Internet-Gefahr: Viren, Würmer und Trojanische Pferde

Gefährlicher als Spionageprogramme oder belästigende Werbemails sind Schädlinge wie Viren, Würmer oder Trojanische Pferde. Sie können auf befallenen PC-Systemen zu einem unwiederbringlichen Verlust von Daten und zu Softwareschäden führen. Viren verstecken sich häufig in E-Mail-Anhängen, in infizierten Anwendungen oder Dateien, die aus dem Internet heruntergeladen werden; sie können aber auch über externe Datenträger wie USB-Stick oder USB-Festplatten sowie über besuchte Websites verbreitet werden.

Wird die Anwendung gestartet oder das Dokument geöffnet, aktiviert sich der Virus und beginnt sein zerstörerisches Wirken auf dem Rechner. Das kann vom Verändern von Bildschirminhalten oder Anzeigen von Mitteilungen bis zum Manipulieren, Zerstören oder Löschen von Daten reichen.

Virus, Wurm, Trojanisches Pferd: Was ist das eigentlich?

Gelegentlich wird "Virus" als Oberbegriff für alle drei Formen von Schädlingen verwendet, doch genau genommen ist das nicht korrekt, da es zwischen ihnen Unterschiede gibt:

- Ein Virus ist ein kleines Programm, das sich bei der Ausführung selbst repliziert und verbreitet. Ein Virus kann schwere Schäden anrichten, kann sowohl Daten löschen als auch Programme funktionsunfähig machen - je nachdem, wozu er programmiert wurde. Der Virus funktioniert allerdings nicht völlig selbstständig: Um zu starten, muss er sich entweder in die Startroutinen der Software eines Rechners einklinken oder den Nutzer dazu bringen, ihn

direkt manuell zu starten.

- Ein Trojanisches Pferd ist ein Programm, das vorgibt, eine nützliche Funktion zu erfüllen - und dies möglicherweise auch tut -, um zugleich auf eine andere Weise aktiv zu werden, die vor dem Nutzer verborgen bleibt. Ein Beispiel wäre eine Datei, die sich als Windows-System-datei tarnt, aber in Wirklichkeit dazu dient, übers Internet eine Verbindung mit demjenigen aufzubauen, der das Trojanische Pferd eingeschleust hat und auf diese Weise Zugriff auf den Rechner bekommt. Diesen kann er nun nutzen, um z. B. Software darauf zu installieren oder Informationen auszuspähen. Anders als ein Virus repliziert und verbreitet ein Trojaner sich nicht von selbst.
  Bekannt wurden auch Fälle, bei denen Hacker über eingeschleuste Software Zugriff auf Webcams erlangten und damit besonders unangenehm in die Privatsphäre vordrangen, zum Beispiel um Kinder im Kinderzimmer zu beobachten - hier hilft es, die Webcam bei Nicht-Nutzung abzuklemmen oder, wenn sie fest eingebaut ist, zu überkleben.

- Ein Wurm ist ebenfalls ein sich selbst replizierender Schädling, der es jedoch im Unterschied zum Virus nicht dem Zufall überlässt, wann und wie er vom einen zum anderen Rechner gelangt, sondern aktiv versucht, auf andere Systeme überzugreifen. Er benötigt kein "Wirts-programm" wie der Virus. Bei den berüchtigten "Viren", die sich selbst als E-Mail-Anhänge an die Kontakte verschicken, die im Adressbuch des infizierten Systems gespeichert sind, handelt es sich streng genommen um Würmer.

Rechner, die fürs Surfen im Web benutzt werden, sollten grundsätzlich mit aktueller Software betrieben werden, was neben dem Betriebssystem vor allem für Programme gilt, die Internet-verbindungen nutzen, z. B. Browser und Browser-Plug-ins, E-Mail-Software, Messenger usw. Meist wird man von der Software automatisch darüber informiert, wenn es Updates gibt. Man sollte diese dann schnellstmöglich herunterladen und installieren, denn oft werden damit Sicherheitslücken gestopft, die bereits bekannt sind und daher von Angreifern relativ einfach ausgenutzt werden können.

Des Weiteren sollten Internetrechner mit einer Anti-Viren-Software ausgestattet sein, die durch regelmäßiges Updaten auf dem neuesten Stand gehalten wird. Eine solche bekommt man als Privatanwender auch kostenlos. Auch der Einsatz einer Personal Firewall ist unter Umständen ratsam, da diese Zugriffsversuche von außen auf bestimmte Ports erkennen und gegebenenfalls blockieren kann. Am wichtigsten ist es aber, im Internet entsprechend aufmerksam zu agieren, damit man sich Viren, Würmer oder Trojaner möglichst gar nicht erst einfängt.

Vor allem sollte man keine Software aus zweifelhaften Quellen herunterladen und keine E-Mail-Anhänge von unbekannten Absendern öffnen - letzteres ist ein klassischer Verbrei-tungsweg von Schädlingen. Die Anhänge tarnen sich als Textdokumente, Fotos, Rechnungen etc., sind in Wirklichkeit aber ausführbare Dateien, die den Schädling aktivieren, wenn man sie öffnet. Öffnen Sie niemals einen E-Mail-Anhang, wenn Sie nicht genau wissen, worum es sich handelt, oder dem Absender vollkommen vertrauen.

Schädlinge, die von besuchten Webseiten her übertragen werden, nutzen dazu Skriptsprachen, die dazu gedacht sind, dynamische und interaktive Inhalte zu ermöglichen - vor allem JavaScript und früher auch ActiveX. Natürlich kommt es auch hier darauf an, zwielich-tige Websites im Zweifelsfall gar nicht erst zu besuchen. Dies ist jedoch nicht immer leicht einzuschätzen.

Die von Microsoft konzipierte ActiveX-Technologie fand sich unter den Web-Browsern nur im Internet Explorer, der mittlerweile durch Microsoft Edge abgelöst wurde. Sie hatte weitreichende Zugriffe auf das System und wenn man Internet Explorer immer noch verwendet, kann es daher eine sinnvolle Maßnahme sein, sie komplett zu deaktivieren. Allerdings war ActiveX früher zum Beispiel für das manuelle Windows Update notwendig.

Die Befugnisse von JavaScript sind dagegen durch das sogenannte Sandboxing auf Daten des Browsers beschränkt, wobei auch unterschiedliche Webseiten gegeneinander abgeschirmt sind. Trotzdem bietet auch JavaScript Missbrauchsmöglichkeiten für Angreifer.

Wer seine Sicherheit erhöhen will, kann dazu die Unterstützung für Skriptsprachen im Browser abschalten. Bei Bedarf lassen sie sich dann für die Dauer einer Sitzung oder auch für bestimmte vertrauenswürdige Websites wieder aktivieren. Das ist auch sinnvoll, um bequem im Web surfen zu können, da heutzutage die meisten Webseiten JavaScript-Elemente enthalten wie zum Beispiel von sozialen Netzwerken oder Webmail-Anbietern und sonst nur sehr eingeschränkt oder gar nicht mehr nutzbar sind.

Firefox-Nutzer können hierfür auf die passenden Add-Ons zurückgreifen, Opera bietet von Haus aus ähnliche Funktionen. Im Internet Explorer konnte man die relevanten Browserfunktionen unter "Extras", "Internetoptionen", "Sicherheit", "Stufe anpassen" ein- und abschalten; der einfachere Weg war es aber, den Regler für die Sicherheitsstufe auf "hoch" zu setzen.

Während früher häufig empfohlen wurde, PDF- statt Office-Dateien zum Austausch von Texten zu nutzen, galten PDF-Dokumente bzw. PDF-Reader zwischenzeitlich ebenfalls als Sicherheitsrisiko. Insbesondere Sicherheitslücken des Adobe Readers wurden für Attacken ausgenutzt, sodass selbst das Bundesamt für Sicherheit in der Informationstechnik (BSI) dazu riet, auf andere PDF-Reader auszuweichen oder beim Adobe Reader JavaScript zu deaktivieren - dies wird vor allem bei der Eingabe von Daten in Formulare benötigt. Möchte der Nutzer ein Dokument nur betrachten, so entsteht aus der Deaktivierung kein Nachteil.

Auch ein zweites Adobe-Produkt entpuppte sich zunehmend als Sicherheitsrisiko: Der Flash Player. Darum wurde dessen Entwicklung seitens Adobe inzwischen eingestellt. Für die Anzeige von Web-Inhalten ist er wegen HTML5 ohnehin nicht mehr erforderlich, deswegen sollte man ihn auf allen Systemen deinstallieren.