Informationssicherheit, Datenschutz, Urheberrecht

ISDS

Themenübersicht

06
Verschlüsselung Signatur

Grundlagen

Symmetrische & Asymmetrische Verschlüsselung

Verschlüsselungs-protokolle und ihre Anwendung

Signaturen

07
IDS, IPS, Firewalls

Intrusion Detection System

Intrusion Prevention System

Honeypot

Firewall

Sandbox

08
Proaktive Sicherheit

Defensive Programmierung

Gehärtete Betriebssysteme

Patches

Vulnerability Assessment

Aktive Sicherheit von Netzwerk-komponenten

09
Urheberrecht

Der Urheber

Das Werk

Urheber-persönlichkeitsrecht

Verwertungsrechte

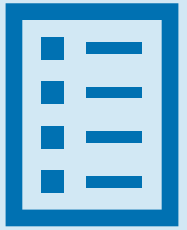
Nutzungsrechte

Ausnahmen

Dauer

Recht am eigenem Bild

10
Lernstands-messung



Agenda

1. Intrusion Detection System
2. Intrusion Prevention System
3. Honeypot
4. Firewall
5. Sandbox

1 Intrusion Detection System

1 Intrusion Detection System

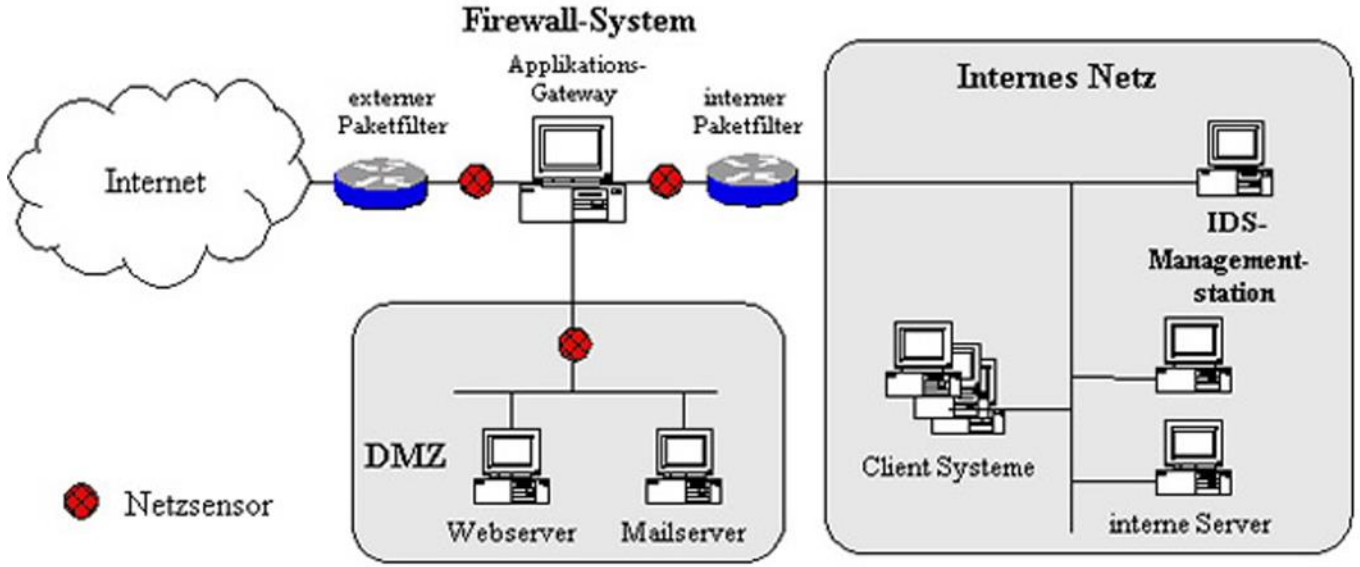
- Ein Intrusion-Detection-System (IDS) ist, ein System zur Erkennung eines Einbruchs/Eindringens in das Datenverarbeitungssystem.
- Zur Erkennung werden der Netzwerkverkehr (network-oriented) oder die Zugriffe auf einem Server (host-oriented) beobachtet und mit gespeicherten Angriffsmustern (misuse detection) oder gespeicherten Benutzerverhaltensmuster (anomaly detection) verglichen.

1 Intrusion Detection System

- Bei Erkennung eines Angriffes wird eine Aktion ausgeführt, wie z.B. ein Alarm ausgelöst.
- Ziel des IDS ist die Erkennung von Angriffen und die Einschränkung von Angriffsmöglichkeiten
- Es können nicht alle Angriffe erkannt werden.
- Die Analyse und Bewertung von Angriffen erfordert einen hohen personellen Aufwand

1 Intrusion Detection System

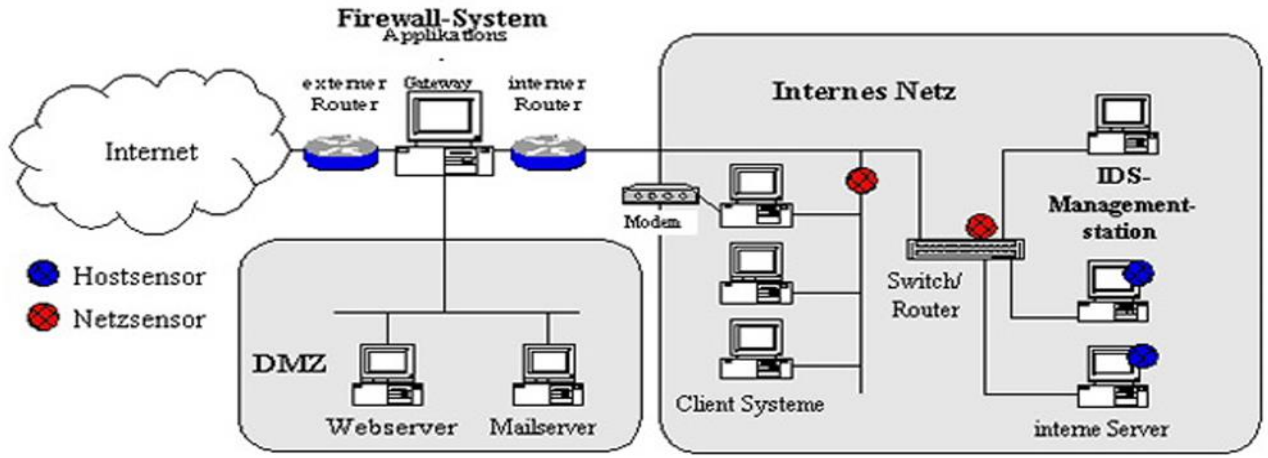
- Platzierung eines IDS erfolgt in Abhängigkeit vom Einsatzzweck
  - Vor der Firewall und dem zu schützenden Netz
    - Das IDS sieht, sofern bekannt, sämtliche Angriffe von außen.



Quelle: BSI

1 Intrusion Detection System

- Platzierung eines IDS erfolgt in Abhängigkeit vom Einsatzzweck
  - Hinter der Firewall im geschützten Netz
    - Das IDS für Angreifer nicht einfach erkennbar.
    - Nur erfolgreiche Angriffe werden registriert
    - Sicherheitsverletzungen von innen können erkannt werden.



Quelle: BSI

2 Intrusion Prevention System

2 Intrusion Prevention System

- Ein Intrusion Prevention System (IPS), ist in der Lage, Angriffe auf Netzwerke oder Computersysteme zu erkennen und automatische Abwehrmaßnahmen zu ergreifen.
- IPS werden wegen des hohen personellen Arbeitsaufwands bei der Analyse und Bewertung der Angriffe eingesetzt.
- Sie leiten programmgesteuert Sicherheitsmaßnahmen (Umkonfigurierung, Neuparametrisierung von Firewalls, Abschalten von Servern etc.).

2 Intrusion Prevention System

- Abwehrmaßnahmen eines IPS:
  - Alarmierung des Administrators
  - Trennen oder Zurücksetzen der Verbindung
  - Datenverkehr von einer Quelle oder zu einem bestimmten Ziel unterbinden
  - Automatische Rekonfiguration der Firewall, um die Verbindung zu unterbrechen

2 Intrusion Prevention System

- Arten eines IPS
  - Das Host-basierte IPS ist direkt auf dem zu schützenden System installiert. Es analysiert alle empfangenen und gesendeten Daten und die vom System selbst bereitgestellten Daten.
  - Netzwerk-basierte IPS überwachen direkt den Netzverkehr und sind als separates Gerät oder integriert in eine Firewall inline installiert. Sie können vor Angriffen über das Netzwerk schützen
- Neben Intrusion Prevention Systemen, die als Standalone-Geräte konzipiert sind, existieren Firewall-Systeme, in denen die IPS Funktion direkt integriert ist. (Keine Aufwendige Kommunikation zwischen FW und IPS notwendig.)

3 Honeypot

3 Honeypot

- Als Honeypot wird in der IT ein Sicherheitsmechanismus bezeichnet, mit dem Administratoren Hacker täuschen und Cyberattacken ins Leere laufen lassen.
- Ein Honeypot kommt in der Regel als Ergänzung zu anderen IT-Sicherheitskomponenten wie dem Intrusion-Detection-System (IDS) und Firewalls zum Einsatz.
- Ein solcher Honigtopf simuliert Netzwerkdienste oder Anwendungs-programme, um Angreifer anzulocken und das Produktivsystem vor Schäden zu schützen.
- Da Honeypots im Normalbetrieb keine Funktion übernehmen, stellt jede Aktivität in diesen Kontrollsystemen einen potenziellen Angriff dar.

3 Honeypot

- Honeypots werden technologisch mit serverseitiger und clientseitiger Technologien eingerichtet.
- Serverseitiges Honeypotting:
  Die Grundidee eines serverseitigen Honeypots ist es, Angreifer in isolierte Bereiche eines IT-Systems zu locken und so von kritischen Netzwerkkomponenten fernzuhalten. Darüber hinaus bieten Honeypots die Möglichkeit, das Vorgehen von Angreifern zu tracken.

3 Honeypot

- Honeypots werden technologisch mit serverseitiger und clientseitiger Technologien eingerichtet.
- Clientseitiges Honeypotting:
  Ein clientseitiger Honeypot imitiert eine Anwendungssoftware, die Serverdienste in Anspruch nimmt. Das Paradebeispiel ist die Simulation eines Browsers, der gezielt unsichere Webseiten besucht, um Daten über Sicherheitsrisiken zu sammeln.

4 Firewall

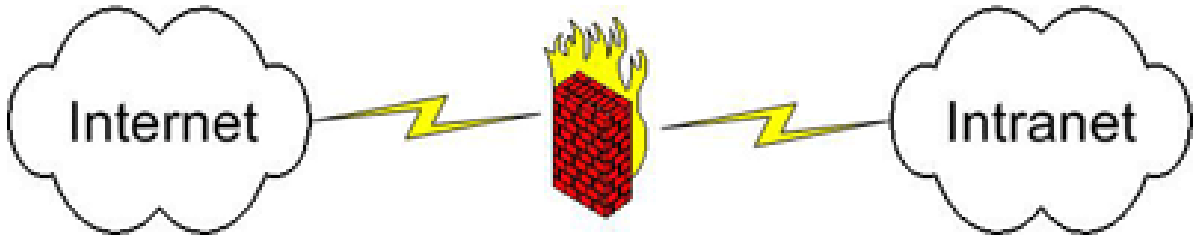
4 Firewall

- Firewalls schützen Netzwerke oder einzelne Computersysteme vor unerwünschten Netzwerkverkehr
- Jede Firewall basiert auf eine Softwarekomponente
- Überwacht den Datenverkehr und entscheidet anhand von festgelegten Regeln
- Eine Firewall soll nicht Angriffe erkennen sondern Regeln für den Datenverkehr umsetzen
- Unterscheidung zwischen Personal Firewall (Desktop Firewall) und externer Firewall (Netzwerk- oder Hardware-Firewall)

4 Firewall

Bastion-Host

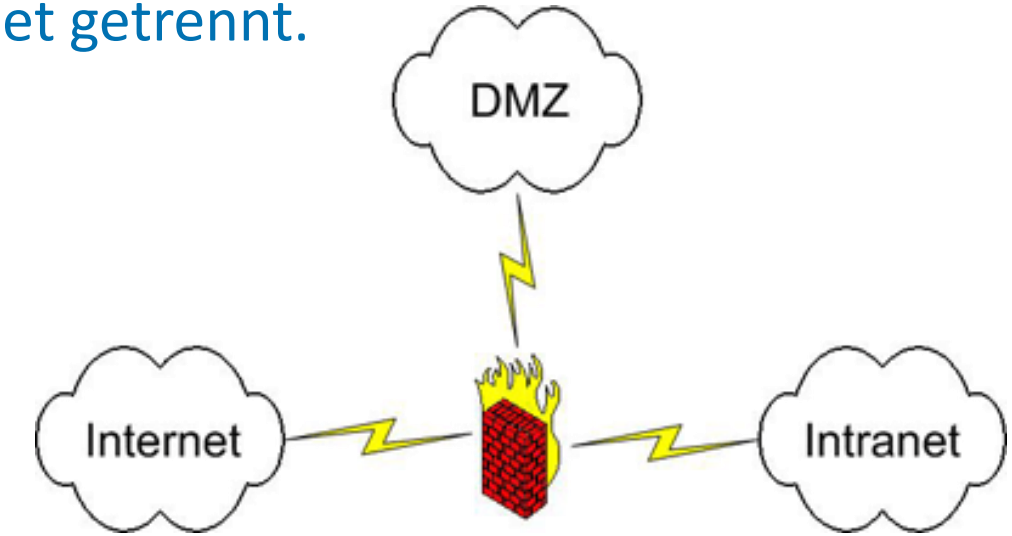
- Ein Bastion-Host ist der Hauptkontaktpunkt, über den Clients von internen Netzwerken auf das Internet zugreifen.
- Der Bastion-Host ist als Schutz vor Angriffen auf das interne Netzwerk und zur Kontrolle des ausgehenden Datenverkehrs konzipiert.
- Ein Bastion-Host wird normalerweise bei kleineren Netzwerken eingesetzt, die keine öffentlichen Server bereitstellen.



4 Firewall

Abgeschirmtes Subnetz (Screened Subnet)

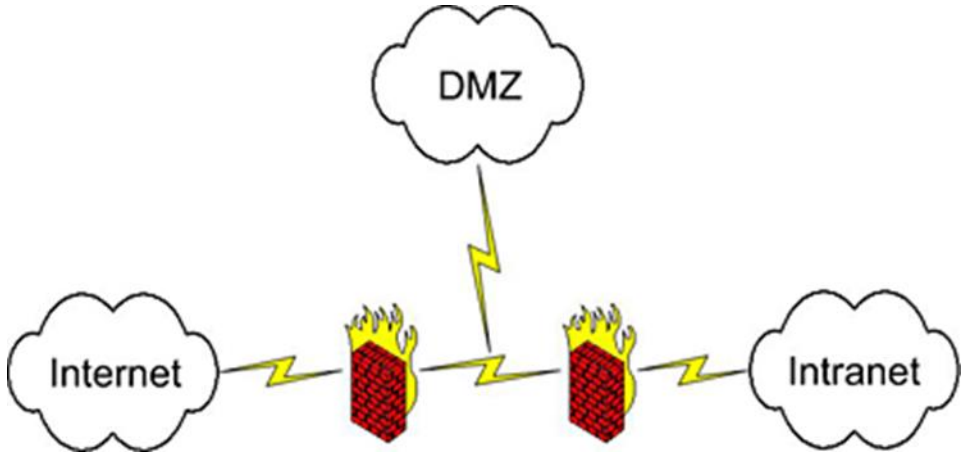
- Eine Firewall mit 3 Netzwerkkarten (Triple Home Firewall).
- Ein Server der öffentlichen Service anbietet, wird in der DMZ (demilitarisierte Zone) platziert.
- Die DMZ ist vom internen Netzwerk und dem Internet getrennt.
- Wenn die Firewall kompromittiert wird hat der Angreifer nicht zwangsweise Zugriff auf das Intranet



4 Firewall

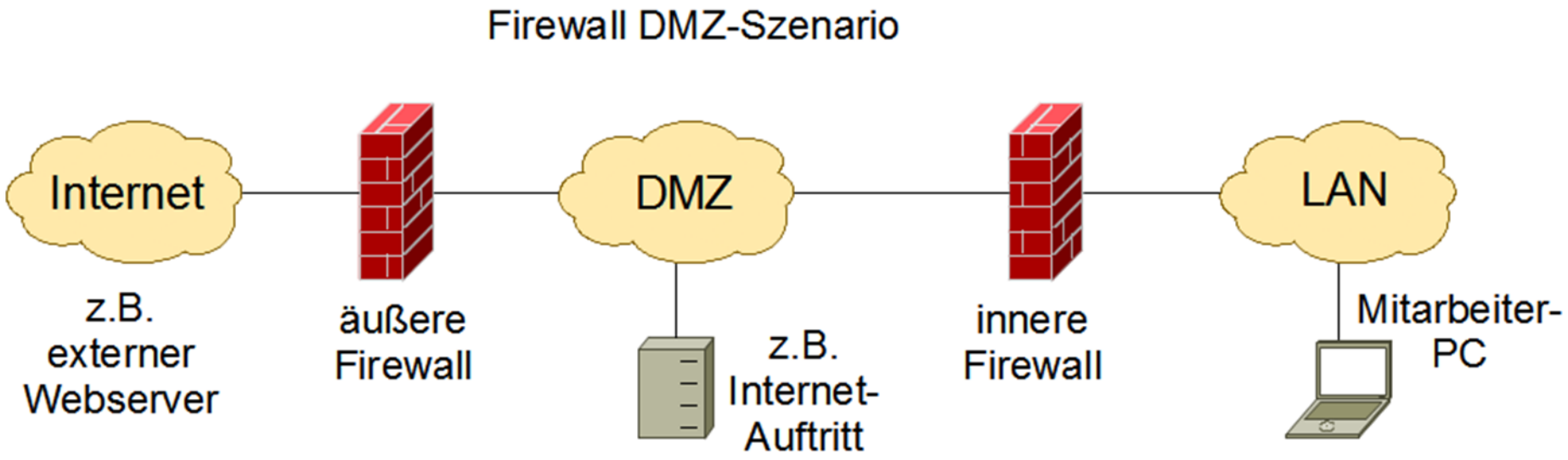
Doppelte Firewall (Dual Firewall)

- Ein abgeschirmtes Netzwerk (DMZ), in dem die öffentlichen Server/Dienste zur Verfügung gestellt sind, wird zwischen zwei Firewalls platziert
- Dadurch gibt eine zusätzliche Schutzschicht für das interne Netz
- Sollte der Angreifer die erste Firewall überwunden haben so schützt eine weitere Firewall das Intranet



4 Firewall

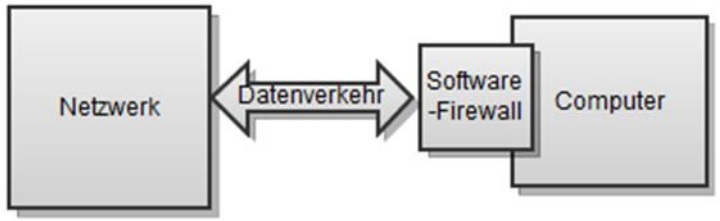
Doppelte Firewall (Dual Firewall)



4 Firewall

Software-Firewalls

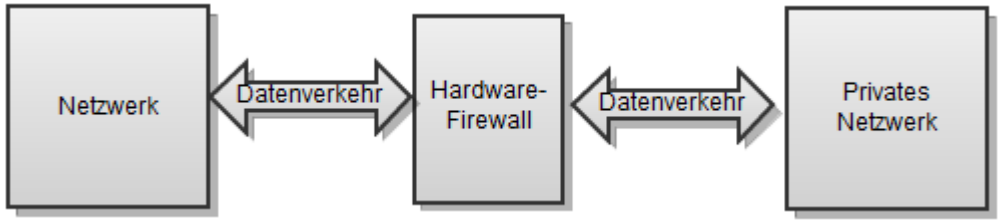
- Eine Software-Firewall ist eine Software, die auf dem System läuft, das sie beschützt.
- Daher kann die Firewall auch nur den Datenverkehr zwischen Computer und verbundenen Netzwerken überwachen.



4 Firewall

Hardware-Firewalls

- Hardware-Firewalls sind auf einem externen System installiert und beobachten den Datenverkehr zwischen zwei Netzwerken.
- Daher können sie alle Verbindungen zwischen diesen Netzen überwachen.
- Hierbei ist der Begriff „Hardware-Firewall“ unglücklich gewählt, da es sich auch um Software handelt, die aber nicht auf dem System/den Systemen installiert ist, das sie überwacht, sondern auf einem speziell dafür vorgesehenen Computer.



4 Firewall

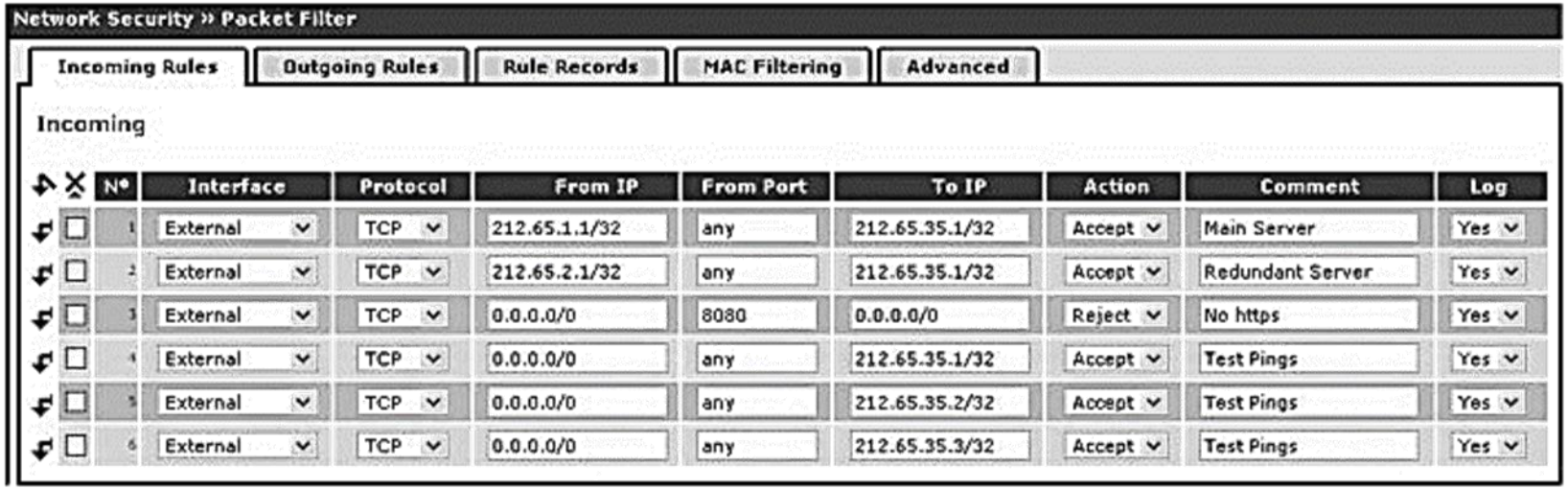
Strategien

- Firewall-Strategie: Alles sperren
  - Alles ist gesperrt. Bekannte sichere und erwünschte Vorgänge werden freigegeben.
  - Diese Variante ist sehr sicher. Allerdings erfordert sie eine aufwendige Konfiguration der Firewall.
- Firewall-Strategie: Alles freigeben
  - Alles ist freigegeben. Bekannte unsichere und unerwünschte Vorgänge werden gesperrt.
  - Diese Variante ist relativ komfortabel aber unsicher.

4 Firewall

Regeln

- Firewall Regeln werden in der Reihenfolge wie sie in der „Regeltabelle“ abgelegt sind abgearbeitet.
- Die erste zutreffende Regel wird angewendet und alle nachfolgenden werden nicht weiter betrachtet.



4 Firewall

Regeln

- ALLOW oder PASS (Erlauben)
  - Das Paket ist erlaubt und wird durchgelassen.
- DENY oder DROP (Verwerfen)
  - Das Paket wird verworfen. Der Absender erhält keine Nachricht darüber, dass sein Verbindungsversuch blockiert wurde.
- REJECT (Ablehnen)
  - Das Paket wird verworfen und dem Absender wird mitgeteilt, dass die Verbindung abgelehnt wurde.
- FORWARD oder PERMIT (Erlauben)
  - Die Netzwerkanfrage ist erlaubt und wird weitergeleitet, was die Möglichkeit einer Umleitung auf eine vom Administrator festgelegte Netzwerkadresse einschließt.

5 Sandbox

5 Sandbox

- Eine Sandbox ist ein vom System abgeschotteter Bereich, in dem sich potentiell unsichere Aktionen ausführen lassen.
- Die Sandbox ist von den Ressourcen des Systems getrennt und stellt der auszuführenden Software eine spezielle Laufzeitumgebung zur Verfügung.
- In diesem Bereich wird die potentiell gefährliche Datei geöffnet oder installiert. Das Verhalten der Dateien bzw. Software kann so beobachtet bzw. auf unerwünschtes Verhalten überprüft werden.
- Ziel des Einsatzes ist der Schutz des IT-Systems.

5 Sandbox

- Ansätze zur Realisierung
  - OS Emulation: dabei wird in einer virtuellen Maschine ein Gast Betriebssystem installiert. Die Hardware des Host Systems kann dann optional mit den Gast Systemen geteilt werden, beispielsweise Zugriff auf USB Sticks oder die Freigabe von Verzeichnissen auf der Harddisk des Hosts.
  - Applikation Sandbox: im Gegensatz zu den virtuellen Maschinen der OS Emulation und deren generellem Ansatz, bietet eine Application Sandbox spezifischen Schutz für einzelne Applikationen.

VIELEN DANK!

Quellen

- Grafiken:
- https://storyset.com