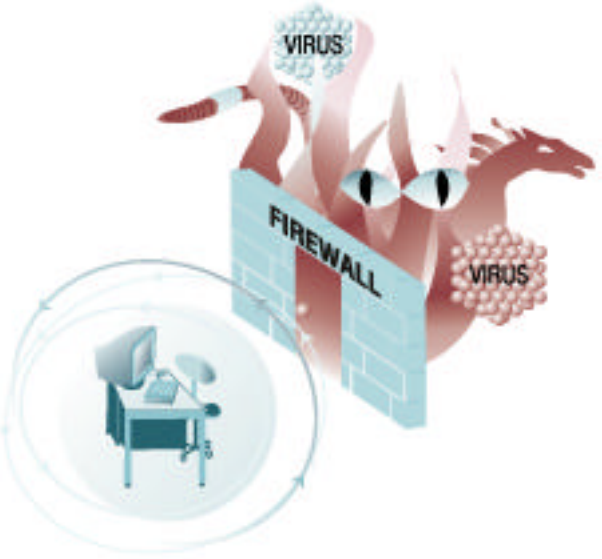


Inhaltsverzeichnis

4.1 Technische Sicherheitsmaßnahmen

Firewall

- Trennt 2 Netze mit **unterschiedlichem Schutzbedarf**
  - Kontrolliert **Datenaustausch** zwischen ihnen
  - **Meist**: Schützt Intranet vor unbefugten Zugriffen aus dem Internet
- "**Infrastruktur**" aus drei Bausteinen:
  - Paketfilter (häufig als "Firewall" bezeichnet)
  - Malicious Code Scanner (häufig als "Virenscanner" bezeichnet)
  - Proxy-Server (Circuit- und Application Gateways)



4.1 Technische Sicherheitsmaßnahmen

Paketfilter

- Arbeitet rein auf der Basis einzelner "Datenpakete"
- Enthält **Regel-Liste** der Form: **Kriterium** ® **Aktion**
  - **Aktion** pro ein- / ausgehendes Datenpaket
    - – Durchlassen (ACCEPT)
    - – Zurückweisen (REJECT)
    - – Verwerfen (DROP)

  - **Kriterien**
    - – IP-Adresse (= Client / Server)
    - – Port-Nummer (= Dienst)
    - – Verbindungs-Status (Stateful-Inspection)
- Hat **Default**-"**Policy**"
  - **Gut**: Nichts erlauben + Liste positiver Fälle → **unbequem**
  - **Schlecht**: Alles erlauben + Liste negativer Fälle → **bequem**

4.1 Technische Sicherheitsmaßnahmen

Paketfilter

- Vorteil
  - Performant
  - Geringer Hardware-Bedarf
- Nachteil
  - Kein Zugriff auf Anwendungsdaten
  - Erkennt Angriffe auf Anwendungsebene nicht (kann z.B. keine Viren herausfiltern)
- Sinnvolle Realisierung
  - Möglichst "abgespecktes" **Minimalsystem**
  - Konfiguration Read-Only (CD / Diskette)
  - Keine Fernwartung

4.1 Technische Sicherheitsmaßnahmen

Malicious Code Scanner (Virenscanner)

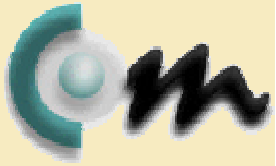
- Überprüft vorhandene, eingehende und ausgehende Daten kontinuierlich anhand
  - Tabellen auf bekannte Viren
  - Heuristischer Verfahren auf unbekannte Viren
- Liste bekannter Viren-Muster muss regelmäßig aktualisiert werden
- Auf allen Rechnern zu installieren
  - Server (File, Print, …)
  - Proxies (Mail, Web, ...)
  - Clients
- Kostet Performance (z.B. Archive)

4.1 Technische Sicherheitsmaßnahmen

Proxy Server (Circuit / Application Gateway)

- Gewollter "man-in-the-middle"
- Vertritt Client / Server beim Verbindungs-Auf / Abbau
- Alle Verbindungsdaten passieren den Proxy-Server
- Vorteile
  - Hält Angriffe auf IP-Ebene ab
  - Verbirgt eigene Netzwerk-Struktur (Clients / Server)
  - Authentifizieren von Benutzern / Rechnern möglich
  - Regelt den Zugang benutzerbezogen
  - Protokolliert die Zugriffe

4.1 Technische Sicherheitsmaßnahmen



- Zusätzliche Vorteile von **Application Gateways**
  - Anwendungsbezogene Datenüberprüfung
  - Content Filtering (z.B. "WebWasher")
  - Caching (zwischenspeichern)
  - Transportierte Daten protokollieren

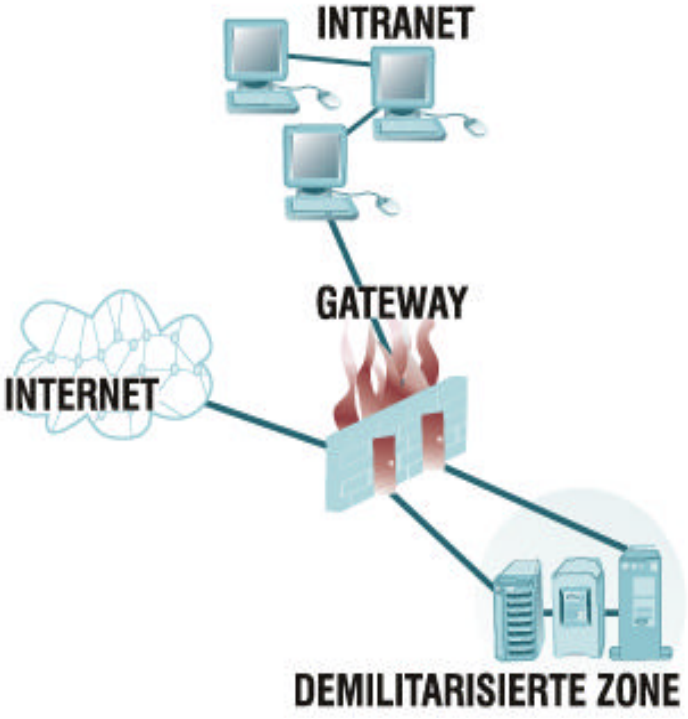
- **Nachteile beider Typen von Proxy Servern**
  - Konfigurations- und Wartungsaufwand
  - Performance-Verlust
  - End-zu-End Verbindung ausgehebelt!

4.1 Technische Sicherheitsmaßnahmen

Firewall-Ausprägungen

- **1 Rechner**
  Alles auf einem Rechner
  (typischer Personal Firewall,
  ohne Abbildung da unsinnig!)

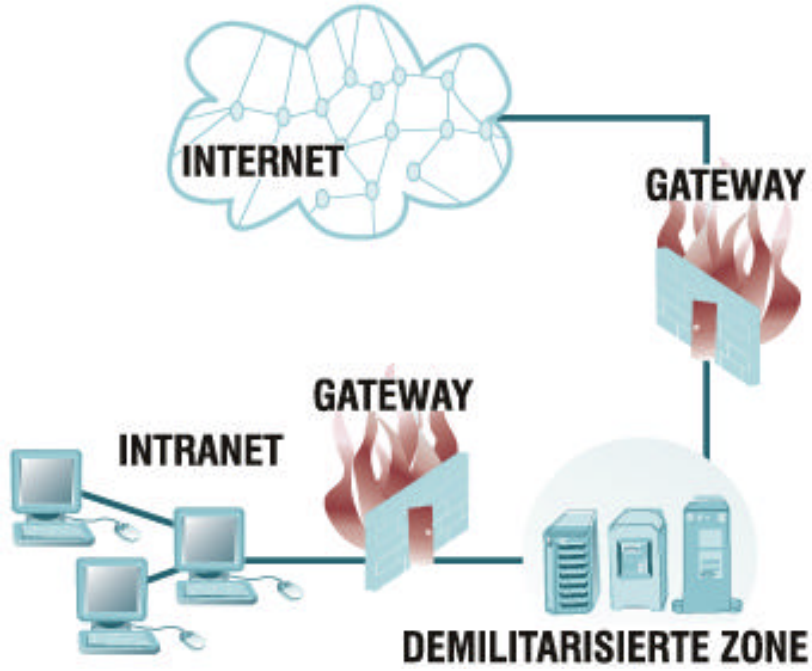
- **2 Rechner**
  2 Paketfilter auf einem Rechner
  + Demilitarisierte Zone (DMZ)
  mit Proxy-Server(n)



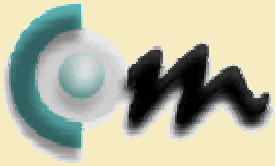
Firewall-Ausprägungen

- **3 oder mehr Rechner**
  2 Paketfilter-Rechner
  + Demilitarisierte Zone (DMZ)
  mit Proxy-Server(n)

- Entspricht "**PAP-Modell**" aus BSI-Grundschutzhandbuch
  - Paketfilter
  - Applikation Gateway
  - Paketfilter



4.1 Technische Sicherheitsmaßnahmen



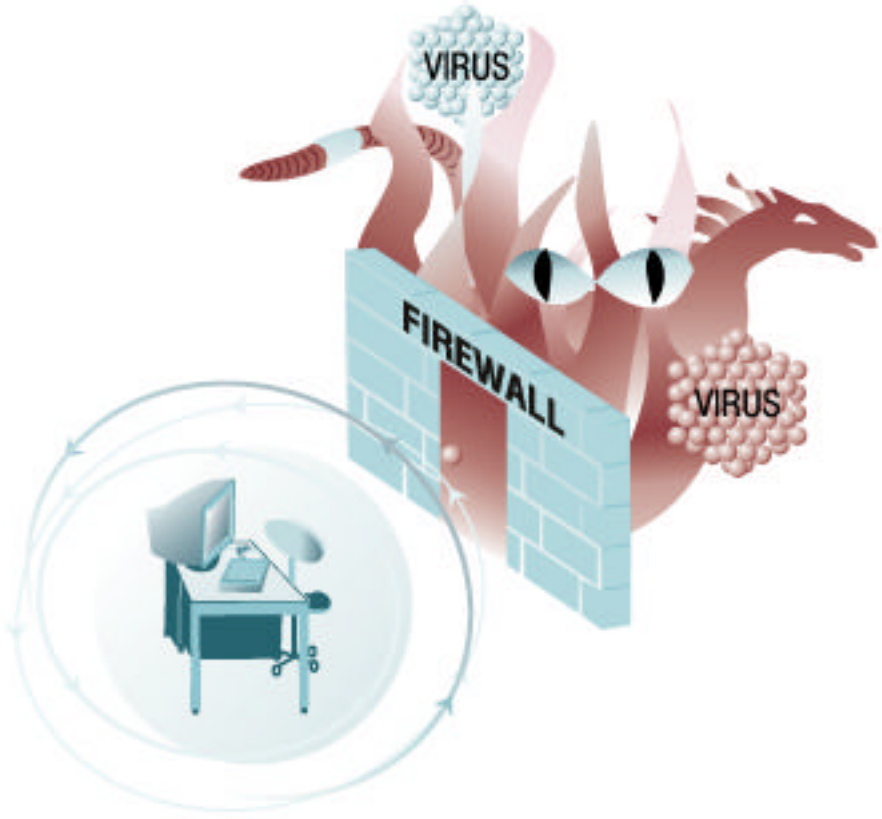
Heterogener Systemaufbau

- **System-Monokultur** ist problematisch, besser z.B.
  - Clients auf Windows-Basis
  - Internetzugang / Server auf UNIX-Basis
  - Paketfilter auf Basis von "Black-Box"-Lösung

- Gründe dafür
  - Mehrere Barrieren
  - Gegenseitige Schwachstellen-Kompensation
  - Kompromittierung erfordert Expertenwissen zu allen Systemen
  - "Open Source"-Software wird von vielen überprüft

4.1 Technische Sicherheitsmaßnahmen

Jeder Übergang zum Internet
muss durch eine Firewall
einheitlicher Qualität
gesichert werden



4.1 Technische Sicherheitsmaßnahmen

Periodischer Penetrationstest

- Sicherheitsprobleme effizient aufdeckbar
- Methodik

Durchführung	Angekündigt oder unangekündigt
Ausführender	Selbst oder externer Dienstleister
Aggressivität	Gering bis sehr hoch
Ausgangspunkt	Intranet oder Internet
Informationsstand	Zero Knowledge oder Systemkenntnis
Social Engineering	Anruf, Firmen-Info, Adresslisten, Passwort,… (um Startpunkt für Angriffe aufzusetzen)

4.1 Technische Sicherheitsmaßnahmen

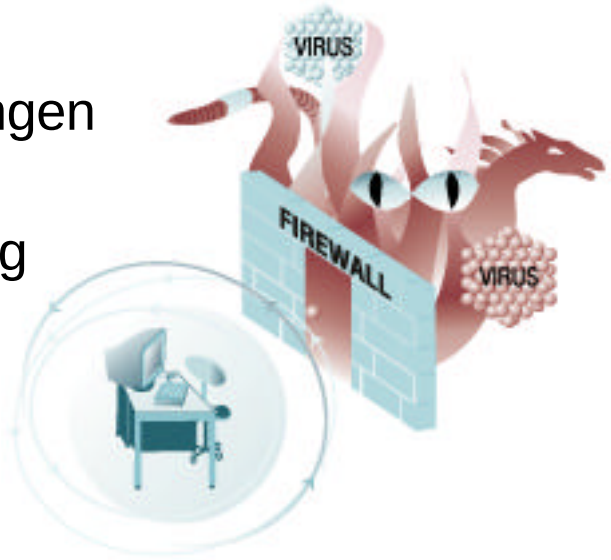
Weitere Möglichkeiten

- "Härten" von Betriebssystem / Anwendungen
- Dienste auf Minimum reduzieren
- Intrusion Detection System (IDS)
- Honeypot ("Honigtopf")
- Public Key Infrastructure (PKI)
  - Persönlicher Schlüsselaustausch
  - Zentraler Schlüsselaustausch
    - Interne(r) Trust Center
    - Externe(r) Trust Center
- Virtual Private Network (VPN)
  - Zwischen Netzwerk und Client
  - Zwischen Netzwerken

4.2 Kommerzielle Firewall-Lösungen

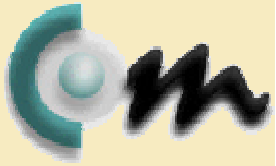
- Sehr viele Produkte erhältlich (meist auf UNIX-Basis)
  - CheckPoint FW-1 (Marktführer mit 50% Marktanteil)
  - Cisco Pix
  - Symantec
  - WatchGuard
  - ISA Server (MicroSoft)
  - GeNUGate (GeNUA)
  - ...
- Auswahl extrem abhängig von Anforderungen
- Sehr viele Bewertungs-Kriterien möglich
- Technische Features wenig aussagekräftig
- Sinnvoll: Zwei externe Dienstleister
  - a) Planung + b) Realisierung
- Guter Produktvergleich: www.itseccity.de

Die optimale Lösung gibt es nicht "von der Stange"



Inhaltsverzeichnis

5 .NET – Neue Technologien, neue Gefahren!

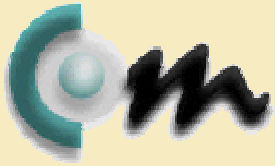


.NET = verteiltes Betriebssystem über das Internet

Basiert auf:

- **Web Services UDDI / WSDL / XMI / RDF**
  Plattformübergreifend im Internet angebotene Software-Dienste
- **SOAP** – Simple Object Access Protocol
  Standard zum Funktionsaufruf und Datentransfer zwischen Rechnern
- **XML** – eXtensible Markup Language
  Standard-Sprache zur Repräsentation strukturierter Daten
- **HTTP** – Hyper Text Transfer Protocol
  Standard-Protokoll zwischen Browsern und Web-Servern
- **TCP/IP** – Transmission Control Protocol / Internet Protocol
  Standard-Internet-Protokolle

5 .NET – Neue Technologien, neue Gefahren!



- Problem: Gesamte Kommunikation läuft über HTTP-Port 80
  → Sämtliche Paketfilter-Regeln werden nutzlos
  → Keine zentrale Sicherheits-Administration mehr möglich

"SOAP goes through firewalls like a knife through butter"

(Tim Bray, Alan Cox, James Gosling)

- Zwang zu zertifizierter Hard- und Software soll Problem lösen
  - TCPA – Trusted Computing Platform Alliance (Intel)
  - TPM – Trusted Platform Module
  - Palladium (Microsoft)
- Nachteile
  - Vollständige Auslieferung an Hersteller / Lieferant
  - Keine eigene Verwaltung der Sicherheit möglich
  - "Open Source" (z.B. Linux) nicht mehr einsetzbar

5 WLAN – 802.11

WLAN

- Nie so sicher wie kabelgebundene Netzwerke,
  da jeder in der Nähe prinzipiell Zugang zum Netz hat.
  - Reichweite 25 – 100 m (je nach baulichen Gegebenheiten)
  - Zugangskontrolle durch:
    - Netzwerknamen
    - Verschlüsselung (40 Bit unsicher, 64 / 128Bit verwenden)
    - Nur registrierte MACs dürfen Verbindung
      zum Access Point aufnehmen
  - Default-Zugangsdaten am Access Point abändern
    (meist Web-Interface-Zugang)
  - Leichte Decodierbarkeit des WEP-Protokolls erfordert
    dringend zusätzliche Maßnahmen wie z.B. VPN

5 Einschätzung der Situation

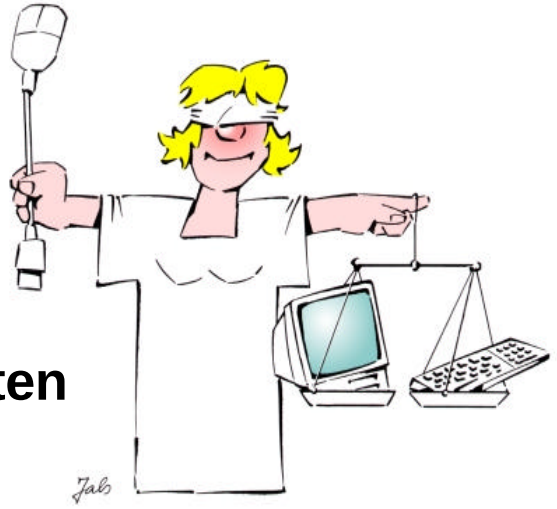
- Die **Abhängigkeit vom Internet** nimmt immer mehr zu
  - Die Sicherheits-Problematik wird **häufig unterschätzt**
- Mit neuen Internet-Diensten und Netzwerk-Technologien kommen **ständig neue Gefahren-Potenziale** hinzu
  - WLAN
  - Bluetooth
- "**Scheinsicherheit**" durch
  - Marketing
  - Personal Firewalls
  - Black-Box Lösungen
- Last but not least: "**Mangelnde Budgets**"

Viele Anwender sind sich der Gefahren nicht bewusst!

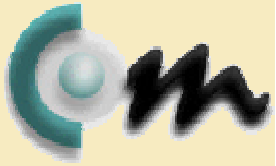
Viele Fälle werden nicht publik gemacht!

5 Rechtssprechung

- **Die Rechtssprechung ist noch im Fluss**
  - Thematik zu neu
  - Thematik sehr komplex
- **Das Internet erstreckt sich weltweit**
  - Wo enden nationale Rechte?
  - Wo fangen internationale Rechte an?
- **Es kommt kaum zur Ahndung von Straftaten**
  - Nachweis sehr schwierig
  - Identifizierung der Täter zu schwierig
  - Häufig unter den Tisch gekehrt
    - Negative Publicity vermeiden
    - Üblicherweise Aufhebungsvertrag



5 Was können Sie als Anwender tun?



- Gute Passwörter wählen (und sie geheim halten)
- Vorhandene Infrastruktur nutzen (ChipCard)
- Emails verschlüsseln (PGP, S/MIME)
- Eigene Zugänge zum Internet (Modem, ISDN, …) melden, um sie absichern zu lassen
- Sicherheits-"Advisories" zeitnah einspielen
- Benötigte Server-Dienste warten, unnötige deaktivieren (z.B. SQL-Server, Internet Information Server)
- Veraltete Hard- und Software, die nicht mehr gewartet und geändert werden kann, in getrenntes Netz auslagern
- Interne Sicherheits-Beratung in Anspruch nehmen

Wir wollen nichts verbieten, sondern bei der sicheren Umsetzung Ihrer Anforderungen helfen!

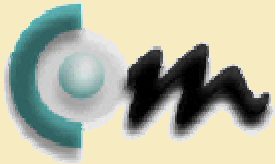
5 Fazit

- **Was wird kommen?**
  - Nachweis der eigenen Systemsicherheit notwendig
  - Beeinträchtigung von Geschäftspartnern strafbar
  - Einbruch in ungenügend gesicherte Netze nicht strafbar

- **Sicherheits-Konzepte sind**
  - Firmenspezifisch
  - Organisatorisch & technisch
  - Dynamisch

Intensivieren der Sicherheits-Aktivitäten
dringend erforderlich!

5 Quellen zum Thema Sicherheit



- **BSI** (Deutschland, www.bsi.de)
  Bundesministerium für Sicherheit in der Informationstechnik
  → Grundschutz-Handbuch
- **Bugtraq** (www.securityfocus.com)
- **CSE** (Kanada, www.cse-cst.gc.ca)
  Communications Security Establishment
- **Common Criteria** (USA / Europa, www.commoncriteria.org)
- **CERT** (Computer Emergency Response Team, www.cert.org)
- **ITSEC** (Europa, www.bsi.de/zertifiz/itkrit/itsec.htm)
  Information Technology Security Evaluation Criteria
- **SANS** (SysAdmin, Audit, Network, Security, www.sans.org)

Vielen Dank für Ihre Aufmerksamkeit!
Für Fragen stehen wir Ihnen zur Verfügung

Hermann Gottschalk
Thomas Birnthaler