Verschiedene Arten von „Schädlingen“

Was ist ein Computervirus?

Ein **Computervirus** verbreitet sich von PC zu PC, indem er Dateien oder Datenträger mit seinem Programmcode befällt. Im Unterschied zu einem Wurm braucht es stets die Mithilfe des Computer-Anwenders, damit ein Virus aktiv wird. Es gibt verschiedene Typen von Computerviren:

Datei- oder Link-Viren befallen ausführbare Programmdateien, die zum Beispiel mit den Dateinamenserweiterungen ".exe", ".com" oder ".scr" gekennzeichnet sind. Betroffen sind davon fast alle Bestandteile von Windows und installierte Programme. Diese Viren-Spezies schreibt ihren Code in die jeweilige Datei hinein. Sobald der Anwender die Datei startet, wird der Virus automatisch mit ausgeführt.

Bootviren infizieren Datenträger und verbreiten sich in erster Linie über USB-Sticks oder früher über Disketten. Sie nisten sich im Bootsektor der Festplatte ein, also in dem Bereich, in dem steht, wie groß das Speichermedium ist und wie der Computer gestartet werden soll. Bei jedem Systemstart wird das Virus aktiv, befällt weitere Sektoren oder infiziert angeschlossene Speichermedien. Weil moderne PCs beim Starten Änderungen des Bootsektors bemerken, ist diese Virenart heute nicht mehr häufig anzutreffen.

Makroviren verstecken sich nicht in Programmen, sondern in Word- oder Excel-Dokumenten. Makros werden in einer Office-eigenen Programmiersprache geschrieben; vor allem, um Arbeitsabläufe zu automatisieren. Beim Laden des verseuchten Dokuments beginnt das Virus automatisch mit seiner Schadensroutine. Diese reicht von einfachen Scherzen, wie etwa das Verstecken von Menü-Einträgen, bis hin zum Löschen von Dateien. Hinzu kommt, dass einige Varianten erst an einem bestimmten Tag oder nach einer bestimmten Anzahl von Starts aktiv werden.

Was ist ein Computer-Wurm?

Würmer verbreiten sich selbstständig innerhalb eines Netzwerks, ohne Dateien direkt zu befallen und praktisch ohne Nutzereingriff. Sie sausen bevorzugt als E-Mail-Anhang kreuz und quer durch das Internet, wo sie optimale Bedingungen vorfinden. Im günstigsten Fall besteht ihr Ziel in ihrer endlosen Vermehrung und der Belegung von Speicherressourcen – dadurch sinkt die Rechenleistung eines infizierten PCs. Würmer haben in der Vergangenheit bereits ganze Netzwerke lahmgelegt. Auch gibt es viele Würmer, deren Code mit den Eigenschaften von PC-Viren kombiniert wurde. Einige haben sogar Trojaner als Schadfracht mit an Bord.

Was ist ein Trojaner?

Trojaner, besser Trojanisches Pferd, bezeichnet ein scheinbar harmloses Programm mit einer verdeckten Schadensfunktion: einem Virus, Wurm oder Spyware. Der Zweck der meisten Trojaner ist es, schädliche Programme auf den PC zu schleusen, die unbemerkt sensible Daten wie Passwörter für Homebanking oder Mail-Accounts, Kreditkartennummern und ähnliches ausspähen und übermitteln. Eine besonders gefährliche Form des Trojanischen Pferdes sind so genannte Backdoor-Trojaner. Hierbei handelt es sich um Hilfsprogramme, durch die ein Hacker auf fremde Computer zugreifen kann**.**

Was ist ein Spyware?

Spyware bezeichnet Programme, die Informationen über PC-Nutzer wie etwa persönliche Daten und Surfgewohnheiten ausspionieren und sie über das Internet übertragen. Die Hintermänner können so zum Beispiel Vorlieben des Surfers erfahren und gezielt Werbung auf den PC schleusen. Spyware-Anbieter locken oft mit hübschen Bildschirmschonern oder anderen attraktiven Gratis-Programmen, in denen sie ihre Schadsoftware verstecken. Zunehmend wird Spyware auch über Trojaner und Würmer verbreitet.

Was ist ein Hoax?

Hoax bedeutet an sich "schlechter Scherz" und wird im Internet allgemein für eine Falschmeldung verwendet. Ergänzt werden derartige Meldungen meistens um die Bitte, die Nachricht an Freunde und Bekannte weiterzuleiten. Hoaxes sind im engeren Sinn keine Malware, denn in der Regel verfolgen sie keine kriminellen Absichten. Dennoch können solche "Scheinviren" gefährlich werden. Einige dieser Hoaxes fordern den PC-Nutzer zum Beispiel auf, bestimmte und zum Teil wichtige System-Dateien zu löschen. Einige Hoaxes geistern schon seit vielen Jahren durchs Internet. Einer der bekanntesten ist der *Budweiser Hoax*, der vor einem angeblichen Virus in einem Bildschirmschoner der Brauerei warnt.

Was ist Adware?

Als Adware bezeichnet man kostenlose Software-Angebote und Apps, die dem Anwender auf seinem Gerät Werbung einblenden. Die Programme machen in der Regel keinen Hehl daraus, was ihre Absicht ist und bitten den Anwender vor der Installation um Erlaubnis. Da es aber Anwendungen gibt, die zugleich *Adware* und *Spyware* sind, stehen alle Vertreter der Klasse Adware unter dem generellen Verdacht, Spyware zu sein.

Was ist ein Keylogger?

Ein Keylogger dient dazu, Tastatureingaben des Nutzers aufzuzeichnen. Online-Kriminelle benutzen Keylogger, um persönliche Daten wie Passwörter direkt "von den Fingern" des Anwenders abzugreifen.

Was ist Scareware?

Scareware (englisch scare = Schrecken) dient dazu, Computeranwender zu verunsichern und sie dazu zu verleiten, eine Software zu installieren. In der Regel handelt es sich um professionell aufgemachte Programme, die vorgeben, den PC auf Malware-Befall, Hacker-Angriffe oder auf Systemprobleme zu testen. Geht der Computernutzer darauf ein, erhält er anschließend einen umfassenden und erschreckenden Fehlerbericht – zusammen mit der Aufforderung ein Programm zu installieren, dass angeblich gefundene Viren oder Systemprobleme beseitigt. Tatsächlich führt Scareware keine Tests durch, der angebliche Befall steht schon vorher fest. Die Hintermänner verkaufen auf diese Weise nutzlose Software oder verbreiten ihrerseits weitere Malware.