Verteilte Systeme

...für C++ Programmierer

Firewalls

by

Dr. Günter Kolousek

12. April 2016

Firewalls & Aufgaben

- Komponente im Sicherheitssystem
- Schutz einzelner Rechner oder Rechnernetze vor unerlaubten Zugriffen
  - d.h. keine Angriffserkennung, sondern Umsetzung von Regeln
- internes vom externen Netz trennen und abschotten
- eingehenden und **ausgehenden** Datenstrom regulieren
  - d.h. nicht durchlassen, wenn Regeln verletzt
- Umsetzung der Sicherheitspolicy
- Alarm bei Verletzung der Regeln
- Protokollierung des Datenverkehrs

Arten

- Personal Firewall
  - SW auf dem zu schützenden Rechner
- externe Firewall
  - eigenes Gerät: Firewall SW oder Appliance

Personal Firewall

- Schutz des Rechners
- filtert zwischen Rechner und Netzwerk
- Vorteile
  - einfach installierbar, keine externen Abhängigkeiten
  - Konfiguration für einzelnen Rechner!
- Nachteile
  - Firewall-SW kann selbst angegriffen werden
    - z.B. Deaktivierung
  - Firewall-SW kann abstürzen

Externe Firewall

- Schutz von Rechnern und Netzen
- filtert zwischen Netzen
- Vorteile
  - bei Kompromittierung $\rightarrow$ kein Endsystem kompromittiert
  - gesamtes Netz geschützt
- Nachteile
  - Kosten
  - zusätzliches Netz (wenn dieses nicht benötigt wird)

Typen

- Paketfilter
  - nur Header wird betrachtet
  - jedes Paket wird einzeln betrachtet
  - z.B. Verwerfen auf Grund der Source IP
- stateful Paketfilter
  - nur Header wird betrachtet
  - es wird Folge von Paketen betrachtet
  - z.B. Verwerfen wenn nicht zu einer Verbindung
- Application Gateway
  - Inhalt wird ebenfalls betrachtet
  - z.B. wenn Virus als Attachment bei E-Mail

Paketfilter

- Header
  - Source IP, Destination IP, Identification, DF, MF,…
  - Port, SequenceNum, SYN, ACK, FIN, RST,…
- Aktionen
  - accept: akzeptieren
  - reject: ablehnen, senden von ICMP *port unreachable*
  - drop: verwerfen

Sichtbarkeit

- sichtbar
  - Proxy-Funktionalität
- transparent
  - Router
  - auf IP Ebene sichtbar
- unsichtbar
  - Bridge
  - auf IP Ebene *un*sichtbar
  - Vorteile
    - Router muss kein Firewalling beherschen
    - können nachträglich eingebaut werden

Aufteilung in Netze

- internes Netz
- demilitarisierte Zone (DMZ)
  - angriffsgefährdet, da externe Dienste
  - zusätzliche Sicherheitsschicht
- externes Netz
  - unsicher

DMZ

- Hosts in der DMZ
  - begrenzter Zugriff auf internes Netz
    - da nicht so sicher wie internes Netz
  - begrenzter Zugriff auf externes Netz
    - um DMZ sicherer zu machen
- kein Zugriff von externen Netz auf internes Netz
- Arten
  - einstufig
  - zweistufig

Services

- internes Netz
  - LDAP, DHCP
  - Dateiserver, Datenbankserver
  - Application Server
  - interne SMTP Server
- DMZ
  - Proxy
  - Reverse Proxy, WWW
  - extern zugreifbare SMTP Server
  - externe DNS