Einfallstore für Angriffe auf Datennetze

1. Ergänze die Beschreibungen für die Begriffe:
   - **Computerviren** verursachen aktiv Schaden, z. B. *Dateien verändern oder löschen.*

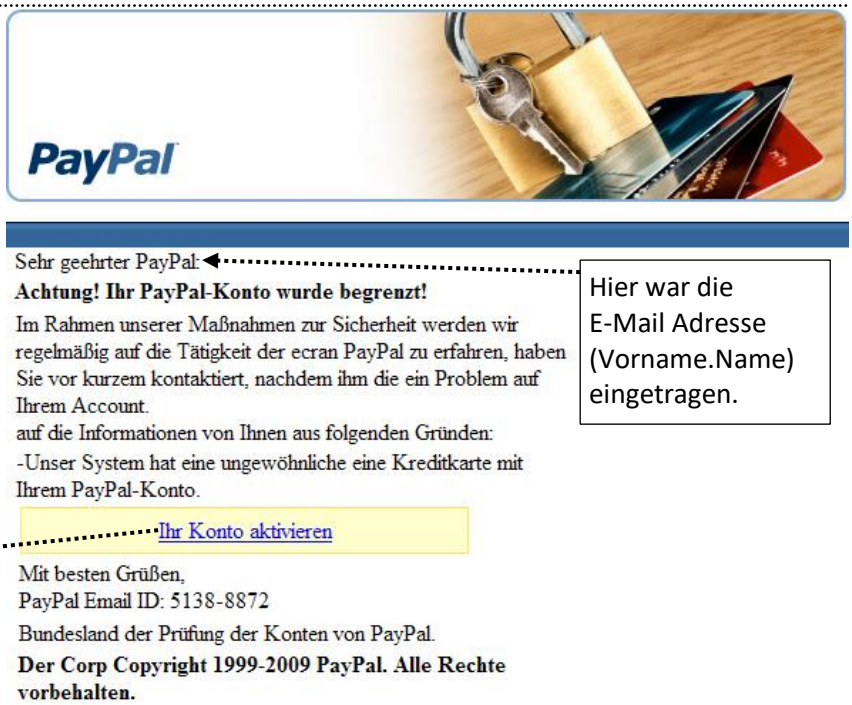
     Viren pflanzen sich fort, indem sie *sich selbst in vorhandene Dateien schreiben.*

     Verbreitet werden Viren oft über *Wechseldatenträger oder Dateianhänge von E-Mails.*
   - Beim **Phishing** werden Daten *erschlichen, z. B. mit Hilfe gefälschter Internetadressen.*

     Die Informationen können verkauft bzw. für weitere Straftaten genutzt werden.

Fallbeispiel:
Bei der Phishing-Mail lautet der Absender service@paypal.de
Den Link „Ihr Konto aktivieren“ kann man im Quelltext überprüfen (rechte Maustaste -> Quelltext anzeigen).
Der Link führt nicht zu “PayPal”, sondern zu “diloip.com“:

```
<a target="_blank"
href="/jump.htm?goto=
http%3A%2F%2F
www.diloip.com
%2Fcl%2Fwww.paypal.de
%2Fpaypal%2Fde%2F">
Ihr Konto aktivieren
</a>
```



2. Wenn du eine Benachrichtigung erhältst, solltest du dir immer die folgenden Gedanken machen, um die Authentizität zu klären – denn nicht immer sind Spams so offensichtlich wie in dem Beispiel:
   - Abgleich der Absenderadresse mit dem E-Mail-Text: *Ist plausibel*
   - Überprüfen der Grammatik und Rechtschreibung: *Fehlerhaft*
   - Klären der Notwendigkeit einer persönlichen Anrede: *Keine korrekte Anrede*

     ➔ Die E-Mail ist *nicht authentisch.*

   Wenn die E-Mail bis dahin glaubhaft wirkt, sollten im Zweifelsfall weitere Maßnahmen zur Klärung der Authentizität ausgeführt werden:
   - Internetrecherche mit Hilfe einer Suchmaschine nach einer prägnanten Formulierung, evtl. ergänzt um den Suchbegriff „spam“. Begriffe in Grafiken sind nutzlos.
   - Suche nach Hinweisen auf Spam in dem Internetauftritt des angeblichen Anbieters. Verwende **nicht** den Link in der E-Mail, sondern öffne einen neuen Tab oder ein neues Fenster.

➢ Dasselbe gilt natürlich genauso für **Instant-Messaging-Dienste wie ICQ, WhatsApp sowie Skype** und wie für PCs auch für Smartphones und Tablet-PCs – egal, welches Betriebssystem verwendet wird. Glaube niemandem, der dir das Märchen auftischt, bestimmte Geräte oder Betriebssysteme wären sicher vor Angriffen!

3. **Computerwürmer** üben nicht unbedingt eine direkte Sabotage aus. Vielmehr ergibt sich schon dadurch eine Schadfunktion, dass sie *sich über Netzwerke fortpflanzen,*
denn das kann für erheblichen Datenverkehr sorgen und Datennetze lahmlegen.
Dafür benötigen sie keine Datei als Wirt, sondern nutzen das System des infizierten Computers.
Würmer können aber oft weitere Funktionen ausführen, z. B. die E-Mail-Adressen im System

   auslesen und diese sowie sich selbst an alle Adressen senden.

   ➢ So kannst du scheinbar eine E-Mail von einem guten Freund erhalten, die authentisch wirkt. Sobald du den Dateianhang öffnest, wird das Schadprogramm aktiv. Der Wurm kann dann

   eventuell auch *weitere Sabotage- oder Spionagefunktionen ausführen.*

4. **Trojaner** verbreiten sich, indem sie aktiv ausgeführt werden.

   Dazu täuschen sie *eine sinnvolle Anwendung vor,*

   enthalten aber zusätzliche Funktionen, *mit denen sie Schaden verursachen.*

   Das kann z. B. *der Diebstahl von Zugangsdaten zum Online-Banking sein*

   oder einem Hacker die Möglichkeit eröffnen, beliebig auf den Rechner zugreifen zu können.

5. Um über ein WLAN Daten abzugreifen, muss man nicht den technischen Aufwand für einen man-in-the-middle Angriff betreiben. Es genügt oft schon, Daten in einem öffentlichen WLAN mitzulesen. Dafür gibt es Tools, deren Nutzung legal ist, wenn dies zur Administrierung eines Netzes geschieht. Für PCs ist hier *Wireshark* zu nennen und auch für Smartphones gibt es Apps, die den Datenverkehr mitschneiden. „Komfortabler" sind Tools, die gleich Details benachbarter Geräte anzeigen, für PCs z. B. *ZenMap* und für Smartphones z. B. *iNet*. Wenn man damit jemanden belauscht, ist das illegal – die Gefahr, dabei erwischt zu werden, ist aber minimal. Der Kriminelle hat also ein geringes Risiko. Es gibt auch Tools (z. B. *DroidSheep*), die Sitzungs-Cookies aufgreifen. So kann man sich auch in eine verschlüsselte Verbindung einklinken, indem man die bereits aktivierte Sitzung übernimmt. Das kann auch andauern, wenn sich der Nutzer entfernt, sofern er sich nicht explizit von dem Dienst abmeldet.
   - Gib mögliche Ziele für einen solchen Lauschangriff an.

     IP- und MAC-Adresse, um Angriffe starten zu können.

     Unverschlüsselte oder unzureichend verschlüsselte Kommunikation,

     z. B. mit einer Smarthome-Komponente oder mit einer Smartphone-App.

   Anmerkung: Durch einen *man-in-the-middle Angriff* kann auch eine verschlüsselte Verbindung kompromittiert werden. In den Lerninhalten 03 wird auf dieses Thema detailliert eingegangen.

6. Es gibt legal Hardware zu kaufen, mit der Systemadministratoren Datennetze auf Sicherheitslücken hin untersuchen können. Solche Geräte lassen sich für Angriffe auf Computernetze missbrauchen. Häufig handelt es sich um USB-Sticks, die öffentlich zugänglich abgelegt werden. Wenn jemand den Stick findet und in seinen Computer steckt, werden Schadfunktionen aktiv. Beispielsweise kann ein *Keylogger* installiert werden, der Tastatureingaben mitliest und an den Angreifer übermittelt. So können Kennwörter erfasst werden, auch wenn die Kommunikation verschlüsselt stattfindet. Oder es wird eine *Backdoor* installiert, mit der ein Krimineller stets auf den Rechner bzw. den Datenverkehr zugreifen kann. Es ist auch möglich, gleich Angriffe auf Netzwerkgeräte zu starten, z. B. Alarmanlagen auszuschalten oder Telefongespräche zu belauschen. Man kann auch fertig konfigurierte WLAN-Router für *Snarfing*-Angriffe kaufen. Beachte also:
   - Öffentliche Hotspots *nicht ungeprüft verwenden.*

     (Hinweise auf den Hotspot suchen, z. B. Aufkleber oder Schilder)
   - Wenn du einen USB-Stick findest, *diesen nicht verwenden. Eventuell vermisst ihn ja jemand?*