Firewalls

Roland LIEGER Harput VAHAN

Grzegorz RUMATOWSKI Patrik AWART

12. Dezember 1996

Einführung:

Was soll geschützt werden?

- Daten: (Vertraulichkeit, Integrität, Verfügbarkeit)
- EDV-Resourcen: (CPU-Kapazität, Plattenplatz)
- Reputation

Vor wem soll es geschützt werden?

- Spaßvögel
- Punktesammler
- Vandalen
- Spione
- Dummheit/Unfälle

Sicherheitsmodelle:

- Keine Sicherheit
- Sicherheit durch Täuschung
- Rechnerzentrierte Sicherheit
- Netzwerkzentrierte Sicherheit

Möglichkeiten einer Firewall:

Eine Firewall bietet:

- Fokus für Sicherheitsentscheidungen
- Zentraler Ein-/Ausstiegspunkt
- Begrenzung der Angriffsfläche

Eine Firewall bietet KEINEN Schutz vor:

- Angriffe durch Insider
- Umgehung durch weitere Datenleitungen
- Viren, Trojanische Pferde etc.
- Unbekannte Gefahren

Internet Dienste:

- EMail
- File Transfer - FTP
- Remote Login - Telnet
- Usenet News
- Domain Name Service - DNS
- Internet Control Message Protocol - ICMP
- und viele weitere ...

Sicherheitsstrategien:

- Minimale Privilegien
- Mehrstufioge Verteidigung
- Zentraler verbindungsknoten mit Drosselfunktion
- Achte auf das Schwächste Glied
- Ausfallssicherheit:
  - Alles was nicht verboten ist, ist erlaubt
  - Alles was nicht erlaubt ist, ist verboten
- Diversitäre Systeme
- Mitarbeit aller Betroffenen
- Einfachheit - Keep It Straight and Simple

Grundformen der Filterung:

- IP-Paket Filter:
- Proxy-Systeme:

Aufbau von Firewalls:

- Dual-Homed Host:
- Screened Host:
- Systeme mit peripherem Netz: