

Seminar Internet Technologien

Sicherheit im Internet

Christian Wachsmann

Gliederung

1. Einführung
2. Grundlagen der Kryptographie
3. Firewalls
4. Ausgewählte Angriffsmöglichkeiten
5. Ausgewählte Gegenmaßnahmen
6. Ausblick
7. Literatur & Links

Grundsätzliche Gefahren eines Internetanschlusses

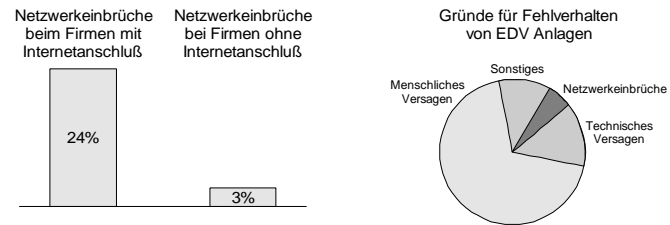
- Löschung, Verfälschung und Einfügung von Daten
- Verlust vertraulicher Informationen
- Störung der Netzverfügbarkeit
- Vortäuschung falscher Identität
- Viren und Trojanische Pferde

Sicherheit im Internet – Folie 3/22

Grundsätzliche Risiken einer EDV-Infrastruktur

- Menschliches Versagen
 - Fehlbedienung
 - „wollte nur sehen, was passiert wenn...“
 - Einschleppen von Viren
- Technisches Versagen
 - Stromausfall
 - Festplattencrash
- Sonstiges
 - Netzwerkeinbrüche

Risikovergleich



Quelle: National Computer Security Association 1995

Sicherheit im Internet – Folie 5/22

Risikoanalyse

Definition Risiko nach DIN, VDE Norm 31000:

- Häufigkeit eines gefährdenden Ereignisses
- Schadensausmaß beim einem gefährdenden Ereigniseintritt

Verschiedene Risiken:

- Sicherheitsrelevanter Vorfall auf einem Host: einmal in 45 Jahren
- Festplattencrash: einmal in 75 Jahren
- Tödlicher Autounfall: einmal in 6250 Jahren

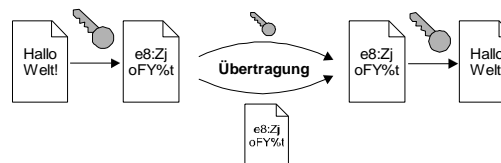
Grundlagen der Kryptographie

Begriffe:

- Identifizierung:
Zusicherung der eigenen Identität
- Authentifizierung:
Vorgang des Beweisens der eigenen Identität
- Autorisierung:
Ableitung von Rechten aus einer Identität

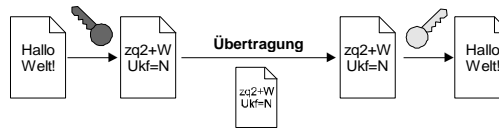
Sicherheit im Internet – Folie 7/22

Symmetrische Verschlüsselung



- Nur 1 Schlüssel zum Kodieren und Dekodieren
- Pro Teilnehmerpaar wird ein Schlüssel benötigt
- Wichtige Blockchiffren: (Triple-) DES, IDEA

Asymmetrische Verschlüsselung



- Ein Schlüssel zum codieren, einer zum decodieren
- Pro Teilnehmer nur ein Schlüsselpaar
- Umkehrung des Prinzips: Digitale Signaturen
- Wichtigstes Public-Key-System: RSA

Sicherheit im Internet – Folie 9/22

Sichere Hashfunktionen

- Abbildung eines beliebig langen Textes auf einen Hashwert (digitaler Fingerabdruck)
- Garantiert die Integrität eines Dokuments
- Digitale Signatursysteme können auf den Hashwert statt auf das Dokument angewendet werden
- Beispiel Message-Digest-Funktionen (MD5):
2 Dokumente besitzen nur in einem von 2^{64} Fällen den gleichen Hashwert.

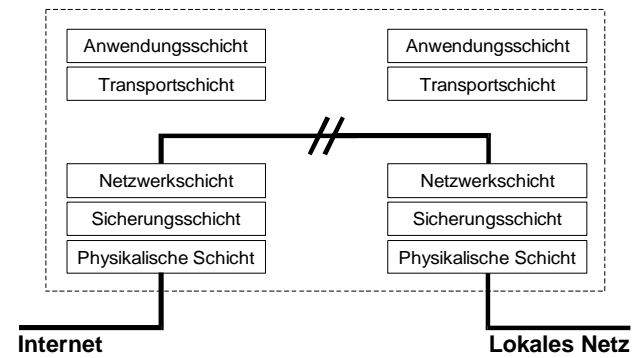
Firewalls

Eigenschaften von Firewalls:

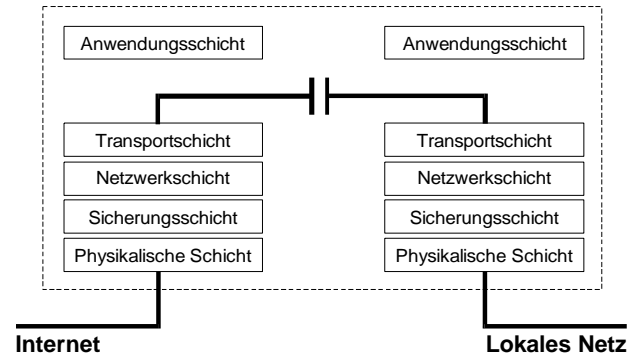
- Jeglicher Datenverkehr zwischen innen und außen muß die Firewall passieren
- Nur der im Sicherheitskonzept vorgesehene Datenverkehr wird durchgeschleust
- Die Firewall selbst muß immun gegen Angriffe sein

Sicherheit im Internet – Folie 11/22

Paketfilter

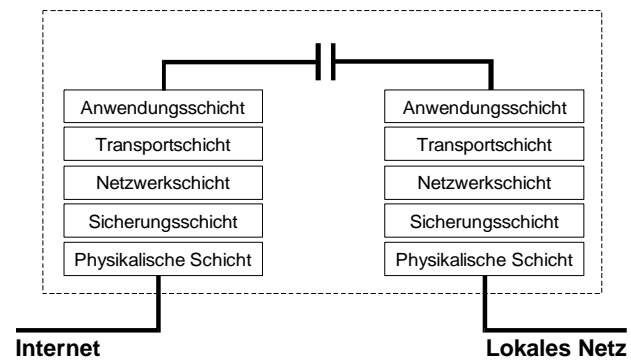


Circuit Relay



Sicherheit im Internet – Folie 13/22

Application Gateway



Grenzen von Firewalls

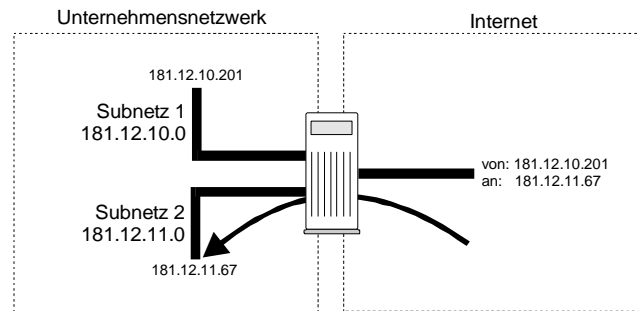
- Kein Schutz gegen Bedrohung von innen
- Korrektheit einer Firewall kann nicht bewiesen werden, und komplexe Systeme haben Fehler
- Firewalls können Netzaktivitäten nur zwischen den OSI Schichten 3 und 7 überwachen
- Meistens werden mehrere Firewall-Typen kombiniert

Sicherheit im Internet – Folie 15/22

Ausgewählte Angriffsarten

- Paßwort Attacken
- Social Engineering
- Protokollfehler und Hintertürchen
- Denial-of-Service Angriffe

Internet-Address-Spoofing

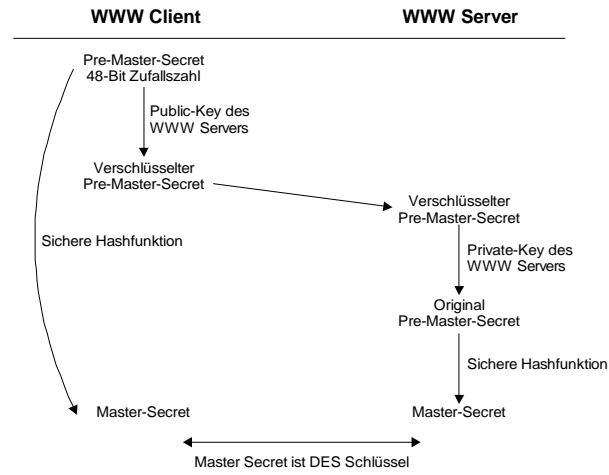


Sicherheit im Internet – Folie 17/22

Secure Socket Layer (SSL)

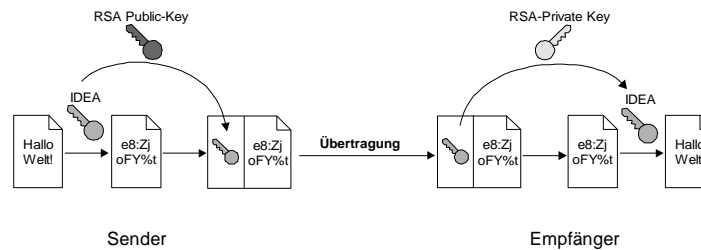
- HTTP Kommunikation erfolgt im Klartext
- Schutz vor Löschung, Verfälschung und Einfügung durch Sicherheitsprotokoll SSL (Netscape, Inc.)
- Zusätzliche Protokollschicht zwischen TCP/IP und höheren Schichten
- Mechanismus bleibt dem Benutzer verborgen
- Erkennbar an HTTPS:// anstatt HTTP://

Funktionsweise von SSL



Sicherheit im Internet – Folie 19/22

Pretty Good Privacy (PGP)



- E-Mail (und Datei) Verschlüsselungssystem
- Ziel: Verschlüsselung der Nachricht und Authentifikation

Ausblick

- Neue Protokoll Versionen
 - IPv6: Authentifikation und Verschlüsselung auf IP-Ebene
 - HTTP-NG: Übernimmt Funktionalität von SSL
- Firewalls auf Basis von Expertensystemen

Sicherheit im Internet – Folie 21/22

Literatur

O. Kyas: Sicherheit im Internet
International Thomson Publishing, 1998

W. Cheswick, S. Bellovin: Firewalls and Internet Security
Addison Wesley, 1996

B. Schneier: Applied Cryptography
Wiley, 1994

Internet Links

[http://www.yahoo.com/text/Computers_and_Internet/
Security_and_Encryption](http://www.yahoo.com/text/Computers_and_Internet/Security_and_Encryption)

<http://www.cs.purdue.edu/coast>