IT - Sicherheit und Firewalls

C. Lenz, B. Schenner, R. Weiglmaier

24. Jänner 2003

TEIL 1

- **Grundlegendes**
- **Cookies**
- **Web-Log**
- **Spoofing**

IT-Sicherheit:

- Integrität
- Verbindlichkeit
- Verfügbarkeit
- Vertraulichkeit

Integrität:

- alle berechtigten Benutzer dürfen darauf vertrauen, dass Daten nicht unautorisiert verändert oder zerstört werden.

Verbindlichkeit:

- Nachweisbarkeit
- Urheberschaft
- Übermittlung
- Rechtssicherheit

Verfügbarkeit - Vertraulichkeit:

- Berechtigte können auf Daten zugreifen.
- Informationen und Dienstleistungen dürfen nur den Berechtigten zugänglich sein.

§ 14 DSG 2000:

- Maßnahmen zur Gewährleistung der Datensicherheit.

- unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit.

Cookies:

- Informationsstücke werden am Computer des surfenden Anwenders abgespeichert.
- Passwort kann gespeichert werden.
- Bezug zu einer konkreten Person kann hergestellt werden.

Web-Log:

- Protokollierung am Server eines Internet Providers.
- User (IP- Adresse)
- Datum und Name des Zugriffs
- verlangte Datei und deren Größe
- Statuscode

Zusätzlich:

- von welcher URL
- welches Betriebssystem
- welcher Browser

Spoofing:

- Vortäuschen einer falschen Absenderadresse, mit der Absicht, durch die gefälschte Absenderadresse authentifiziert zu werden.

Vorgehen:

- das Ziel wird identifiziert.
- der Host, als den man sich ausgeben will, wird lahmgelegt.
- die Adresse des Hosts wird vorgetäuscht.
- Verbindung mit dem Ziel, indem man sich als der lahmgelegte Host ausgibt.
- Sequenznummer erraten, die vom Ziel verlangt wird.

Testlauf:

- Kontakt mit dem Ziel und Verbindung anfordern.
- das Ziel antwortet mit einer Reihe von Sequenznummern.
- Protokollierung
- Analyse der aufgezeichneten Sequenznummern: Algorithmus herausfinden.
- Vorhersage welche Sequenznummern für die Authentifizierung erforderlich sind.
- in das System eindringen (z.B. *rhosts* umzuschreiben).

Die Opfer:

- jedes System mit SunRPC.
- jeder Netzwerkdienst der IP- Authentifizierung verwendet.
- X- Window- System von MIT, wenn eine host- basierte Authentifizierung verwendet wird.
- die r-Utilities (rlogin, rsh, rcp, rcmd).
- Windows NT

Wie kann man Spoofing-Attacken verhindern?

- Netzwerk konfigurieren.
- Netzwerk überwachen.
- Protokollierung.

TEIL 2

- **Passwort-Cracking**
- **Scanner**
- **Trojaner**

Passwort-Cracking:

- sicheres Passwort
- DES (= Data Encryption Standard)
- Dictionary-Attack
- Brute-Force-Methode

Scanner:

- Sind Programme, mit deren Hilfe ein Angreifer seinen Ziel-Host nach vermeintliche fehlerhaften Diensten abtasten kann.
- Legalität ist umstritten.
- Scanner sind wichtige Instrumente, um Netzwerksicherheit zu erhöhen.
- Vereinfachen die Arbeit von System Administratoren.

Trojaner:

- Ein Trojaner ist ein unautorisierter Code innerhalb eines legitimen Programms, welcher auf dem Rechner des Benutzers nicht bekannte Aktionen durchführt.

- wie z.B.:
  - Informationen sammeln
  - Passwörter stehlen
  - Dateien kopieren
  - Dateinamen vermischen

- Wenn Programmierer Trojaner einschleusen (z.B. SATAN 1.0).

Trojaner (Fortsetzung):

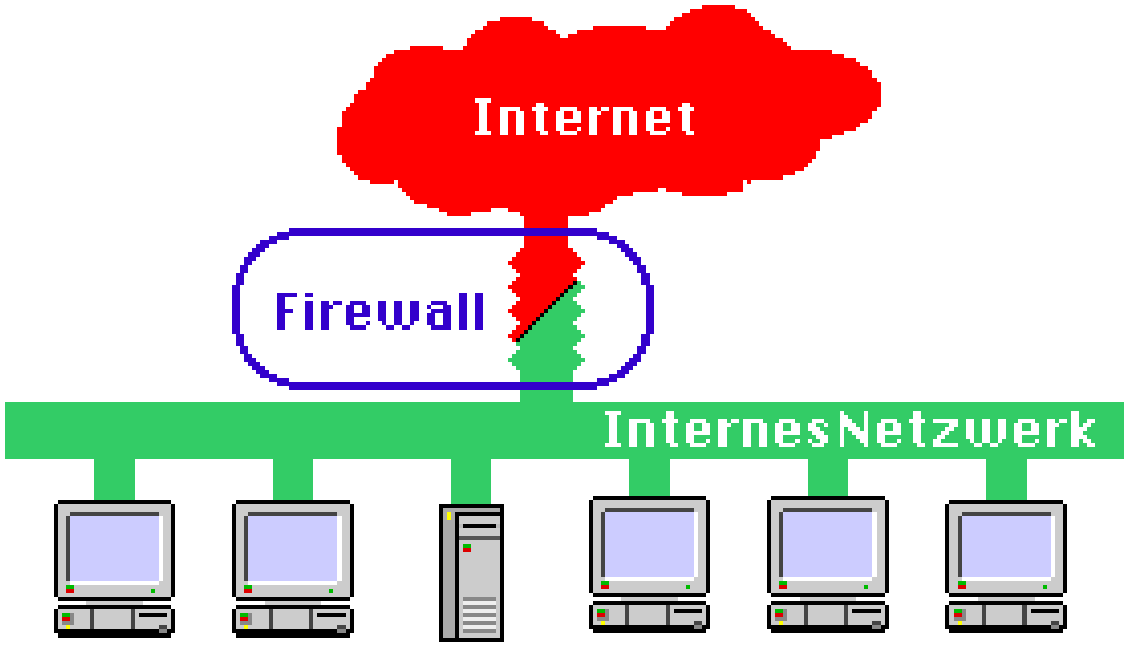
Schutz:

- Aufspüren mittels Objektvergleich.
- Vergleich der letzten Modifikation, dem Entstehungsdatum, oder der Größe der Datei reicht nicht.
- Kontrolle durch Prüfsummen.
- digitalen Fingerabdruck mit dem MD5-Algorithmus erzeugen.
- Dateiintegritätstools wie Tripwire, TAMU, ATP.

TEIL 3

- **Firewalls**
- **Sicherheitsrelevante Komponenten einer Firewall**
- **Kategorien der Firewalls**
- **Resüme**

Firewalls



Sicherheitsrelevante Komponenten einer Firewall

- Hardware
  Die Hardware ist das geringste Problem sie sollte jedoch leistungsfähig genug sein, so dass die Software unproblematisch auf dem Rechner läuft.

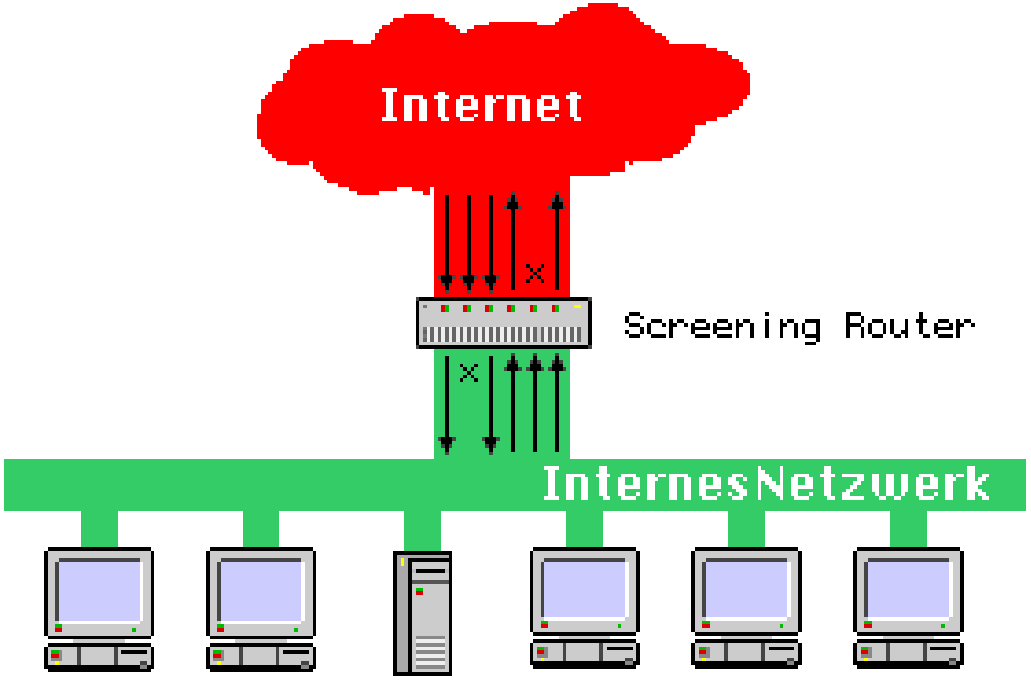
- Software
  Die verwendete Software sollte den Kenntnissen des Benutzers entsprechen. Da das größte Problem eher an der Konfiguration der Firewall als an der Firewall selbst liegt.

- Benutzer

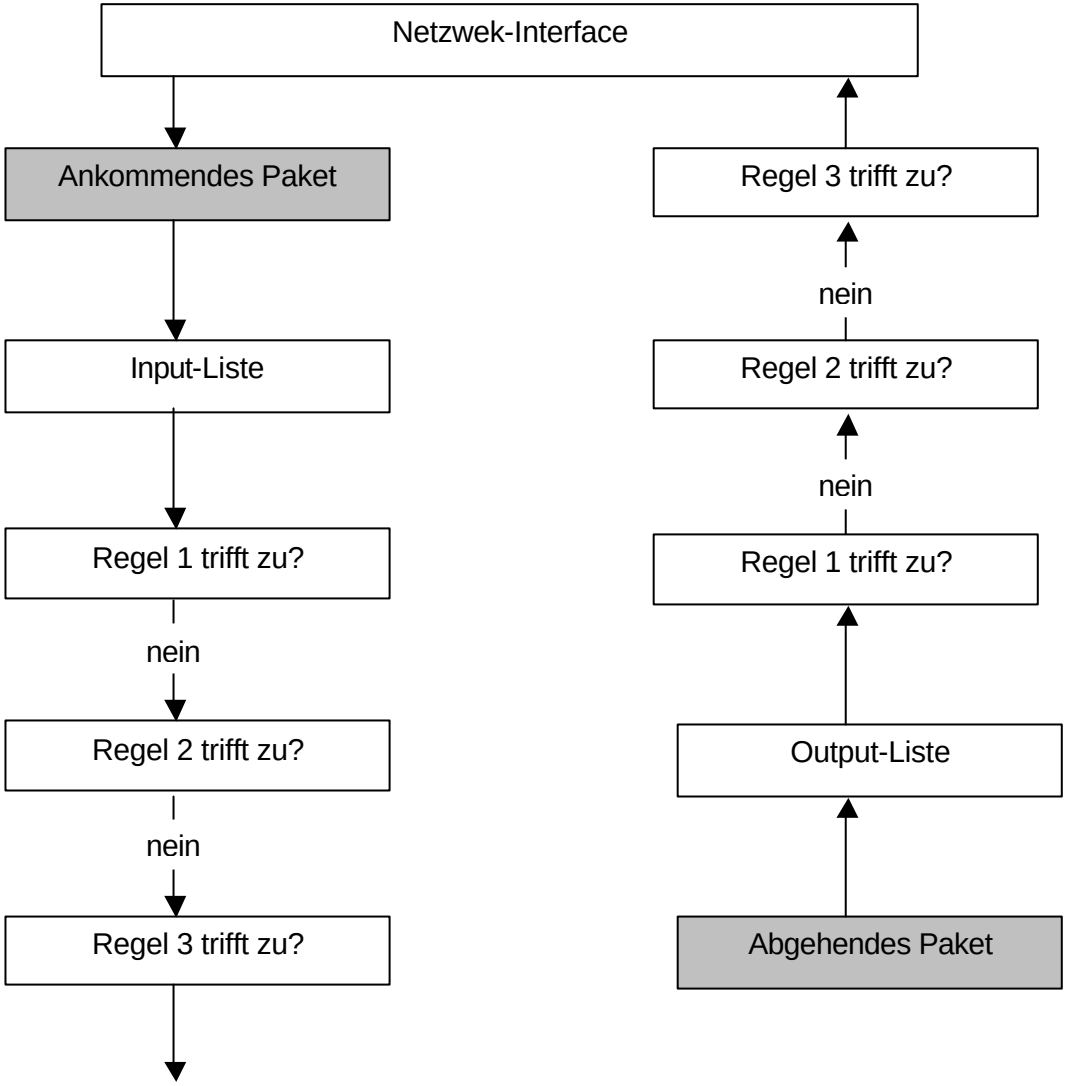
  Aufgaben:
  - o die Firewall ständig up to date zu halten.
  - o Logfiles auswerten.

Kategorien der Firewalls

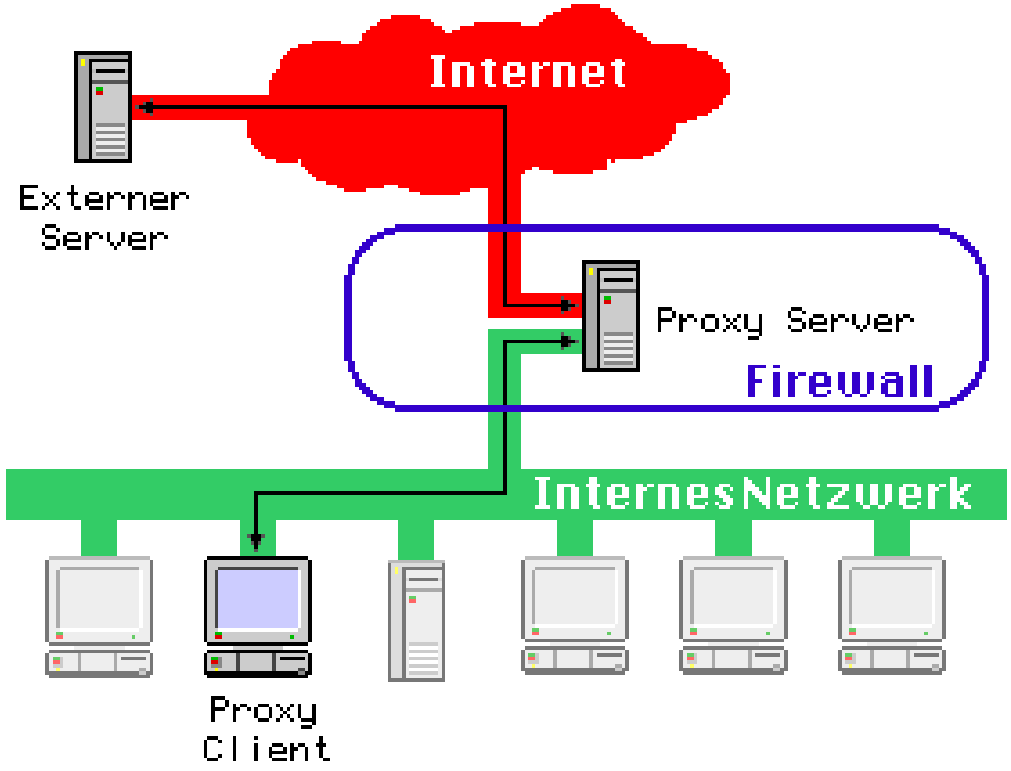
- Netzwerkschicht Firewalls
  - o IP- Filter Firewall (auch Paket- Filter Firewall)



Ablaufschema



- Anwendungsschicht- Gateway Firewalls
  - Application-Proxy-Firewalls



Desktop Firewalls

- laufen auf dem PC selbst

- Aufgaben

    - Sollen Rechner vor Angriffen von außen schützen

Resümee

- Zentrale Fragestellung lautet
  - **Was will ich vor wem und womit schützen?**

- Weiters sollte man sich die Fragen stellen
  - **Wie viel sind meine Daten wert?**
  - **Wie viel würde es kosten, wenn diese Daten verloren gingen?**
  - **Wie teuer ist ein Schutz dieser Daten?**

Literaturhinweis

- **Hacker's guide** Sicherheit im Internet und im lokalen Netz
  Markt & Technik www.mut.de
  ISBN 3-8272-5460-4

- **Linux Hacker's guide** Sicherheit für Linux-Server und –Netze
  Markt & Technik www.mut.de
  ISBN 3-8272-5622-4

- **Linux Firewalls** Konzeption und Implementierung für Netzwerke und PCs
  Markt & Technik www.mut.de
  ISBN 3-8272-5849-9

- **Maximum Security**
  Sams.net Publishing
  ISBN 1-57521-268-4