Kleiner Virenduden

Backdoor	Viele Würmer, Viren und Trojaner öffnen auf dem befallenen PC eine Hintertür (backdoor) ins Internet, z.B. für denjenigen, der ein solches Backdoor-Programm eingeschleust hat Unter Backdoor versteht man ein Programm, über das ein Hacker per Internet auf einen Rechner zugreifen kann (auch auf Ihren). Bekannte Verteter sind z.B. "BackOrifice" oder "Netbus". Teilweise sind Backdoors ausgefeilte Programme, die Dateien kopieren, Tastatureingaben mitschneiden (KeyLogger) oder gar den Bildschirminhalt übertragen. Haben Sie ein Backdoor auf dem PC, so "sieht" der Angreifer jede Ihrer Aktionen, etwa wenn Sie Ihre Kreditkarten-Nummer beim Online-Einkauf eingeben. Zudem lassen sich beliebige Manipulationen am System vornehmen.
Heuristik	Alle Antiviren-Programme versuchen neben der Signaturerkennung, neue unbekannte Schadprogramme anhand typischer Merkmale zu erkennen
Keylogger	Ein Spionageprogramm, das Tastatureingaben und -anschläge genau aufzeichnet, um danach herausfinden zu können, was alles an Daten eingegeben wurde (z.B. Kreditkarten-Nummer, Passwörter)
Makrovirus	Programme wie z.B. Office (Word, Excel, Access etc.) verfügen über Makros, um häufige Vorgänge zu automatisieren. Dieses kann durch Malware ausgenutzt werden
Malware	Kurzform für "malicious software", bösartige/arglistige Software, die zum Einschleusen von Viren/Würmern/Trojanern etc. benutzt wird. Oft werden im Internet als nützlich getarnte Tools zum kostenfreien Download angeboten, die solche Schädlinge enthalten
Wächter	Ein Virenwächter arbeitet immer im Hintergrund und prüft jede Datei vor dem Öffnen oder Starten
Scanner	Der Virenscanner ist ein Teil eines Antivirenprogrammes, der Dateien nach Malware (Viren/Würmern/Trojanern etc.) untersucht
Trojaner	Dieser Schädling gibt vor, ein nützliches Programm oder Tool zu sein. In Wirklichkeit ist es ein Schadprogramm. Ein Trojaner (als Abkürzung für Trojanisches Pferd) nutzt die Neugier der Anwender aus. Die Programmdatei gibt vor, z.B. ein Patch oder ein anderes nützliches Programm zu sein. Der Anwender lädt das Programm herunter oder startet es von einer CD, und damit aktiviert sich gleichzeitig der Trojaner. So gesehen beschreibt der Begriff mehr eine Infektionstechnik als eine Schädlingsart.
Virus	Ein Virus ist ein Programm oder ein Script, das sich selbständig verbreitet. Es kopiert sich dazu in den Code eines harmlosen Programmes. Ruft der Anwender später ein infiziertes Programm auf, so wird im Hintergrund der Virus mitgestartet
Wurm	Ein Wurm infiziert nicht wie ein Virus Software, sondern klinkt sich in Windows (im System) ein und wird beim Neustart oder sofort aktiv. Er sucht ggf. auch selbständig weiter nach Opfern, die er wieder infizieren kann. Auch dieser Schädling arbeitet meist unerkannt auf einem System. Ein Wurm befällt nicht eine einzelne Datei oder einen Bootsektor, er nistet sich vielmehr als normales Programm in das befallene Betriebssystem ein. Dazu kopiert sich der Wurm als Datei auf die Festplatte. Zudem manipuliert er die Registry oder sonstige System-Dateien so, daß die Wurmdatei aktiviert wird, sobald Windows startet.
Netzwerkwurm	Diese Art verbreitet sich besonders schnell im Netzwerk oder im Internet, denn sie sind nicht auf einen Doppelklick oder auf die Ausführung durch einen Benutzer angewiesen. Bekannte Beispiele sind "BLASTER" oder "SASSER". Diese senden von einem infizierten PC aus speziell präparierte Datenpakete an zufällig gewählte Internetadressen. Trifft das Datenpaket auf z.B. Windows 2000 oder Windows XP mit einer Sicherheitslücke, so wird der Wurm auf dem Zielsystem sofort aktiv und er beginnt unmittelbar nach der Infektion damit, selbst infizierte Datenpakete weiter zu versenden.
Virensignatur	Um Viren und andere Schädlinge exakt zu erkennen, entwickeln die Viren-Analysten zu jedem bekannten Schädling eine Art Fingerabdruck
Spyware	Software, die sich wie ein "Spion" im System festsetzt und private Daten auf dem infizierten PC an dessen Absender bei Abruf sendet. Spyware-Tools sind häufig Teil einer vermeintlichen Freeware oder Shareware, bei der der Anwender keinen expliziten Hinweis bei der Installation erhält oder dies nur versteckt im Text der Lizenzvereinbarung ersichtlich ist. Der Spion verrichtet seinen Dienst im Hintergrund und fällt deshalb nicht auf, da es ja dessen Zweck ist, möglichst unerkannt zu operieren.
Hijacker-Tool	Meistens ein Browser-Spion, dessen Fenster sich notorisch vor ein ausgewähltes Fenster einer aufgerufenen Internetseite setzt und keine Möglichkeit lässt, dies zu verhindern. Teilweise wird dem Benutzer vorgegaukelt, er rufe die korrekte Internetseite auf, um weitere Informationen oder Passwörter auszuspionieren. Es können auch andere Startseiten im Browser eingetragen werden (meistens Internet Explorer), die sich nicht mehr ändern lassen. Außerdem leiten Hijacker Suchanfragen oder Adresseingaben auf andere Webseiten um und stehlen einem damit die Kontrolle über den Browser.