



Bedrohung: Schadsoftware

Inhalt: Bedrohung von Schadsoftware (Malware) und ihre Erscheinungsformen, Schutz vor Schadsoftware

Schadsoftware...



..., auch: Malware, umschreibt Programme, die Schaden anrichten oder unerwünschte Aktivitäten im digitalen Raum ausführen sollen, bspw. Datendiebstahl, Systemüberlastung

Arten von Malware

Viren



sich auf einem Gerät selbstständig vermehrende und verbreitende Programme, die Schaden an Programmen und Dateien anrichten

- Verbreitungswege: E-Mail-Anhänge, externe Geräte (USB, Festplatten etc.)
- **Schutz:** Anti-Viren-Softwares, E-Mail-Filter, aufgeklärter Umgang mit E-Mails und Hardware

Trojaner



sich als nützlich/"gutartig" tarnende Programme, die Schaden an Programmen und Dateien anrichten und Daten stehlen können

- Verbreitungswege: Besuch infizierter Webseiten, Phishing-E-Mails
- **Schutz:** Firewalls, Einschränkung der Nutzerrechte auf den Geräten

Würmer



sich im Netzwerk selbstständig verbreitende Programme, die Schaden an Programmen und Dateien anrichten

- Verbreitungswege: Netzwerk-Schwachstellen (veraltete Software etc.), mobile Geräte
- **Schutz:** Patch-Management, Kontrolle der Netzwerkaktivitäten, klare Sicherheitsrichtlinien

Ransomware



Schadsoftware, die Zugriff auf Dateien bzw. Systeme blockiert oder verschlüsselt und für die Wiederherstellung Lösegeld fordert

- Verbreitungswege: u.a. Phishing & Vishing, Social Engineering (menschliche Schwächen)
- **Schutz:** aufgeklärter Umgang mit E-Mails und -Anhängen, Firewalls, aktualisierte Sicherheitssoftware

Exkurs: Advanced Persistent Threats (APTs)

... sind hochentwickelte, langfristige Cyberangriffe, die auf bestimmte Organisationen oder Unternehmen abzielen

- Ablauf: Angreifer erkunden das Ziel, dringen durch Cyberangriffe ein, vermehren sich im Netzwerk, richten Schaden an (Datendiebstahl/Sabotage etc.), halten den Zugang aufrecht
- **Gefahr:** gut getarnte Aktivitäten, gezielter Angriff von Schwachstellen, verheerende (finanzielle) Schäden möglich

Für alle Arten von Malware gilt:



- regelmäßige Softwareaktualisierung
- regelmäßige Backups
- Sensibilisierung & regelmäßige Schulung

Gefördert durch:



Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

