# Malware

Dass Hacker über Netzwerke eindringen, sich *in die Systeme hacken*, das ist lange vorbei.
Jedes Unternehmen und jeder Rechner Zuhause hat heute eine Firewall davor.
Angriffe gegen Rechner erfolgen durch immer ausgefeiltere Schadsoftware,
die auf verschiedene Weise auf den Rechner gelangt. Die Wichtigsten möchte
ich Ihnen kurz vorstellen.

**Verbreitete Infektionswege:**

- **E-Mail-Anhänge**
  E-Mail-Anhänge können Schadsoftware in verschiedenen Formaten enthalten.
  Beliebt sind vor allem Dokumentformate, die ausführbare Skripte beinhalten können.
  Dazu zählen insbesondere Office-Dokumente, PDF-Dateien und HTML-Dateien.
  Verbreitet sind auch direkt ausführbare Programme, die meistens in ZIP-Dateien
  versteckt werden.

  Unter Windows direkt ausführbar sind Dateien/Programme mit den Endungen
  **.exe, .com, .pif, .bat, .scr, .msi, .cmd, .wsh, .vbs**
  um nur mal ein paar davon zu nennen. Es gibt noch viel mehr, die auch ich mir nicht merken
  kann.

- **Web-Download**
  Beim Browsen im Internet kann man ebenfalls die oben genannten Dateien
  herunterladen, Browser können aber noch mehr Elemente ausführen. Dazu zählen
  Java-Programme, JavaScript-Programme und Flash-Applikationen.

  Manche dieser Programme werden auch ohne Ihr zutun aktiv, das Anschauen
  einer Webseite reicht für eine Infektion *(Drive-By Download)*.

- **Portable Datenträger**
  USB-Sticks, SD-Karten (für Digitalkameras) oder CDs und DVDs sind beliebte Sammelorte
  für Schadsoftware.

- **Mediendateien und andere Dateiformate**
  können auch als Transport für Schadsoftware dienen. Anzeigeprogramme für Bilder
  und Videos haben häufig Fehler, wenn sie mit speziellen (fehlerhaften) Mediendateien
  gefüttert werden. Daraus folgende Programmabstürze *(Buffer-Overflow-Attacken)*
  bzw. Fehlfunktionen können zum Ausführen von eingebetteten Schadprogrammen
  genutzt werden, siehe Stagefright.

Das Internet zu nutzen birgt also ein ständiges Risiko. Dagegen helfen bekanntlich Virenscanner.
Oder doch nicht?

**Warum der Virenscanner nichts findet.**

Die Malware-Industrie *(ja, das ist ein richtiger Industriezweig, wenn auch nicht ganz legal)* hat
dazugelernt und führt heute regelmäßige *Qualitätskontrollen* durch. Bevor eine Schadsoftware
auf die Internet-Nutzer losgelassen wird, wird sie mit den 10-20 populärsten Virenscannern
mit den neuesten Virensignaturen geprüft. Natürlich wird sie bei einer Erst-Infektion nicht erkannt.

**Was kann ich tun? Wie soll ich mich schützen?**

Wir alle sind von der Komplexität dessen, was uns umgibt, überfordert. Was wir vor 10 Jahren oder vorher gelernt haben, gilt so nicht mehr. Und die Menge an Möglichkeiten wird immer größer.
Aber ein paar einfache **Tipps** können zumindest helfen, Schaden zu verhindern oder zumindest zu begrenzen.

- **Regelmäßige Datensicherung**
  Bei einer erfolgreichen Infektion sind häufig Daten betroffen. Dateien fehlen, sind nicht mehr lesbar oder *irgendwie* verändert. Wohl dem, der eine aktuelle Datensicherung hat.
  Alle Dateien wegwerfen, Festplatte löschen, Rechner neu installieren sind probate Mittel bei einer Infektion. Mit einer aktuellen Datensicherung geht das auch relativ schnell.

- **Vorsicht beim Öffnen von Webseiten und E-Mail-Anhängen**

- **Beobachten und Hilfe holen**
  Wenn ihnen etwas *spanisch* vorkommt, melden Sie das, holen Sie Hilfe.
  ***Rechtzeitig Hilfe holen vermeidet Schäden.***

- **Segmentieren, Trennen von Aufgaben**
  Nicht alle Aufgaben müssen im gleichen Arbeitskontext, mit den gleichen Programmen, mit den gleichen Internet-Verbindungen durchgeführt werden.

  Überlegen Sie, welche ***gefährlichen Tätigkeiten*** auf andere Software, einen anderen Rechner oder einen *virtuellen Desktop* verlagert werden kann.
  Auch spezielle Schutzprogramme für *Sandboxen* können hilfreich sein.
  Auf jeden Fall hilft die Strategie, für interne Aufgaben und für das Internet zwei unterschiedliche Browser zu verwenden, z.B. ***Internet-Explorer*** für das Intranet und ***Firefox*** oder ***Chrome*** für das Internet.

  Schauen Sie sich mal genauer an, ob ***kritische Daten und Programme*** immer im Zugriff bzw. immer geöffnet sein müssen.
  Selten genutzte Ablagen müssen nicht immer als Laufwerk zugewiesen *(gemapped)* sein.
  Es reicht vielleicht, einen Link auf den *UNC-Pfad* auf dem Desktop zu hinterlegen.

Und zum Schluss…

**Was macht denn Malware überhaupt?**

- **Advanced Persistent Threats**
  Manche Malware macht – nichts. Zumindest zuerst nicht. Spionage-Programme gegen Unternehmen lassen sich manchmal Jahre Zeit, um Informationen zu stehlen. Dabei ist die Geschwindigkeit manchmal in Byte pro Stunde zu bemessen.

- **Keylogger**
  Andere Malware hat es auf Passwörter abgesehen und schreibt *nur* die Tastatureingaben mit.

- **Erpressungs-Trojaner**
  Es gibt Malware, die Dateien verschlüsselt. Gegen eine Zahlung einer Ablöse *(heute meist in Bitcoins)* kann man den Schlüssel wiederbekommen, so man überhaupt mit den Kriminellen in Kontakt kommen kann.

- **Bot-Netz**
  Viele Schadprogramme haben gar nicht den infizierten Rechner zum Ziel. Es geht nur darum, für andere Aktionen *(Spam-Versand, Angriffe gegen große Firmen)* genügend Rechenleistung zu haben. Diese Ro**Bot**er werden anschließend ferngesteuert und ggf. im Hunderttausender-Pack stundenweise an Kunden vermietet.