2017

Wie vermeide ich Schadsoftware?

DIE COMPUTERVIREN

TORBEN FELSCH

ERSTELLT IM RAHMEN VON CORVEY+

Wie vermeide ich Schadsoftware?

DIE COMPUTERVIREN

TORBEN FELSCH

Was sind eigentlich „Viren“?

- **Meist bösartige Programme, die**
  - sich unbeabsichtigt und unbemerkt installieren
  - sich selbst vervielfältigen und evtl. übertragen können.
  - oft ständig laufen, ohne bemerkt zu werden
- **Viren heißen Viren, weil ihr Vorgehen mit dem der biologischen Viren vergleichbar ist:**
  - man kann sich und andere „anstecken“
  - sie breiten sich aus
  - ein infiziertes Programm wird zu einem „Wirtskörper“
- **„Schadsoftware“ ist der neue Oberbegriff für alle Fieslinge, um die es hier geht!**
  - Viren, Würmer, Trojaner, Hoaxes,…
  - Und viele andere, die sich mittlerweile kaum noch eindeutig klassifizieren lassen und deren Funktionen sich teilweise überschneiden.

Platz für Notizen

Glossar

Skript	Vorgegebener Ablauf mehrerer Befehle die sich auf unterschiedliche Programme beziehen können
Sourcecode/ Quellcode	Befehlsabfolge eines Programms, die später mit Hilfe eines „Compilers“ in ein ausführbares Programm gewandelt wird.

Was kann Schadsoftware tun?

Grundsätzlich alles, wozu der Computer in der Lage ist!

- **Computer fernsteuern und mitlesen, z.B.**
  - - Tastatur- und Mauseingaben aufzeichnen oder simulieren
  - - Bilder unbemerkt über die Webcam aufnehmen
  - - Bildschirminhalte streamen (live Übertragung)
  - - beliebige Programme starten oder beenden
  - - Nachrichten senden/löschen
- **Daten zerstören bzw. löschen**
  - einfach um generell böse zu sein oder um einer bestimmten Person/Firma zu schaden

- **Daten verschlüsseln**
  - um sie z.B. gegen Geldzahlung wieder zu entschlüsseln
    Siehe: Trojaner „WannaCry“ vom 12/13.5.17, bei dem mehrere 10.000 Rechner verschlüsselt wurden (unter anderem in Krankenhäusern).
- **Daten sammeln**
  - um z.B. an Zugangsdaten, Bankverbindungen oder Mailadressen zu gelangen.
- **Daten an andere Systeme übertragen**
  - um z.B. ganz von selbst über längere Zeit eine umfassende Datenbank über beliebige Daten zu erhalten (meist Kreditkarten, Passwörter), oder um ganze Datenbestände zu kopieren.
- **Weitere Schadsoftware aus dem Internet laden und installieren**
- **Sich in andere Programme einklinken und diese dann fernsteuern/manipulieren**

Viren entfernen

- **Übernimmt meist das Virenschutzprogramm**
- **In schwierigen Fällen sollte man Experten fragen (aber nicht mich ;)**
  - - er kann versuchen, Bestandteile des Virus zu finden und zu löschen
  - - ggf. werden nur die Daten gerettet und der Rechner neu installiert.
  - - trotzdem keine 100% sichere Methode.
- **Früheren, gesicherten Computerzustand wieder herstellen**
  - - Wenn man sicher ist, dass die Sicherung vor der Infektion erfolgte
- **Betriebssystem neu installieren.**
  - - sicherste, aber aufwändigste Methode, weil alle Programme neu installiert werden müssen.

Sofortmaßnahmen bei Befall

- **Herunterfahren ist nie verkehrt**
  - dann sollte der PC aber wirklich aus sein (es gibt Viren, welche einen ausgeschalteten PC simulieren)
    Dadurch wird das Starten im abgesicherten Modus ermöglicht.
- **Sofort Netzwerkstecker ziehen bzw. vom WLAN trennen und Fachmann fragen/Broschüre weiterlesen :)**
- **Im abgesicherten Modus über den Virenscanner einen ausführlichen Scan starten und alle Treffer beseitigen lassen.**

Diese Tipps kann man alle ausführen, klappen aber nicht alle in der Reihenfolge (auch nicht empfehlenswert)

Wie erhält man Schadsoftware?

- **Durch Öffnen einer bereits infizierten Datei**
  - - die entweder selbst als Programm ausführbar ist oder
  - - die von einem Programm geöffnet wird, das deren Inhalt ausführen kann.
  - - von einem beliebigen Ort aus (Download, USB-Stick, E-Mail-Anhang etc.)
- **Durch Besuch einer präparierten Webseite**
  - Webseiten enthalten sehr oft notwendige Programme oder „Skripts“, um nützliche Dinge tun zu können. Genau so können aber auch bösartige Dinge ausgeführt werden. Oft weiß der Betreiber gar nicht, dass seine Website „gehackt“ wurde und somit die Schadsoftware verbreitet.
- **Durch modifizierte Updates**
  - von Betriebssystemen oder regulären Programmen (allerdings sehr unwahrscheinlich!)

Vorbeugung

- **Selbstschutz ist immer noch am besten.**
  - - am besten ist immer noch, sich selbst bewusst zu sein, was man tut, und nicht einfach unerwartetem Verhalten folgt.
  - - Warnmeldungen oder Bestätigungsabfragen nicht einfach wegklicken/bestätigen, sondern lesen und ggf. hinterfragen.
  - - Virenschutzprogramme sind zwar Pflicht, können aber auch nicht alles abblocken.
- **Keine Mails von Fremden öffnen**
  - - Mails von mysteriösen/unbekannten Absendern NICHT öffnen
  - - keine Anhänge öffnen, die von jemandem Fremden kommen oder die ein gefährliches Dateiformat haben (.exe .com .cmd .jar .zip .bat .doc .docx .js…), es sei denn man erwartet so einen Anhang.
- **Vorsicht vor fremden Datenträgern**
  - - USB-Sticks und DVD können selbst ausführende Programme enthalten.

Nicht immer gleich jeden Link anklicken.

- - Links können auf bösartige Webseiten führen.
- - Man kann auch auf Phishing-Seiten geführt werden, wo man vertrauliche Daten preisgeben soll.
- - ein Link kann anders sein als er dargestellt wird, z.B. www.amazon.de wird angezeigt, führt aber zu www.phishing.de

- **Virenscanner**
  - - Falls man einen Firmen-PC besitzt, nach einer Variante für Virenschutz vom Unternehmen fragen. Oftmals haben Firmen den besseren Virenschutz als Privatanwender!
- **Backups durchführen**
  - Möglichst Komplettsystem sichern
  - Mindestens regelmäßig für einen selbst wichtige Dokumente sichern (Schreiben, Fotos, Musik, Videos…)
  - Gerade nach Befall durch einen Verschlüsselungs-Trojaner oft der einzige Weg, wieder an die Daten zu gelangen.