

Firewall-Versuch

1 Sicherheitsmanagement

Aktive und passive Angriffe können zu Verlust führen von:

- Datenintegrität,
- Vertraulichkeit (hier auch verdeckte Kanäle berücksichtigen),
- Verfügbarkeit.

Anforderungen an das Sicherheitsmanagement ist die Abwehr von Bedrohungen die die obigen 3 Punkte betreffen, aber gegebenenfalls auch der:

- Verbindlichkeit (nicht abstreitbar) und der
- Anonymität.

→ Zuordnung der Subjekte durch interne IDs und Zuordnung von Rechten (Autorisierung).
→ Notwendigkeit der Authentisierung.

Häufiger Angriff: Einbruch von Außen. Unberechtigtes Erlangen von Rechten. Firewall versucht dies zu verhindern.

2 Firewall-Arten

- Packet Filter

- Feature: Entscheidung über Weiterleitung von IP-Paketen
- Nachteil: Fragmentierte IP-Pakete, kein Status verfügbar \implies manches geht nicht (FTP), Pakete unverändert in internes Netz gelassen, grobgranular, geringe Differenzierung, bzw. Differenzierung schwierig zu erreichen \implies Fehleranfällig, beruht z.T. auf Ungenauigkeit des ACK-Flags
- Vorteil: einfach, billig (in Router enthalten)
- Realisierung: Geordnete Liste von Regeln, die der Reihe nach abgearbeitet werden. Wenn eine passt, wird die dazugehörige Aktion ausgeführt. Ende.
- statisch: Problem bei UDP, weil kein ACK Flag
- dynamisch: dynamische Regeln für erwartete Pakete (z.B. für UDP)

- Circuit Level Gateway

- Konfiguration: Quellport \implies IP-Adresse + Zielport
- Feature: Weiterleitung von TCP-Verbindungen
- Nachteil: Keine anwendungsspezifischen Sicherungen und Log-Features, oft eingriff in den Quellcode der Applikationen nötig
- Vorteil: für viele TCP-basierte Anwendungen geeignet

- Application Level Gateway

- Feature: Proxy mit Verständnis für das Protokoll
- Nachteil: hoher Ressourcenverbrauch
- Vorteil: „versiebt“ Protokolle auf höheren Schichten, Application level Logging & Eingriffe (z.B. URL-Filter)

Bild

3 Architekturen

- Dual Homed Gateways

- im Praktikum
- besser als nix
- für Heimbereich/Kleinbetriebe mit temporärem Anschluß
- komplex \implies gefährlich

- screened subnet

- screening = Filterung nach IP-Adressen
- zusätzliches Subnet. Keine direkte Verbindung von Innen und Außen.
- Gateway so komplex wie vorher
- aber Absicherung durch Paketfilter

- * äußerer Filter: läßt nur Verbindung zu Hosts in DMZ zu (\implies keine direkte Verbindung nach innen)
- * innerer Filter: läßt nur Verbindungen von Gateway zu ganz bestimmte Rechnern durch
- * Vorteil: einfache Filterregeln, einfache Features \implies relativ sicher
- * Rechner innen mißtrauen Gateway
- * Wenn Gateway geknackt wird muß Administrator das mitbekommen \implies Policy

4 Einbettung in Unternehmensstruktur und strategie

Aufstellen und Durchsetzen von Policies:

- Welche Anwendungen muß ich unterstützen, welche will ich unterstützen
- Ansatz
 - optimistisch: Was nicht verboten ist, ist erlaubt.
 - pessimistisch (=Erlaubnisprinzip) : Was nicht erlaubt ist, ist verboten. (\leftarrow bevorzugt!)

- Log-Files anschauen, Rechner überwachen
- Laufend über neue Sicherheitslücken informieren
- Umgang mit Mail-Attachments
- Umgang mit Denial-of-Service Angriffen

Bei der Umsetzung der Policies muß natürlich auf die Durchsetzbarkeit geachtet werden bzgl.:

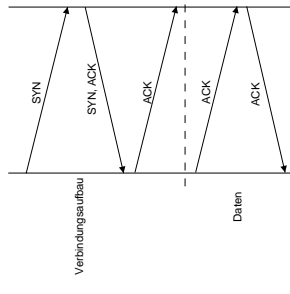
- Benutzerakzeptanz
 - Schulung/Weiterbildung (Zeit/Lust)
 - Gewohnheiten verändern (z.T. „umständlichere“ Arbeitsschritte)
 - Einschränkungen in Kauf nehmen

- Kosten
 - direkte:
 - * Hardware/Software (Kauf+Installation+Betrieb) (neu vs. Umrüstung)
 - * Schulungen/Weiterbildung
 - indirekte:
 - * direkte: Hardware/Software (neu vs. Umrüstung)
 - * indirekte: Beeinträchtigung der Arbeitsprozesse/-geschwindigkeit (zusätzliche Arbeitsschritte + s. Benutzerakzeptanz)

In beiden Fällen spielt die Integration/Anpassung/etc. bestehender Systeme, Vorgänge und Gewohnheiten eine besondere Rolle.

5 Header

- IP
 - Quelladresse
 - Zieladresse
 - Protokoll (TCP, UDP, ...)
- UDP
 - Quellport
 - Zielport
 - Problem: keine Verbindungen erkennbar
- TCP
 - Quellport
 - Zielport
 - Flags: Zeigen Richtung des Verbindungsaufbaus an



Bild