Übung 14 - Viren, Antivirenprogramm und Firewall

1. Was ist Malware?

Malware ist ein Sammelbegriff für schädliche Programme.

Dazu gehören:

- Viren
- Würmer
- Trojaner
- Ransomware
- Spyware
- Adware

2. Arten von Schadsoftware

Virus

Benötigt eine „Wirtsdatei“ und verbreitet sich durch Datenaustausch.

Wurm

Verbreitet sich selbstständig über Netzwerke.

Trojaner

Tarnt sich als nützliches Programm, enthält aber Schadcode.

Ransomware

Verschlüsselt Daten und verlangt Lösegeld.

Spyware

Spioniert Benutzerdaten aus.

Keylogger

Zeichnet Tastatureingaben auf.

3. Wie gelangen Viren auf den Computer?

- E-Mail-Anhänge
- Downloads
- Unsichere Webseiten
- USB-Sticks
- Fake-Updates
- Phishing

Auch Computer ohne Internet können über USB-Sticks infiziert werden.

4. Schäden durch Malware

- Datenverlust & Datendiebstahl
- Systemverlangsamung
- Erpressung
- Zugriff auf Kamera/Mikrofon
- Identitätsdiebstahl

5. Antivirenprogramme

Ein Antivirenprogramm schützt den Computer durch:

- Echtzeitschutz
- Regelmäßige Systemprüfung
- Erkennung von Virensignaturen
- Heuristische Analyse

5.1 Virensignaturen

Antivirenprogramme vergleichen Dateien mit bekannten Schadcodes.
Deshalb sind Updates wichtig.

5.2 Quarantäne

Infizierte Dateien werden isoliert gespeichert.

6. Firewall

Eine Firewall überwacht den Datenverkehr zwischen:

- Computer und Internet
- Zwei Netzwerken

Arten der Firewall

Software-Firewall	Auf dem Computer installiert.
Hardware-Firewall	Im Router integriert.

Aufgabe

- Blockiert unerlaubte Zugriffe
- Kontrolliert Programme
- Schützt vor Angriffen

7. Schutzmaßnahmen

Neben Antivirenprogramm und Firewall wichtig:

- Regelmäßige Updates
- Sichere Passwörter
- 2-Faktor-Authentifizierung
- Keine unbekannten Anhänge öffnen
- Backup erstellen