

KONTROLLFRAGEN LEKTION 37: NETZWERKSICHERHEIT

1. Erklären Sie den Unterschied zwischen einem Computervirus und einem Computerwurm.
 - Das Computervirus verbreitet sich nur innerhalb des Computersystems. Das Computervirus ist zum Beispiel in einer Programmdatei, einer Skriptdatei oder einem Dokument mit Makros vorhanden. Damit sich das Computervirus verbreitet, muss die Datei von Benutzenden auf den Computer geladen und gestartet werden.
 - Der Computerwurm verbreitet sich zum Beispiel als E-Mail getarnt über das Internet auf weitere Rechner.

2. Was sind trojanische Pferde (Trojaner), und was tun sie?
 - Trojaner sind meistens Spionageprogramme.
 - Sie zeichnen Tastatureingaben auf (Spyware, Sniffer, Keylogger) oder steuern den Computer unbemerkt über ein Netzwerk fern (Backdoorprogramme).

3. Was ist Spam (Junk), und was bewirkt es?
 - Spam oder Junk sind auf elektronischem Weg übertragene Nachrichten.
 - Sie werden dem Empfänger ungebeten zugestellt und enthalten meistens Werbung.
 - Durch die zusätzliche Datenmenge belasten sie das Internet stark.

4. Erklären Sie, was Phishing ist.

Das Stehlen von persönlichen Daten.

5. Nennen Sie zwei Möglichkeiten, wie Ransomware auf den Computer gelangen kann.
 - Als präparierte E-Mail-Anhänge
 - Durch Ausnutzung von Sicherheitslücken in Webbrowsern
 - Durch das Fehlen einer Firewall

6. Was verhindert eine eingeschaltete und korrekt eingerichtete Firewall? Nennen Sie zwei Aspekte.

- Schützt vor Hackern
- Verhindert, dass Schadsoftware (z.B. Würmer) über ein Netzwerk Zugriff auf den Computer erlangen.
- Verhindert, dass der Computer schädliche Software an andere Computer weiter-schickt.

7. Was wird durch das Einschalten der automatischen Updates für das Betriebssystem erhöht? Nennen Sie zwei Aspekte.

- Zuverlässigkeit
- Leistungsfähigkeit
- Sicherheit

8. Nennen Sie zwei Rechte, die beim Anlegen eines Standardbenutzers festgelegt werden.

- Zeitlimits
- Spielfreigaben
- Spieltypen
- Programme

9. Können Cookies durch Benutzende gelöscht werden?

Ja

10. Nennen Sie vier Regeln zum Schutz eines Computers oder computerähnlichen Gerätes.

- Schalten Sie die Firewall immer ein.
- Schalten Sie das automatische Up-date des Betriebssystems ein.
- Schalten Sie die Sicherung des Betriebssystems auf einen externen Massenspeicher immer ein.
- Surfen Sie nicht im Administram-Konto.
- Schützen Sie jedes Konto mit einem separaten und sicheren Passwort.
- Treffen Sie die Einstellung von Cookies, Pop-ups und Add-ons entsprechend Ihrem Verhalten beim Surfen.
- Wählen Sie einen sicheren Browser.
- Installieren Sie geeignete Sicherheitssoftware.