

Glossar zu Computerviren

Zusammenstellung: BSI - Bundesamt für Sicherheit in der Informationstechnik

BIOS

BIOS (engl. Abkürzung von **B**asic **I**nput **O**utput **S**ystem) Steuert die Hardware-Komponenten von Hardware-Herstellern und speichert diese im CMOS-RAM.

Boot-Sektor

Dieser Sektor ist auf Festplatten und Disketten (auch Daten-Disketten) vorhanden und enthält ein Ladeprogramm für das Betriebssystem und eine Tabelle zum physikalischen Aufbau der Diskette. Er wird im Inhaltsverzeichnis des Datenträgers nicht angezeigt.

Boot-Viren

Boot-Viren setzen sich in Bereiche der Datenträger, die beim Start des Rechners bearbeitet werden. Bei der Diskette ist das der Boot-Sektor, bei der Festplatte der Partition-Sektor (engl. Master Boot Record, MBR) oder der Boot-Sektor. Die Viren werden durch einen Kalt- oder Warmstart (bzw. bei Daten-Disketten auch erfolglosem Boot-Versuch) aktiviert.

CERT

Anlauf- und Beratungsstelle für Computer-Notfälle (engl. Abk. von computer emergency response team).

CMOS-RAM

Spezieller Speicher im Computer, in dem technische Daten über die Ausstattung des Rechners und andere Informationen auch nach dem Ausschalten gespeichert bleiben. Programme können in diesem Speicher nicht laufen. Er kann daher auch keine Viren enthalten, diese können allerdings die dort gespeicherten Daten löschen oder verändern.

Companion-Virus

Virus nutzt die Hierarchie des Betriebssystems beim Aufruf von Programmen aus und erzeugt namensgleiche Dateien mit seinem Code, die bei Aufruf des Programms dann zuerst ausgeführt werden (z.B. FORMAT.COM zusätzlich zu FORMAT.EXE).

CRC

standardisiertes Verfahren zur Berechnung von Prüfsummen (engl. Abk. von "cyclic redundancy check").

Falltür (Hintertür)

Funktion eines Programms, bei dem eine nicht dokumentierte Funktion dem Kundigen (z.B. dem Entwickler) zur Verfügung steht (Beispiel: Zugangskontrollprogramm mit Passwort, bei dem sich vom Anwender

gewählte Passwörter mit nicht dokumentierten Funktionen umgehen lassen).

FAT

Die FAT enthält die Zuordnung zwischen dem Datei-Namen und dem zugehörigen Speicherplatz auf dem Datenträger (engl. Abk. von "file allocation table", deutsch: "Datei-Zuordnungs-Tabelle").

File-System

Art der Verwaltung der Dateien (englisch "files") auf Festplatten. Viele DOS-Viren funktionieren nur mit dem FAT-System, nicht mit NTFS (Windows NT) und HTFS (OS/2) oder anderen.

File-Viren

Viren sind in einem Programm (Wirts-Programm) enthalten und werden durch Aufruf eines Wirts-Programms aktiviert.

Heuristik

Mit dem Begriff "Heuristik" wird ein Suchverfahren bezeichnet, bei dem Programme nach "verdächtigen" Befehlsfolgen durchsucht werden, also nicht nach bekanntem Viren-Code.

Informationstechnik (IT)

Die IT umfasst alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen.

Label

Das Programm LABEL verändert, den beim Formatieren einer Diskette oder Festplatte, festgelegten Volume-Namen.

logische Bombe

Manchmal Bezeichnung des Sonderfalls eines Trojanischen Pferdes: Programm, dessen Schadensfunktion von einer logischen Bedingung gesteuert wird, z.B. dem Datum; der Spezialfall einer zeitlichen Bedingung wird auch als "Zeitbombe" (*time bomb*) bezeichnet.

Makro

Befehlsfolge oder kurzes Programm zur Vereinfachung für häufig benötigte Aufgaben. Zur Ausführung wird nur der Makro-Name aufgerufen.

Makro-Virus

Virus, der in einer Programmiersprache für Makros geschrieben wurde (z.B. Word-Basic).

Multipartite-Virus

Virus, der sich über verschiedene Ausprägungen seines Wirtes verbreiten kann (z.B. sowohl als Boot-Virus als auch als File-Virus)

Partition-Sektor

Erster physikalischer Sektor von Festplatten, der eine Tabelle mit der logischen Organisation (Partitionierung) der Festplatte sowie ein Programm zur Auswertung der Tabelle enthält. Er wird im Inhaltsver-

zeichnung nicht angezeigt. Mit der Abarbeitung des Programms beginnt das Laden des Betriebssystems von Festplatte.

permanenter Schreibschutz (bei Disketten)

Disketten, die beim Format 5,25" keine Schreibschutz-Kerbe und beim Format 3,5" keinen Schreibschutz-Schieber aufweisen, so dass sie ohne weitere Maßnahmen nur gelesen und nicht beschrieben werden können.

polymorpher Virus

Virus, dessen Code durch unterschiedliche Reihenfolge und Verwendung von Maschinenbefehlen (bei gleicher Wirkung) gekennzeichnet ist.

Programm mit Schadensfunktionen (malicious software)

Alle Arten von Programmen, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige Veränderungen unkontrollierbare Schäden an Programmen und Daten bewirken und somit zusätzliche Arbeit und Kosten verursachen oder Vertraulichkeit und Verfügbarkeit von Daten oder Programmen negativ beeinflussen.

Prüfsummen-Programm (Integritäts-Tester)

Programm, das Veränderungen an Dateien oder anderen Datenblöcken (z.B. durch Viren oder andere Manipulationen) mittels einer Prüfsumme feststellen kann.

residenter Virus

Virus, der nach Aktivierung bis zum Ausschalten des Rechners im Hauptspeicher aktiv bleibt.

RISC-Prozessoren

RISC-Prozessoren sind Prozessoren mit einem eingeschränkten Befehlsatz. RISC-Prozessoren werden für spezielle Aufgaben in so genannten "Hochleistungs-Computern" eingesetzt.

ROM

Festwertspeicher (engl. Abk. von "read only memory").

Selbstverschlüsselnder Virus (selbst kryptierender Virus)

Virus verschlüsselt (kryptiert) seinen Code mit festem oder wechselndem Schlüssel.

Tarnkappen-Virus (Stealth-Virus)

Residenter Virus, der seine Anwesenheit im infizierten System durch Manipulation des Betriebssystems zu verbergen versucht.

Trigger

Auslösebedingung, bei der bestimmte Aktionen (z.B. eine Schadensfunktion) ausgeführt werden.

Trojanisches Pferd

Selbständiges Programm mit einer verdeckten Schadensfunktion, ohne Selbstreproduktion.

TSR

Zusätzliche Routine, die im Speicher resident verbleiben kann, wie z.B. der Maus-Treiber (engl. Abk. von " **terminate, stay resident**", deutsch: "beenden, aber (im Speicher) anwesend bleiben").

Viren-Suchprogramm (Scanner)

Programm, das bei Aufruf Datenträger, Systembereiche, Unterverzeichnisse oder Dateigruppen und einzelne Dateien nach bekannten Viren durchsucht. Dies geschieht entweder mittels fester Zeichenfolgen (Signaturen), spezieller Algorithmen oder heuristischer Verfahren.

Virus

Nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen (payload, damage) des Virus vorhanden sein.)

Wurm

Selbständiges, selbst reproduzierendes Programm, das sich in einem System (vor allem in Netzen) ausbreitet.

Weitere Informationen zur Computersicherheit über das
BSI - Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185 - 189, 53175 Bonn