**Lernzettel 7: Netzwerksicherheit**

**1. Bedrohungsmodell**

* **Ziel eines Angreifers:** Angreifer können nicht nur an Kommunikationsverbindungen, sondern auch an Endgeräten interessiert sein, um z.B. Bots zu installieren.
* **Fähigkeiten eines bösartigen Knotens:** Kann Nachrichten lesen, Senderadressen fälschen und versuchen, ungesehene Nachrichtenfelder zu erraten.

**Lernbrücke:** Während traditionelle Sicherheitsansätze oft nur die Kommunikationskanäle schützen, müssen auch Endpunkte gesichert werden, um umfassenden Schutz zu gewährleisten.

**2. Firewalls**

* **Funktionalität:** Firewalls kontrollieren den Datenverkehr zwischen Netzen unterschiedlicher Vertrauenswürdigkeit und setzen Sicherheitsrichtlinien durch.
* **Grundprinzipien:**
  + **Paketfilter:** Überprüfen IP-Adressen und Ports und entscheiden, ob ein Paket durchgelassen wird.
  + **Circuit-Level Gateway:** Agiert auf der Transportschicht, ersetzt die Absenderadresse und verbirgt die interne Netzstruktur.
  + **Application-Level Gateway:** Funktioniert als Proxy auf Anwendungsebene, analysiert Protokolle und Inhalte.

**Lernbrücke:** Unterschiedliche Firewall-Typen bieten unterschiedliche Schutzmechanismen, von der einfachen Paketfilterung bis zur komplexen Inhaltsanalyse auf Anwendungsebene.

**3. Firewall-Architekturen**

* **Dual-Homed Firewall:** Verfügt über zwei Netzwerkkarten, eine für das interne und eine für das externe Netzwerk, wodurch eine sichere Trennung gewährleistet wird.
* **Screened Host:** Kombiniert Paketfilter und Bastion Host, bietet hohe Flexibilität, aber Pakete können dennoch ins interne Netz gelangen.
* **Screened Subnet:** Schützt ein demilitarisiertes Subnetz (DMZ) sowohl nach innen als auch nach außen, indem die Firewall den Verkehr in und aus der DMZ filtert.

**Lernbrücke:** Die Wahl der richtigen Firewall-Architektur hängt von den spezifischen Sicherheitsanforderungen und der Netzwerkinfrastruktur ab.

**4. Vorteile und Grenzen von Firewalls**

* **Vorteile:**
  + Erhöhte Netzwerksicherheit durch differenzierte Zugriffskontrollen.
  + Möglichkeit der Protokollierung und Erkennung von Angriffsmustern.
* **Grenzen:**
  + Kein Schutz vor internen Angriffen oder vor Verschlüsseltem, was durch die Firewall hindurchgeht (z.B. HTTPS).
  + Erfordern tiefgehendes Wissen über Netzwerke und Sicherheitsstrategien.

**Lernbrücke:** Firewalls sind ein wichtiges Werkzeug zur Netzwerksicherheit, jedoch keine Allheilmittel; sie müssen in ein umfassendes Sicherheitskonzept integriert werden.

**5. Technische Umsetzung von Firewalls**

* **Paketfilter:** Arbeiten zustandslos und basieren auf statischen Regeln. Sie sind einfach und effizient, aber weniger flexibel.
* **Circuit-Level Gateways:** Vermitteln Verbindungen auf der Transportschicht und bieten anwendungsunabhängigen Schutz.
* **Application-Level Gateways:** Erfordern spezifische Proxies für verschiedene Anwendungen, bieten dafür aber granulare Kontrolle.

**Lernbrücke:** Die technischen Unterschiede der Firewall-Typen beeinflussen deren Einsatzgebiete und Leistungsfähigkeit. Je nach Bedarf können einfache Paketfilter ausreichend sein oder komplexe Application-Level Gateways benötigt werden.