IT Sicherheit

00 Wiederholung

Hash Funktionen

- Unidirektionale, deterministische Funktionen zur Komprimierung von Eingangsdaten beliebiger Länge auf Ausgangsdaten fixer Länge

- Beispiele:
  - MD5, SHA-1
  - SHA-2 (SHA-256, SHA-512)
  - SHA-3

- Kollisionen: Mehrere, unterschiedliche Eingangsdaten liefern die selben Ausgangsdaten

Hash Funktionen

- Avalanche effect: “Minimale Änderung der Eingangsdaten führt zu maximaler Änderung der Ausgangsdaten”
  - SHA-1(abc) = a9993e364706816aba3e25717850c26c9cd0d89d
  - SHA-1(abd) = cb4cc28df0fdbe0ecf9d9662e294b118092a5735

- Anwendungsfälle:
  - Einfacher/Schneller Vergleich von Daten
  - Prüfwerte (Integrität von Daten feststellen)

Verschlüsselung

- Bidirektionale Funktion, welche Eingangsdaten unter der Verwendung eines Schlüssels in Ausgangsdaten überführt (=Verschlüsselung).
- Mit Hilfe des Schlüssels können die Ausgangsdaten wieder in die Eingangsdaten überführt werden, ohne Schlüssel ist dies nicht möglich (=Entschlüsselung).

- Varianten:
  - Symmetrisch
  - Asymmetrisch

Verschlüsselung - Symmetrisch

- Es wird der selbe Schlüssel für die Verschlüsselung und Entschlüsselung verwendet.

- Vorteile:
  - Schnell
  - Einfachere Implementierung

- Nachteile:
  - Wie Schlüssel austauschen?
  - Alle Beteiligten kennen Schlüssel (Authentizität der Nachricht?)

Verschlüsselung - Asymmetrisch

- Es warden für Ver- und Entschlüsselung unterschiedliche Schlüssel eingesetzt (üblicherweise ist einer davon privat und der andere öffentlich)

- Vorteile:
  - Es gibt einen öffentlichen Schlüssel – Austausch sehr einfach
  - Authentizität von Nachrichten kann gewährleistet werden

- Nachteile:
  - Langsam
  - Komplexere Implentierungen notwendig

Verschlüsselung - Kombination

- Oft werden symmetrische und asymmetrische Verschlüsselung kombiniert, um die Vorteile aus beiden Welten nutzen zu können

- Beispiel:
  - TLS – Asymmetrische Verschlüsselung wird verwendet, um symmetrischen Schlüssel auszutauschen. Kommunikation wird dann mit symmetrischen Schlüssel verschlüsselt. Symmetrischer Schlüssel wird regelmäßig getauscht.

Phishing

- Phishing Quiz

- Betrugsmasche, bei der offizielle Emails/Websites nachgebaut warden um an sensible Informationen zu kommen

- Wie kann Phishing erkannt werden?

Zwei-/Mehr-Faktor Authentifizierung

- Authentifizierung = Nachweis einer Identität

- “Something you know” - Passwort / PIN
- “Something you have” – Smartphone / Hardware Token / Token List / OTP App
- “Something you are” – Fingerabdruck / Iris / Handvene
- “Somewhere you are” – IP Adresse / Netzwerk / GPS (Galileo) Standort / Land
- “Sometimes you are” – Zeitfenster

Zwei-/Mehr-Faktor Authentifizierung

- Welche Kombination von Faktoren macht in welchen Szenarien Sinn?

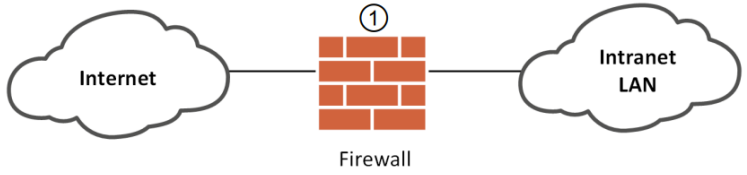
- Welche Kombination von Faktoren macht keinen Sinn?

Firewalls

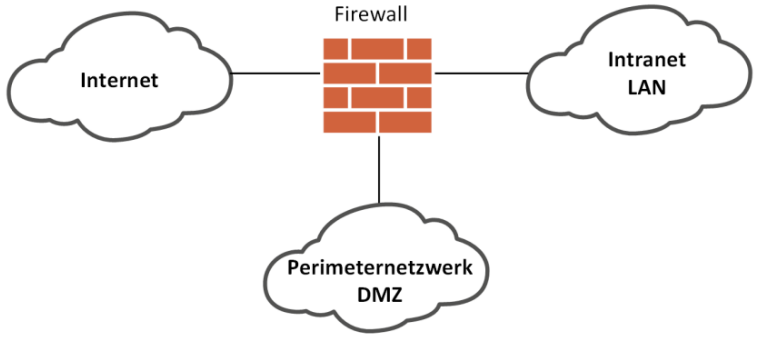
- Aufgabe: Zugriff auf Systeme/Netzwerke nur an Hand von festgelegten Regeln zulassen (Policies)
- Hardware-Appliance / Software-Appliance
- Appliance: Speziell gehärtetes Betriebssystem zur Erhöhung der Sicherheit

Firewalls

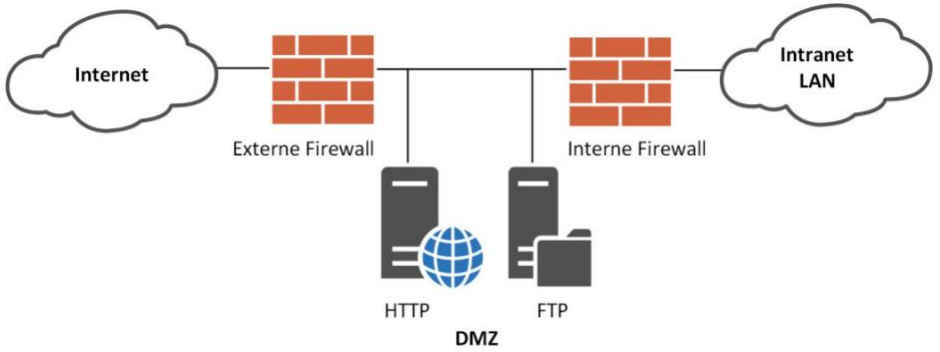
- Platzierung: “Gateway” zu einen Netzwerk (Trennung zw. Internet und internem Netz/zw. Internen Netzen/zw. DMZ und internen Netzen)



Einfache Firewall ohne DMZ



Firewall mit mehreren Interfaces



Mehrstufige Firewall mit jeweils einem internen und einem externen Interface

Firewalls

- Arten von Firewalls:
  - State-less
  - State-full
  - Application-Level

- OSI-Ebene:
  - Layer 3
  - Layer 4
  - Layer 7

Firewalls – State-less

- Paketfilter: Statische Filterung von Paketen aufgrund von Regeln
- Operiert auf Layer 3 und 4 des OSI Modells
- ACL: <Quelle – Host/Subnet/Port> <Ziel – Host/Subnet/Port> <Aktion>
- Beispiele:
  - Any Any 192.168.10.1/32 tcp/80,tcp/443 Allow
  - 192.168.10.1/32 Any 192.168.20.2/32 tcp/3306 Allow
  - Any Any Any Any Deny

Firewalls – State-full

- Zusätzlich zum Paketfilter wird der jeweilige Kontext berücksichtigt
- Zusätzlich zur ACL gibt es eine State Table
- Operiert auch auf Layer 3 und Layer 4 des OSI Modells
- Ermöglicht aufgrund der State Table einen Schutz vor komplexeren Angriffen

Firewalls – Application level

- Analysiert auch höhere Ebenen des OSI Modells

- Beispiele:
  - Webfilter (inkl. SSL Inspection)
  - Erkennung von Protokollen auf untypischen Ports (SSH auf Port 443)

Firewalls – NAT

- NAT = Network Address Translation
- Wurde ursprünglich entwickelt, um zu verhindern, dass zu wenige IPv4 Adressen verfügbar sind
- Dient dem Verstecken von Ips/Netzwerken hinter anderen Ips/Netzwerken

VPN – Virtual Private Network

Zugriff auf Firmennetzwerk ohne physikalisch vor Ort zu sein

- Site – 2 – Site Tunnel
- Remote-Access Tunnel