IT-Sicherheit

Vortrag am 06.06.2002

in Hannover (DVG)

Arbeitskreis Informationstechnologie

IHK – Uni Hildesheim

Prof. Dr. E. Schwarzer

Literatur

- O. Kyas, M. a Campo, IT-Crackdown (Sicherheit im Internet), MITP-Verlag Bonn, 2000, ISBN 3-8266-4080-2
- W. Stallings, Sicherheit im Internet, Addison-Wesley Verlag München, 2000, ISBN 3-8273-1697-9
- R. W. Gerling, Planung einer Firewall, in: IT-Sicherheit 6/2000, S. 10ff
- D. Henze, Sicherheit im Internet, in: Frauenhofer Magazin 1/2002, S. 13
- http:// www.bsi.bund.de/: Bundesamt für Sicherheit in der Informationstechnik

Gliederung

1. Einführung
2. Angriffe
3. Viren
4. Firewalls
5. Betriebsvereinbarungen
6. Schlussbetrachtungen

Schädigungen von Unternehmen durch Hackerangriffe

- Durch Spionage können Firmengeheimnisse (Angebote, Knowhow) verraten werden.
- Durch Sabotage kann der Firmenbetrieb nachhaltig gestört werden.
- Durch Vertrauensschwund bei Verbrauchern können IT-Zukunftsmärkte zusammenbrechen.

Angriffe

- Ausspähen von Passwörtern (Eindringen in fremde Rechner)
- Ausspähen von Bankpinnummern (Betrug)
- Ausspähen von Firmengeheimnissen (Spionage)
- Zerstörung von Daten und Systemen (Vandalismus)
- Ausgabe von Fehlmeldungen
- Systeme übernehmen oder für Abgriffe vorbereiten
- Viren verbreiten
- Denial-of-Service-Attacken (DoS) durchführen

Angriffswege

- Viren, Würmer, Trojanische Pferde
- Gefälschte Rechneradressen
- Unsicherer Dienste
- Ausnützen von Sicherheitslücken

Angreifer

- Schüler und Studenten
- Hacker aus der Computer-Untergrundszene
- Herkömmliche Kriminelle
- Industriespione
- Mitarbeiter des eigenen Unternehmens

Angriffsschutz

- Virenscanner:
  Viren, Würmer, Trojanische Pferde
- Firewalls:
  risikobehaftete Dienste, Sicherheitslücken
- Verschlüsselungen (Kryptographie):
  unsichere Nachrichtenübertragungen
- Betriebsvereinbarungen:
  eigene, unzuverlässige Mitarbeiter

Merkmale von Viren

Computerviren sind Programme, die

- ihre bösartigen Funktionen verbergen
- sich vervielfältigen
- u.U. mutieren

Virentypen

- Boot-Viren
- System- oder Cluster-Viren
- Programm-Viren
- Polymorphe-Viren
- Retro-Viren
- Daten-Viren

Im weiteren Sinne:

- Trojanische Pferde
- Würmer
- Hoax

Aufgaben von Firewalls

- Ermöglichen des ungestörten Zugriffs der Nutzer des internen Netzes auf externe Netze Benutzerkontrolle
- Aufbau eines Schutzes des internen Netzes vor externen Übergriffen

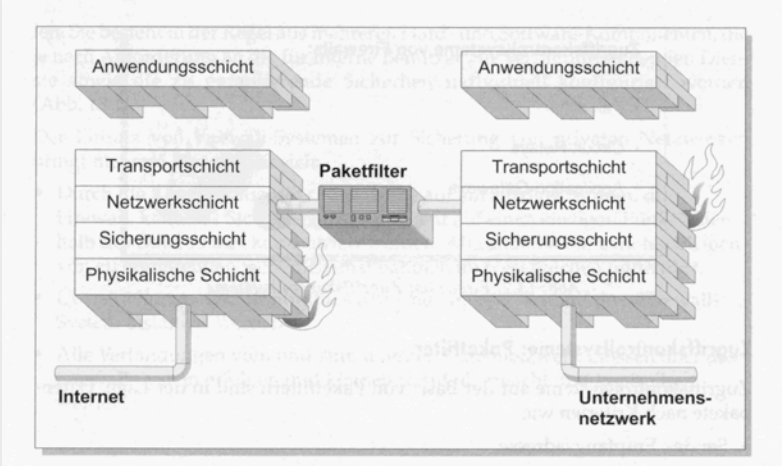
Funktionen einer Firewall

- Definition eines einigen Datendurchflusspunktes
- Fernhalten nichtautorisierter Benutzer vom Netz
- Verbieten anfälliger Dienste
- Schutz vor IP-Datenmanipulationen und Routing-Angriffen
- Bereitstellung einer Reihe von Überwachungs- und Alarmfunktionen
- Plattform für nichtsicherheitsrelevante Internet-Funktionen

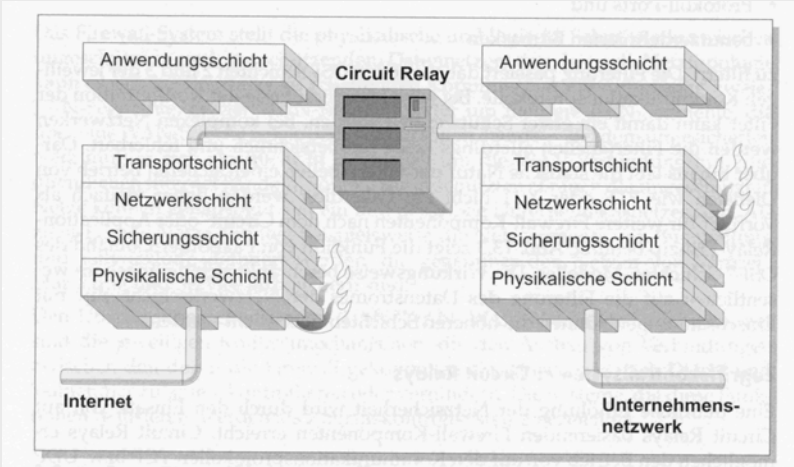
Aktivitäten von Firewalls

- Kontrolle der Dienste
  - Festlegung der Dienste, auf die vom Netz zugegriffen werden kann
  - Filtern des Datenverkehrs
- Benutzerkontrolle
- Verhaltenskontrolle
  - Zugriffe werden nur auf bestimmte Informationen auf dem lokalen Web-Server beschränkt

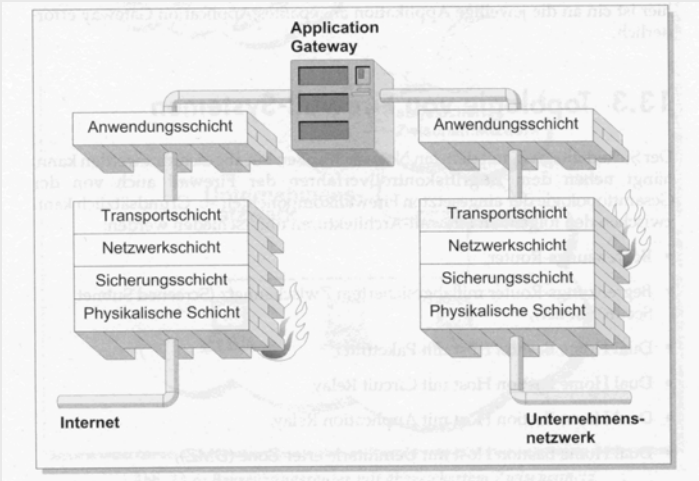
Firewall: Paketfilter



Firewall: Circuit Relais



Firewall: Application-Gateway



Grenzen der Schutzfunktionen von Firewalls

Firewalls bieten keinen Schutz:

- wenn die Firewall umgangen wird z.B. durch ein Modem
- vor internen Angriffen
- vor Angriffen, oberhalb der Anwendungsschicht, dem Anwendungsbereich, z.B. vor vireninfizierten Programmen

Konzepte zur Einrichtung einer Firewall

- Alles, was nicht verboten ist, ist erlaubt!
  - Vorteil:
    - Beeinträchtigt den eingefahrenen Betrieb wenig
  - Nachteil:
    - Riskante Dienste sind erlaubt, wenn vergessen wurde, sie zu verbieten
    - Das System muss ständig beobachtet werden, um die Verbotsliste zu aktualisiern
- Alles, was nicht erlaubt ist, ist verboten!
  - Vorteil:
    - Keine risikobehafteten Dienste können auf das interne Netz zugreifen
  - Nachteil:
    - Bei fehlerhafter oder schlecht konfigurierter Firewall kann das EDV-System zusammenbrechen

Konzepte für den Betrieb einer Firewall

- Der Zugriff von aussen auf die Rechner innerhalb eines Unternehmens soll nur durch Berechtigte erfolgen und auf das notwendige Maß eingeschränkt werden.
- Alle Dienste, die Passworte im Klartext über das Netz verschicken, werden blockiert und durch Varianten mit verschlüsselten Passworten ersetzt.
- Die Firewall soll dem Benutzer nur dann auffallen, wenn er etwas Unerlaubtes tun will.

Resumée (Firewalls)

- Firewalls garantieren keine Sicherheit!
- Firewalls reduzieren lediglich das Risiko eines bösartigen Zugriffs!

5. Betriebsvereinbarung Sicherheitsarchitektur

- Unternehmensrichtlinien
  - ordnungsgemäße Benutzung von Computersystemen
- Risikoanalyse
  - Was wird wie gut vor wem geschützt?
- Sicherheitsrichtlinien
  - für Mitarbeiter, Hardwaresysteme, Software, Daten, Datenübertragungen

Das Wahlpflichtfach „Datenschutz und Datensicherheit“

- NN:Vorlesung/Übung: Sicherheit in Netzwerken (Grundlagen, Spezielle Software)
- NN:Vorlesung/Übung: Kryptographie und Krypto-analyse
- Ass. Helmer, DSB, FhG St. Augustin: Vorlesung: Datenschutzrechte (juristische Aspekte)
- Langemeier/Schwarzer: Praktikum: Netzwerk-Sicherheit (Schwachstellenanalyse)
- Langemeier/Schwarzer: Praktikum: Programmierung spezieller Probleme zur Datensicherheit in Java
- Langemeier/Schwarzer: Seminar: Spezielle Probleme der Netzwerkorganisation und des Datenschutzes