

Handout: Malware – Bedrohung aus dem Netz

1. Was ist Malware?

- **Definition:** Malware steht für „malicious software“, also schädliche Software, die entwickelt wurde, um Computer, Netzwerke oder Daten zu manipulieren, zu stehlen oder zu zerstören.
 - **Ziele:**
 - Daten stehlen (z.B. Passwörter, Bankdaten).
 - Systeme stören oder zerstören.
 - Kontrolle über Geräte oder Netzwerke erlangen.
 - **Verbreitungswege:** E-Mails, infizierte Websites, Software-Downloads, USB-Sticks.
-

2. Arten von Malware

- **Virus:** Infiziert Dateien und verbreitet sich beim Öffnen; kann Daten verändern oder löschen.
 - **Wurm:** Verbreitet sich selbstständig über Netzwerke; verursacht oft Netzwerküberlastung.
 - **Trojaner:** Tarnung als legitime Software, führt im Hintergrund schädliche Aktionen aus.
 - **Ransomware:** Verschlüsselt Daten und verlangt Lösegeld für deren Freigabe.
 - **Spyware:** Überwacht das Verhalten des Nutzers und sammelt vertrauliche Daten.
 - **Adware:** Zeigt unerwünschte Werbung an und verfolgt das Nutzerverhalten.
-

3. Wie funktioniert Malware?

- **Infektionsmethoden:**
 - Phishing-E-Mails (Anhänge öffnen).
 - Infizierte Websites (Drive-by-Download).
 - Ausnutzung von Software-Schwachstellen.
 - **Ausführung:** Malware wird installiert und bleibt oft unentdeckt.
 - **Schaden:** Datenverlust, Identitätsdiebstahl, komplette Kontrolle über Systeme.
-

4. Verbreitungswege von Malware

- **E-Mail-Anhänge:** Gefälschte Nachrichten mit bösartigen Anhängen.
 - **Infizierte Websites:** Malware-Downloads durch den Besuch unsicherer Seiten.
 - **Unsichere Downloads:** Heruntergeladene Software aus nicht vertrauenswürdigen Quellen.
 - **Soziale Netzwerke:** Gefälschte Links oder Nachrichten zur Verbreitung von Malware.
-

5. Schutzmaßnahmen

- **Antiviren-Software:** Regelmäßige Scans und Updates, um bekannte Bedrohungen zu erkennen.
 - **Firewalls:** Schutz vor unberechtigtem Zugriff auf das Netzwerk.
 - **Updates und Patches:** Halte Software auf dem neuesten Stand, um Schwachstellen zu schließen.
 - **Sicheres Verhalten:** Keine verdächtigen E-Mails öffnen, nur vertrauenswürdige Downloads, sichere Websites besuchen.
-

6. Aktuelle Bedrohungen und Trends

- **Ransomware-as-a-Service (RaaS):** Ransomware wird von Kriminellen als Dienstleistung angeboten.
 - **Mobile Malware:** Angriffe auf Smartphones und Tablets nehmen zu.
 - **Internet of Things (IoT) Malware:** Zunahme von Angriffen auf vernetzte Geräte (z.B. Smart-Home-Systeme).
-

7. Fallbeispiele

- **WannaCry (2017):** Weltweiter Ransomware-Angriff, der Krankenhäuser und Unternehmen betraf.
 - **NotPetya (2017):** Verbreitete sich wie ein Wurm und zerstörte Systeme.
 - **Emotet (2018):** Trojaner, der über E-Mails verbreitet wurde und Bankdaten stahl.
-

8. Fazit

- Malware ist eine ernstzunehmende und **wachsende Bedrohung**.
- **Schutzmaßnahmen** wie Antivirensoftware, regelmäßige Updates und sicheres Nutzerverhalten sind unerlässlich.
- **Vorsicht und Achtsamkeit** bieten den besten Schutz vor Malware.