# Netzsicherheit
# - ein lösbares Problem?

Hermann Gottschalk
Thomas Birnthaler



eMail: info@ostc.de
Web: http://www.ostc.de

# Inhaltsverzeichnis


1 Motivation

2 Gefahren aus dem Internet

3 Technische Sicherheitsmaßnahmen

4 Neue Technologien - neue Gefahren

5 Fazit

# 1 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

→ Eine Internet-Anbindung ist heutzutage **notwendig**!

# 2 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 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 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 |

# 2 Gefahren aus dem Internet

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

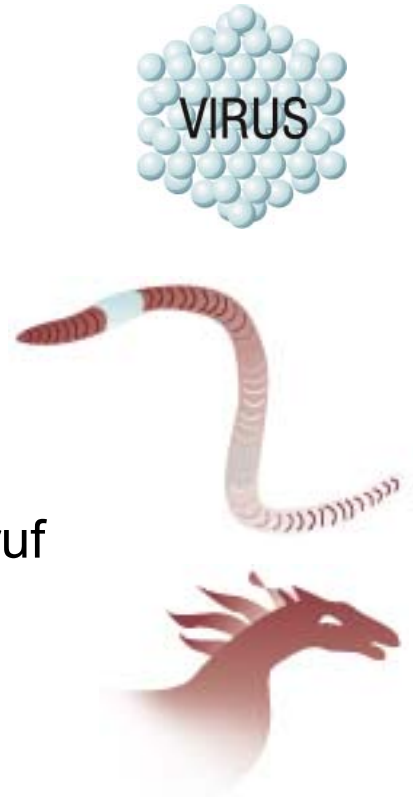
**Ursache**: Die eingesetzte Software (Betriebssystem, Grafikoberfläche, Browser, Server, …) hat **Entwurfs- oder Implementierungs-Fehler**, die für unvorhergesehene Zwecke ausgenützt werden können.

# 2 Angriffsmethoden

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

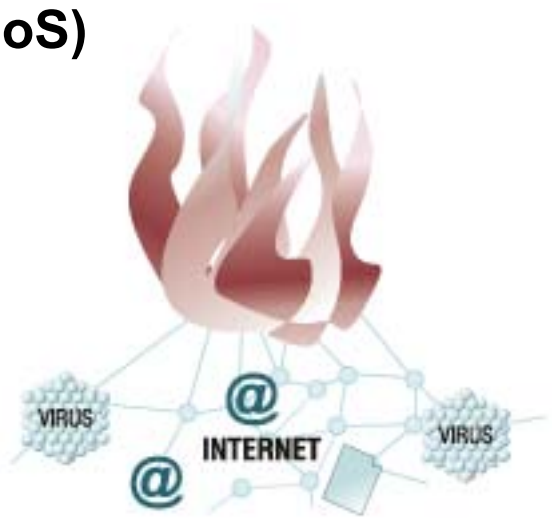
- **Virus**
  Software, die sich zu ihrer Verbreitung an ein anderes Programm hängt
- **Wurm**
  Programme, die sich selbständig ausbreiten und Computer vollautomatisch verseuchen
- **Trojaner**
  Harmlos erscheinende Programme, die beim Aufruf zusätzlich eine Schadensroutine abarbeiten



# 2 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



# 2 Weitere Angriffsmethoden

- Password Cracking
- Network Monitoring
- IP-Address Spoofing
- Man in the middle
- Application Layer Attack
- RootKits / Backdoor
- DNS Poisoning
- E-mail Spoofing
- Session Hijacking
- Replay Attack
- Buffer Overflow (Stack)
- CGI Attack
- Cookie Exploitation
- Social Engineering

**Diese Liste ist bei weitem nicht vollständig,**

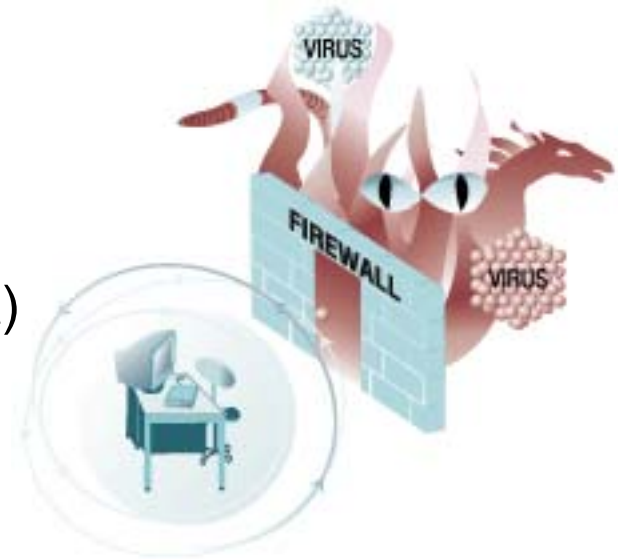
**jeden Tag werden neue Angriffsmethoden entdeckt!**

# 3 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)



# 3 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)

# 3 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

# 3 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)

# 3 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

# 3 Technische Sicherheitsmaßnahmen

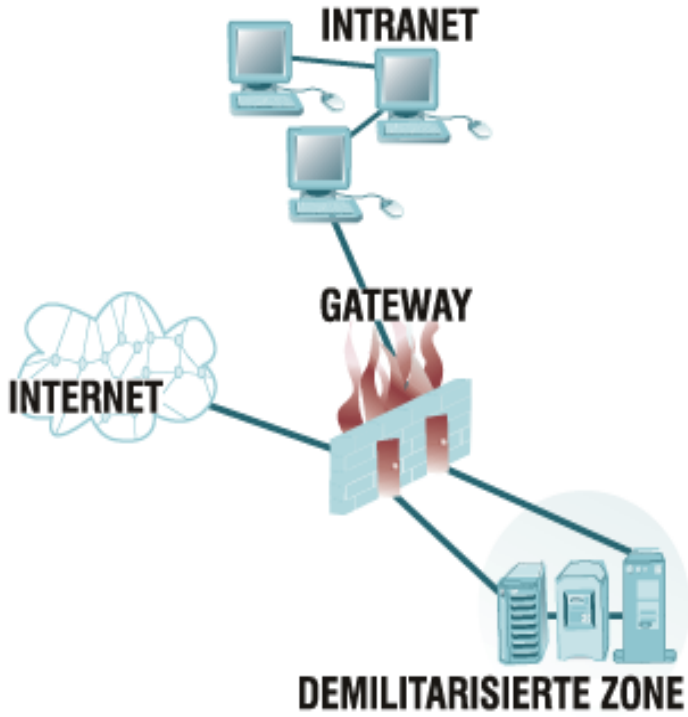
- Zusätzliche Vorteile von **Application Gateways**
  - Anwendungsbezogene Datenüberprüfung
  - Content Filtering (z.B. "WebWasher")
  - Caching (zwischenspeichern)
  - Transportierte Daten protokollieren

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

## 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)

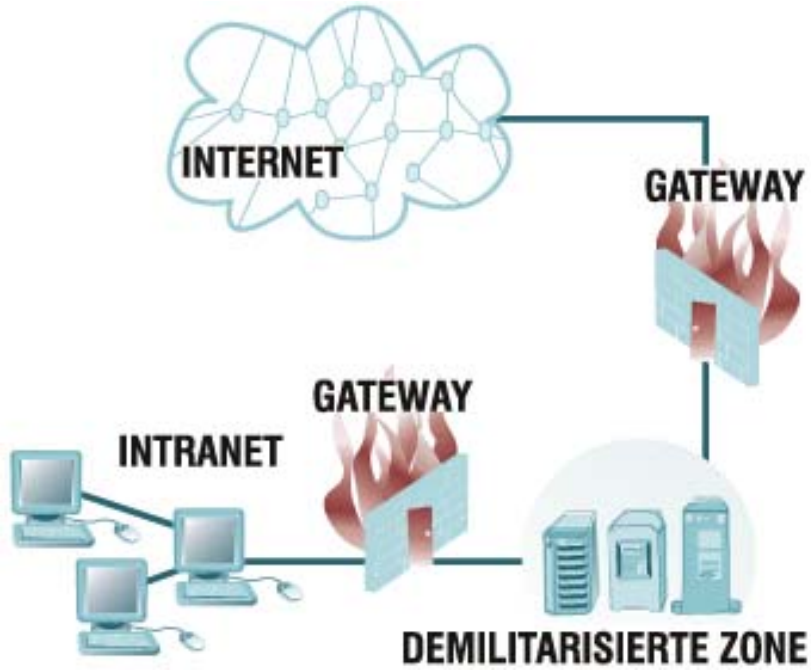


## Firewall-Ausprägungen

- **3 oder mehr Rechner**
  2 Paketfilter-Rechner
  + Screened Subnet
  mit Proxy-Server(n)

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



# 3 Technische Sicherheitsmaßnahmen

## Heterogener Systemaufbau

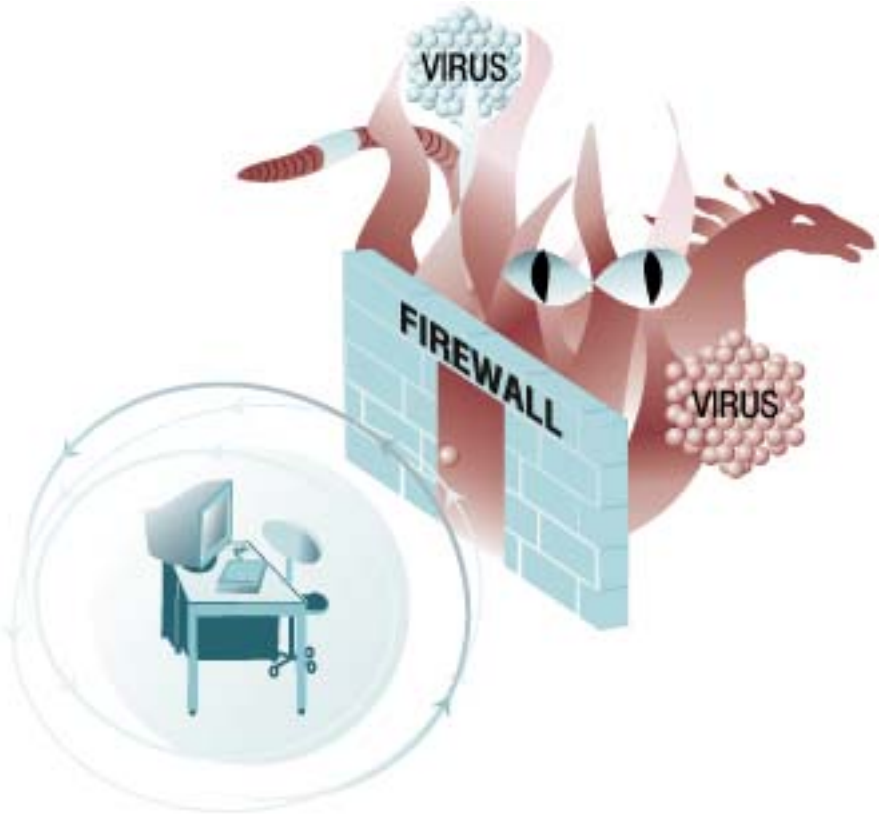
- **System-Monokultur** ist problematisch, besser z.B.
  - Clients auf Windows-Basis
  - Internetzugang / Server auf Linux-Basis
  - Paketfilter auf Basis von OpenBSD

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

# 3 Technische Sicherheitsmaßnahmen

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



# 3 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 .NET – Neue Technologien, neue Gefahren!

**.NET = verteiltes Betriebssystem über das Internet**

Basiert auf:


- **Web Services UDDI / WSDL / XMl / 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

# 4 .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
  - NGSCB - Next Generation Secure Computing Base (Microsoft)
- Nachteile
  - Vollständige Auslieferung an Hersteller
  - Keine eigene Verwaltung der Sicherheit
  - "Open Source" nicht mehr einsetzbar

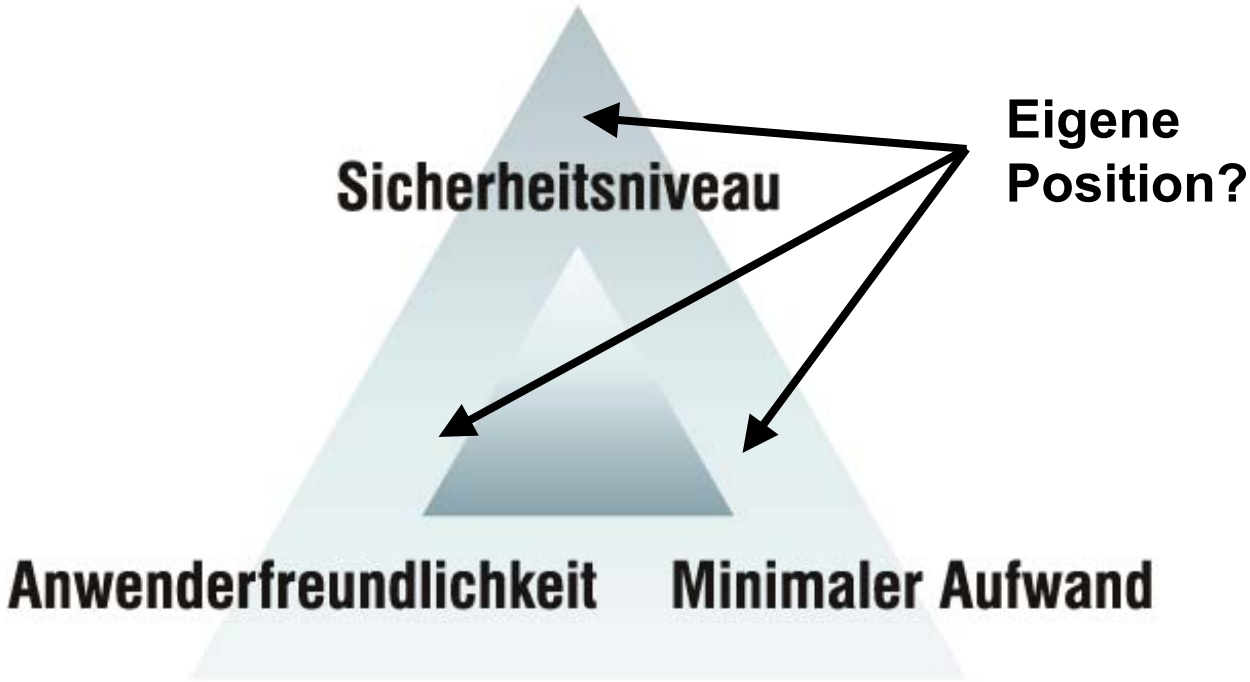
# 5 Fazit

- **Absolute Netzsicherheit ist nicht zu erreichen!**
  - Das **eigene Sicherheitsbedürfnis** muss definiert werden
  - Technische und organisatorische Maßnahmen müssen darauf abgestimmt werden.
  - Das daraus resultierende Risiko muss durch **Notfallpläne** abgesichert werden.
- **Neue Technologien** versprechen mehr Sicherheit, haben aber auch Nachteile:
  - Homogene Systeme sind einfach angreifbar
  - Verlust an Flexibilität
  - Auslieferung an Hersteller
  - Neue SW/HW → Neue Fehler

# 5 Fazit

**Beziehungs-Dreieck**



# 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



eMail: info@ostc.de
Web: http://www.ostc.de