Firewalls

Wächter zwischen den Netzen

Dipl.-Inf. Marco Thorbrügge

DFN-Workshop „RZ-bezogene Netzdienste“

21. bis 22.03.2002 in Kassel

DFN CERT

Unterscheidung: PF und FW

Paketfilter:
Ein Gerät zum Herausfiltern unerwünschten TCP/IP-Datenverkehrs (Bestandteil eines Firewall-Konzeptes)

Firewall-Konzept:
Konzept zur physikalischen und logischen Trennung von Teilnetzen mit unterschiedlichen Sicherheitsanforderungen

DFN CERT

Paketfilter: Was ist das?

Anwendung	*Anwendungen:*
Darstellung	*SMTP, HTTP, FTP, ...*
Steuerung	
Transport	*Transport: TCP, UDP*
Vermittlung	*Internet: IP*
Sicherung	*Netzwerk:*
Bitübertr.	*Ethernet, ATM, Token Ring, ...*

Paketfilter

DFN CERT

Was wird untersucht?

- Source-IP-Adresse (Quell-Host)
- Destination-IP-Adresse (Ziel-Host)
- Source-Port (Service)
- Destination-Port (Service)
- Flags (SYN,ACK, etc.) (nur TCP)
- Service-Nummer (nur ICMP)

DFN CERT

Problem: Vielzahl von Produkten

- Linux netfilter (aka „iptables“)
- *BSD ipfilter
- Cisco Pix
- Checkpoint Firewall-1
- Viele, viele weitere

➢ Umfangreiche Vergleichstests notwendig, um Auswahl treffen zu können

DFN CERT

Policy: Ohne Planung geht nichts!

- ***Das*** „Standard-Netzwerk“ **gibt es nicht!**
- Realisierung von Firewall-Konzepten bedarf genauer Planung
- Regeln müssen individuell erstellt werden (Policy)
- Policies müssen durchgesetzt werden
- Firewall-Lösungen out-of-the-box können nicht funktionieren (und sind sogar gefährlich!)

➢ Sehr anspruchsvolle Aufgabe, erfordert viel Know-How!

DFN CERT

Zukünftige Entwicklungen

- Firewalls gehören bereits jetzt zur Standard-Ausstattung im Security-Umfeld
- Zukünftig werden komplexere Protokolle immer wichtiger (Videokonferenzen, H.323)
  -> Probleme mit herkömmlichen Firewalls (Studie liegt vor)
- Sichere (VPN-)Lösungen nicht immer mit herkömmlichen Firewalls kombinierbar (verschlüsselter Datenverkehr, IPSec)
- Höhere Bandbreiten -> höheres Paketaufkommen -> Performanceprobleme herkömmlicher Firewalls

DFN CERT

Notwendige Unterstützung für Anwender

- Beratung bei Produktauswahl
- Beratung bei Erstellung von Policies
- Forschung: neue Protokolle und Firewalls
- Forschung: Firewalls und höhere Bandbreiten
- Forschung: Firewalls und VPN-Lösungen
- Application-Level Firewalls? Zentrale Administration?

➢ Validierung von Firewall-Konzepten im Testlabor: Sammlung des notwendigen Know-How

➢ Rückfluss des Know-How an DFN-Anwender: Beratung, Schulung, Handbücher etc.

DFN CERT