**Lernzettel 4: Typische Angriffstechniken**

**1. Grundlagen**

* **Angriffstechniken:** Nutzen technische oder menschliche Schwachstellen aus, z.B. Implementierungsfehler, menschliche Nachlässigkeit oder konzeptionelle Fehler.
* **Bedrohungsabwehr:**
  + **Verhinderung:** Einsatz von stark typisierten Programmiersprachen, Code-Verifikation.
  + **Erkennung und Behebung:** Statische Analyse, Virenscanner, Intrusion Detection Systeme.
  + **Schadensbegrenzung:** Sandboxing, um potenzielle Schäden zu isolieren.

**Lernbrücke:** Der Schutz vor Angriffen erfordert eine Kombination aus präventiven Maßnahmen, effektiver Erkennung und gezielter Schadensbegrenzung.

**2. Schadsoftware**

* **Definition:** Programme, die verborgene und schädliche Funktionen ausführen.
* **Typen:**
  + **Trojanisches Pferd:** Täuscht nützliche Software vor, enthält aber schädliche Zusatzfunktionen wie Datenmanipulation.
  + **Viren:** Infizieren Wirtsprogramme und breiten sich durch Nutzeraktionen wie das Öffnen von E-Mails aus.
  + **Würmer:** Selbstreplizierende Programme, die keinen Wirtscomputer benötigen und sich oft über Netzwerke verbreiten.

**Lernbrücke:** Während Trojaner auf Täuschung beruhen, benötigen Viren Wirtsprogramme, und Würmer verbreiten sich eigenständig über Netzwerke.

**3. Bot-Netze**

* **Definition:** Netzwerke von infizierten Computern, die unter der Kontrolle eines Angreifers stehen.
* **Funktion:** Können für DDoS-Angriffe, Spam-Versand oder das Ausführen schädlicher Software verwendet werden.
* **Abwehr:** Verkehrsanalyse, um den Botnetz-Server zu identifizieren und den Angriff zu stoppen.

**Lernbrücke:** Bot-Netze sind eine besonders gefährliche Form von Angriffen, da sie eine Vielzahl von infizierten Computern gleichzeitig einsetzen können.

**4. Mobiler Code**

* **Definition:** Programme, die auf einem entfernten Rechner generiert und auf einem Gastrechner ausgeführt werden, z.B. mobile Apps.
* **Bedrohungen:**
  + **Für den mobilen Code:** Abhören während der Übertragung, Modifikation durch den Gastrechner.
  + **Für den Gastrechner:** Unautorisierte Zugriffe, DoS-Attacken.
* **Gegenmaßnahmen:** Verschlüsselung, Sandboxing, Beschränkung der Zugriffsrechte.

**Lernbrücke:** Der Schutz vor mobilen Bedrohungen erfordert sowohl die Sicherung des Codes während der Übertragung als auch den Schutz des Gastrechners vor möglichen Angriffen durch den Code.

**5. Angriffe zur Ermittlung von Passwörtern**

* **Methoden:**
  + **Brute-Force-Angriffe:** Systematisches Ausprobieren von Passwörtern.
  + **Social Engineering:** Manipulation von Personen, um sensible Informationen zu erhalten.
* **Schutzmaßnahmen:** Verwendung von starken, komplexen Passwörtern, Zwei-Faktor-Authentifizierung, Vorsicht bei der Weitergabe von Informationen.

**Lernbrücke:** Angriffe auf Passwörter kombinieren oft technische Methoden mit der Manipulation von Personen, um Sicherheitsbarrieren zu überwinden.