Das Viren Lexicon

Viren haben nur eines im Sinn – sie wollen sich möglichst schnell vermehren. Genau wie ein Schnupfen sind auch die PC-Schädlinge aus Bits und Bytes leicht ansteckend. Früher fanden sie über infizierte Disketten den Weg auf den Computer, heutzutage sind E-Mails, Internet und Netzwerke die häufigsten Übertragungswege. Einige sind sehr gefährlich, wie „Win32.CIH“, der sogar Bios-Speicherbausteine zerstören kann. Andere sind einfach nur lästig, wie Viren, die zum Beispiel regelmäßig die Schublade des DVD-Laufwerkes öffnen

Cookies sind keine Viren
Einige Begriffe werden häufig mit Viren in Verbindung gebracht, gehören aber zur Funktionalität von Webseiten und sind nicht gefährlich. Wenn Sie im Internet surfen, legen viele Web-Server „Cookies“ (auf deutsch: Kekse) auf Ihrem Rechner ab. In ihnen sind Informationen gespeichert, die bei einem späteren Besuch auf der Homepage wieder abgerufen werden. Sie brauchen oft keine erneuten persönlichen Einstellungen vornehmen oder es werden Ihnen zuletzt angesehene Artikel präsentiert.

E-Mail-Anhänge
Schädlinge verbreiten sich meist über den E-Mail-Versand. Öffnen Sie E-Mail-Anhänge („Attachments“) nur, wenn Sie den Absender kennen. Aber: Würmer machen sich gerade dieses Vertrauen zunutze und verschicken sich selbst mit der E-Mail-Adresse eines Bekannten. Deshalb ist es in jedem Fall unerlässlich, sich mit einem Virenschutz-Programm zu schützen.

Auch die Art des E-Mail-Anhangs verrät etwas über das Gefahrenpotenzial. Ein Bild, zu erkennen etwa an der Endung „JPG“ oder „GIF“, ist meist ungefährlich. Ausführbare Dateien, die zum Beispiel die Endung „EXE“ oder „VBS“ tragen, sind dagegen viel eher ein Sicherheitsrisiko. Vorsicht: Einige E-Mail-Programme blenden die Dateiendungen aus. So können sich etwa gefährliche Schadprogramme als harmlose Bilder tarnen.

Backdoor
Eine Backdoor (deutsch: Hintertür) ist ein Schadprogramm, das Sicherheitsmaßnahmen umgeht, um dann die Kontrolle über einen Computer zu erlangen. Ist die Hintertür geöffnet, kann der Angreifer etwa Rootkits oder Trojaner installieren und so zum Beispiel persönliche Daten ausspionieren.

Boot-Virus
Boot-Viren verändern den Startbereich von Disketten und Festplatten. Das kann beispielsweise den Start des Betriebssystems verhindern.

Dialer

Dialer (deutsch: Einwahlprogramme) können selbstständig eine Telefonverbindung aufbauen und damit extrem hohe Kosten verursachen. Sie funktionieren allerdings nur, wenn Sie per Modem oder ISDN ins Internet gehen. DSL-Anschlüsse sind nicht bedroht. Aber: Wer ein Modem oder eine ISDN-Karte per Fax vom PC aus versendet, kann auch Opfer eines Schadprogramms werden.

Drive by Download
Kriminelle haben eine neue Masche ausgeheckt, mit der sie Massen von Schädlingen verbreiten: Über präparierte Internetseiten jubeln sie Internetnutzern ihre Schadsoftware

schon beim bloßen Besuch einer infizierten Seite unter. Der ahnungslose Nutzer muss nicht mal etwas anklicken. Die Schädlinge gelangen über Schwachstellen sogenannte Exploits des Browsers in den PC.

Firewall
Eine Firewall überwacht den Datenverkehr zwischen Computer und Internet in beide Richtungen – also vom PC ins Internet und umgekehrt. Versucht beispielsweise ein Programm heimlich eine Verbindung vom Computer ins Internet herzustellen, schlägt die Firewall Alarm.
Sie gehen mit einem Router ins Internet? Noch besser, denn meist ist darin auch eine sogenannte Hardware-Firewall eingebaut. Sie überwacht den gesamten Datenstrom vom Internet ins Netzwerk und anders herum. Allerdings schützt eine Hardware-Firewall nur vor Gefahren aus dem Internet. Deshalb sollten Sie zusätzlich eine Software-Firewall auf Ihrem Computer installieren oder zumindest die im Windows-Lieferumfang enthaltene Firewall aktivieren.

Hoax
Ein Hoax (auf Deutsch: Schabernack) heißt eine Falschmeldung, die meist per E-Mail verbreitet wird. Oft wird über Virenfalschmeldungen versucht Angst zu schüren oder Benutzer zu sinnlosen Aktionen zu verleiten. Etwa: „Löschen Sie die Datei XY, um Ihren PC zu schützen."

Keylogger
Ein Keylogger (deutsch: Tasten-Rekorder) kann Tastatureingaben und Screenshots (Bildschirmfotos) aufzeichnen und über das Internet an einen Angreifer schicken oder in einer Datei speichern. So spionieren Gauner geheime persönliche Daten aus, etwa Passwörter oder PINs für das Online-Banking.

Makrovirus

Ein Makro ist ein Programm, das in einem Dokument eingebaut ist und kleine nützliche Aufgaben erfüllt. So fügt ein Makro etwa automatisch Adressen in einen Serienbrief ein. Enthält ein Makro einen Virus, kann der sich auf andere Dokumente übertragen und Daten verändern oder löschen.

Malware
Als Malware (Kunstwort aus engl. malicious – „bösartig" – und Software) bezeichnet man Computerprogramme, die vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen ausführen. Viren, Würmer und Trojaner sind also auch Malware.

Phishing
Der Begriff ist ein englisches Wortspiel, das sich an fishing („angeln", „fischen") nach Passwörtern anlehnt. Es handelt sich hierbei um kein spezielles Schadprogramm. Die Betrüger gaukeln als Absender etwa Ihre Bank vor und wollen Sie auf fingierte Internetseiten locken. Dort sollen Sie Ihre Konto-Zugangsdaten angeben. Mit diesen Daten plündert man schließlich Ihr Bankkonto.

Polymorpher Virus
Ein polymorpher Virus verändert selbstständig seinen Programmcode. Auf diese Weise soll er der Erkennung durch Schutzprogramme entgehen.

Programmvirus
Programmviren brauchen als Wirt ein Programm (etwa mit der Datei-Endung „.exe“ oder „.com“). Sie werden aktiviert, wenn eine befallene Datei ausgeführt wird.

Rootkit
Sie können sich und andere Schädlinge vor Virenschutz-Programmen verstecken. Einmal aufgespielt, greifen Datenräuber unbemerkt auf den Computer zu.

Spam
E-Mails, die unverlangt zugestellt und massenhaft versendet werden, bezeichnet man als Spam. Diese Mails enthalten häufig Werbung, etwa für Medikamente oder gefälschte Produkte.

Spyware
Spyware und Adware sind Programme, die sich oft in kostenloser Software verstecken. Spyware sendet persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software oder an Dritte. Sie verrät zum Beispiel, welche Seiten Sie im Internet besucht haben. Adware blendet unerwünschte Werbung ein.
Trojaner
Trojaner (Synonym: trojanisches Pferd) gaukeln dem PC vor, eine bestimmte Funktion zu haben, die unverdächtig ist. In Wahrheit erledigen sie ganz andere Aufgaben, laden etwa andere Schadprogramme aus dem Internet („Download-Trojaner“) oder spionieren persönliche Daten aus. Trojaner vermehren sich nicht selbst, was sie von Viren und Würmern unterscheidet.

Virus
Viren sind Schadprogramme, die Daten eines Computers beschädigen, manipulieren oder zerstören. Viren vermehren sich selbst und verbreiten sich bei der Weitergabe von Dateien (zum Beispiel auf einem Datenträger oder per E-Mail).

Wurm
Ein Wurm verbreitet sich selbstständig über Computernetzwerke, etwa durch E-Mails. Er richtet nicht unbedingt direkt Schaden an. Da er sowohl auf den infizierten Computern als auch in den Netzwerken für jede Menge Wirbel sorgt, kann er allerdings hohe Kosten verursachen. Etwa in dem er den Datenverkehr blockiert oder Computer herunterfährt – eine Katastrophe in einem Rechenzentrum.