
VTC
VIRUS
TEST
CENTER

# Computerviren bedrohen den PC

***Eine Einführung von***
***Torsten Dargers***
***und Michaela Schröder***

INHALTSVERZEICHNIS







## Was sind Computerviren ?

*Computerviren sind von Menschen geschriebene Programmsegmente, die sich selbst reproduzieren, indem sie sich an andere Programme anhängen. Fast immer enthalten Computerviren einen Programmteil, der Schaden verursacht.*

Man unterscheidet zwischen Programmviren und Systemviren.

**Programmviren** fügen sich in bestehende Programmdateien auf Diskette bzw. Festplatte ein. Dabei wird das bestehende Programm um den Virus erweitert. Wird ein infiziertes Programm gestartet, so wird vor der Ausführung des eigentlichen Programmes der Virus aktiviert. Programmviren kommen also erst beim Starten von Programmdateien zur Ausführung.

**Systemviren** befallen Systembereiche von Disketten und Festplatten. Bei solchen Systembereichen handelt es sich um den sogenannten Bootsector bzw. Master-Boot-Sector (Partitionstabelle). In diesen Bereichen befinden sich Programmteile, die schon beim Starten des Computers ausgeführt werden. Infiziert ein Computervirus einen solchen Bereich, wird der Virus aktiviert, sobald der Computer eingeschaltet wird. Systemviren befinden sich i.d.R. nicht in Programmdateien.

## Welche Schäden entstehen durch Computerviren ?

*Das Ausmaß von Schäden durch Computerviren reicht von einfachen Bildschirmanimationen bis zur Zerstörung aller Programme und Daten auf Disketten und Festplatten.*

Programmviren verändern Programmdateien, so daß nach einer Infektion keine Aussage über die Zuverlässigkeit des infizierten Programmes gemacht werden

kann. Von Viren infizierte Programme können z.T. nicht mehr fehlerfrei ablaufen. Häufig bemerkt der Benutzer einen Fehler nicht sofort, sondern erst später, wenn er den fehlerhaften Programmteil benutzt.

Einige Computerviren **stören gezielt den Arbeitsablauf** am Computer. Hier einige Beispiele:

Der *Herbstlaubvirus* (auch Cascade bzw. 1701-Virus genannt) läßt die Buchstaben auf dem Bildschirm nacheinander nach unten fallen, wo sie sich anhäufen. Bei jedem Auftreffen eines Buchstabens auf den unteren Bildschirmrand ertönt aus dem eingebauten Lautsprecher ein Klicken. Die Bildschirmanzeige wird unlesbar und ein weiteres Arbeiten ist schwer möglich. Startet ein Benutzer den Computer an dieser Stelle neu, so ist jede nicht gesicherte Datei verloren. Im schlimmsten Fall kann eine benutzte Datenbank zerstört werden, da die Datenbankdateien nicht ordnungsgemäß geschlossen wurden.

Der *MIX-1 Virus* stört das Ausdrucken von Texten und Grafiken auf einem Drucker. Er ersetzt dazu auszudruckende Buchstaben über eine Tabelle durch andere Buchstaben.

Z.B. wird der Text

"Sehr geehrte Damen und Herren"

ersetzt durch

"Rahr gaahrta Deman ond Harran"

Damit kann der infizierte Computer für Geschäftsbriefe nicht mehr verwendet werden.





Andere Computerviren **zerstören Daten auf Disketten bzw. Festplatten.** Hierzu ebenfalls einige Beispiele:

Der *DATACRIME-II Virus* führt bei einer Aktivierung zwischen dem 13. Oktober und dem 31. Dezember jeden Jahres (außer montags) eine Low-Level-Formatierung der ersten Spuren der Festplatte durch, so daß ein Benutzer auf die Daten der Festplatte nicht mehr zugreifen kann und die Festplatte neu einrichten muß.

Der *Michelangelo Virus* zerstört jedes Jahr am 6. März, dem Geburtstag des italienischen Bildhauers und Malers Michelangelo Buonarotti, den Datenträger. Dazu werden bei PCs mit CMOS-Uhr auf den Festplatten die Sektoren 1-17; Kopf 0-3; Track 0-256, d.h. einige Mega-Bytes, mit unsinnigen Werten überschrieben. Bei Disketten zerstört dieser Computervirus, abhängig vom Format, die Sektoren 1-9 bzw. 1-14.

Die Zerstörung von Daten durch Computerviren kann fatale Folgen haben.

Werden z.B. in einem Versicherungsunternehmen sämtliche Kundendaten gelöscht, ist ein weiteres Arbeiten des Versicherungsbetriebes nicht möglich, falls keine Datensicherung vorgenommen wurde.

Ebenfalls kann die Zerstörung von Daten fatale Folgen für Patientendateien in Krankenhäusern haben. Gehen dort Eintragungen über lebenswichtige Medikamente für bestimmte Patienten verloren, ist eine Versorgung dieser Patienten mit diesen lebensnotwendigen Medikamenten nicht mehr gewährleistet.

## Wie lassen sich Computerviren entdecken ?

Viele Computerviren lassen sich durch verschiedene Methoden entdecken. Eine sichere Methode alle Computerviren zu entdecken existiert nicht.

**Auf jeden Fall muß der Computer vor der Suche nach Computerviren von einer nicht infizierten, schreibgeschützten Originaldiskette durch einen Kaltstart gestartet werden.**

Ein Benutzer kann das **Verhalten des Computers** beobachten. Tritt ein anomales Verhalten auf, kann die Ursache in der Existenz eines Computervirus liegen. Verlängern sich beispielsweise Programmdateien durch Computerviren, so kann diese Verlängerung durch den Befehl DIR angezeigt werden. Außerdem können die Zeit-/Datumsangaben der Programmdateien mit denen der Programme auf den Originaldisketten verglichen werden. Sollten hier Abweichungen auftreten, *kann* die Ursache hierfür in der Existenz eines Computervirus bestehen. Leider können nicht alle Computerviren auf derart einfache Art und Weise nachgewiesen werden, da z.B. Stealth-Viren ihre Existenz verschleiern.

Weiterhin kann ein Benutzer **Virensuchprogramme (Virenscanner)** einsetzen. Dabei handelt es sich um Programme, die gezielt nach bestimmten Merkmalen in Programmdateien und Systembereichen suchen, die typisch für das Auftreten bestimmter Viren sind.

Virenscanner erkennen nur bekannte Viren. Die Zahl bestehender Viren steigt stetig, so daß Virenscanner vom Hersteller stets überarbeitet werden müssen, damit neue Viren erkannt werden können. Ein Benutzer sollte nur die neuste Version eines Virenscanners einsetzen.





Die Qualität von Virenscannern wird bestimmt durch die Zuverlässigkeit im Erkennen von Viren und die Anzahl der erkannten Viren. Bei der Suche nach Viren in Programmen kommt es vor, daß ein Virenscanner einen Virus meldet, dieser aber nicht vorhanden ist. In diesem Fall weist das Programm ein Merkmal auf, das mit einem Virus-Merkmal übereinstimmt. Solche "FALSE POSITIVES" (Fehlalarme) lassen sich nie ausschließen.

Findet ein Virenscanner einen Virus, sollte der Benutzer Ruhe bewahren und überlegen was zu tun ist, z.B. mit einem weiteren Virenscanner prüfen, ob es sich wirklich um einen Computervirus handelt.

Zur Erkennung von Computerviren können auch **Prüf- / Checksummenprogramme** eingesetzt werden. Diese Programme errechnen für jede Programmdatei eine Prüfsumme und speichern diese in einer Datei. Infiziert ein Computervirus eine Programmdatei, ändert sich (fast immer) die Prüfsumme der Programmdatei, was durch erneutes Prüfen herausgefunden werden kann.

Wurde eine Programmdatei verändert, so kann die Ursache hierfür ein Computervirus sein. Die Veränderung kann aber auch andere Ursachen haben. Einige Programme verändern z.B. ihre eigene Programmdatei um sich Benutzereinstellungen zu merken. Bei diesen Programmen kann die Ursache für die Veränderung der Programmdatei nicht sicher angegeben werden. Im Zweifelsfall sollte zusätzlich ein Virenscanner eingesetzt werden.

Leider lassen sich auch Prüf- / Checksummenprogramme von Stealth-Viren überlisten.

## Wie lassen sich Computerviren entfernen ?

*Computerviren in Programmdateien lassen sich nur durch Löschen aller infizierten Programmdateien sicher entfernen.*

**Dazu muß der Computer von einer nicht infizierten, schreibgeschützten Originaldiskette durch einen Kaltstart gestartet werden.**

Nur so kann ausgeschlossen werden, daß beim Starten des Computers der zu entfernende Virus automatisch (z.B. in der Datei CONFIG.SYS bzw. AUTOEXEC.BAT) aktiviert wird. Viele Benutzer scheuen eine Neuinstallation gelöschter Programmdateien und versuchen, den Virus mit sogenannten **Antiviren / Cleanern** zu entfernen.

Antiviren / Cleaner sind Programme, die in der Lage sein sollen, Viren zu entfernen. Dabei können nur bekannte Viren entfernt werden. Beim Entfernen eines Virus aus einer infizierten Programmdatei versucht der Antivirus / Cleaner die ursprüngliche Programmdatei wiederherzustellen. In einigen Fällen gelingt dieses sogar.

Leider kann ein Benutzer nicht prüfen, ob ein Programm durch einen Antivirus / Cleaner vollständig fehlerfrei wiederhergestellt werden konnte. Fehler beim Versuch, den Virus aus der Programmdatei zu entfernen, können zu Fehlern im Ablauf des bereinigten Programms führen.

Systemviren lassen sich am sichersten durch Experten oder durch den Einsatz von Antiviren / Cleanern entfernen

Nach dem Starten des Computers von einer **schreibgeschützten Startdiskette** beseitigt der DOS-Befehl

**SYS C:**





einen Bootsector-Virus auf der Festplatte C:.

Zum Entfernen von Master-Bootsector-Viren kann der DOS 5.0-Befehl

**FDISK /MBR** benutzt werden.

Dieser DOS 5.0-Befehl kann unabhängig von der installierten DOS-Version benutzt werden.

## Wie kann man sich vor Computerviren schützen ?

*Computerviren verbreiten sich zumeist über Datenträger. Wird auf einem Computer niemals eine "fremde" Diskette eingelegt, keine Software aus Mailboxen verwendet und stets nur Originalsoftware installiert, haben Viren wenig Chancen.*

Wird dagegen ab und zu einmal neue Software von "guten Bekannten" ausprobiert, steigt die Wahrscheinlichkeit einer Infektion.

Viele Viren verbreiten sich über den **Bootsector von Disketten.** (Auch Datendisketten haben einen Bootsector.) Wird der Computer gestartet, prüft der Computer, ob eine Diskette in Laufwerk A: eingelegt ist. Von dieser Diskette wird dann der Bootsector geladen und ausgeführt. Ein Bootsector-Virus auf einer Diskette wird dabei sofort ausgeführt. Kommt dann eine Meldung, diese Diskette enthalte kein Betriebssystem und man solle die Diskette aus dem Laufwerk entfernen und eine Systemdiskette zum Starten einlegen, wurde der Virus längst aktiviert und hat sich eventuell schon auf die Festplatte übertragen.

**Aus diesem Grund sollte vor jedem Start des Computers sichergestellt werden, daß sich in Laufwerk A: entweder die *korrekte Bootdiskette* oder *keine Diskette* befindet.**

**Programmviren** verbreiten sich beim Starten von infizierten Programmen.

Vor dem Starten neuer Programme sollten diese Programme mit einem aktuellen Virenscanner auf Viren untersucht werden. Wird dabei ein Virus gefunden, sollte das Programm sofort gelöscht werden, damit der Virus nicht zur Ausführung gelangen kann.

In **regelmäßigen Abständen** sollte die lokale Festplatte auf Viren untersucht werden. Dazu muß ein Kaltstart des Computers durchgeführt und von einer virenfreien, schreibgeschützten Originaldiskette gestartet werden.

Erst dann sollte ein Virensuchprogramm eingesetzt und die gesamte Festplatte nach bekannten Viren durchsucht werden. Auch der Einsatz von Prüfsummenprogrammen ist sinvoll. Mit diesen können Veränderungen an Programmdateien festgestellt werden. Für jede Veränderung einer Programmdatei sollte nach der Ursache der Veränderung gesucht werden. Läßt sich eine Veränderung nicht erklären, (z.B. durch Software-Updates, selbsttätiges Verändern des Programmes oder Compilation) sollte zusätzlich ein Virensuchprogramm eingesetzt werden und das Verhalten des Rechners beobachtet werden.

Den besten Schutz gegen Computerviren bilden lokale Computernetzwerke (LAN), bei denen ein verantwortungsbewußter Systembetreuer die zu benutzende Software im Netzwerk installiert und bei denen die Arbeitsplätze (Workstations) **keine Diskettenlaufwerke** enthalten. Nur diese Arbeitsstationen sind vor dem Einlegen virenifizierter Disketten sicher.





In Computernetzwerken sollten die Zugriffsrechte für **alle Benutzer auf ein Minimum** reduziert werden. Für Programmdateien sollten nur LESERECHT existieren.

Unter Novell-Netware™ sollten maximal die Rechte [Read, Find] vergeben werden. Der Supervisor sollte eine eigene virenfreie, schreibgeschüzte Bootdiskette haben und sich nur nach Booten von dieser Diskette aus einloggen. Verlangt ein Programm Schreibrechte im Programmverzeichnis, sollten alle *.COM, *.EXE und *.BAT Dateien in diesem Verzeichnis auf ReadOnly gesetzt werden und das Recht [Modify] allen Benutzern entzogen werden. Dann darf auch das Recht [Write] vergeben werden.

Die maximal zu vergebenden Rechte sind also entweder

[Read Find] oder

[Read Write Find], wenn alle Programmdateien mit den Befehlen

FLAG *.EXE RO
FLAG *.COM RO
FLAG *.BAT RO

auf Readonly gesetzt wurden.

Nach Vergabe dieser Rechte bildet nur die Supervisorkennung eine Sicherheitslücke. Aus diesem Grund sollte der Supervisor zum "normalen Arbeiten" eine Kennung besitzen, die ebenfalls in den Rechten (wie oben) eingeschränkt ist.

Viele Firmen stellen ihren Mitarbeitern inzwischen Stand-alone "Sozial-PCs" zur Verfügung, auf denen eigene Software z.B. Spiele installiert werden dürfen.

Tummeln sich auf diesem "Sozial-PC" die Viren, hat dieses keinerlei Auswirkungen auf die Computer die für den Firmenbetrieb benutzt werden. (Vorausge-

setzt, diese haben kein Disketten-laufwerk.)

Einen weiteren Schutz gegen Computerviren bilden die sogenannten **Speicher-Monitore**. Dabei handelt es sich um Programme, welche sofort nach dem Starten des Computers aktiviert werden, z.B. in der Datei CONFIG.SYS. Diese übernehmen dann die Kontrolle über alle Schreibzugriffe auf die Festplatte. Stellen diese Monitore Schreibzugriffe auf Programmdateien fest, melden sie dieses dem Benutzer, der dann entscheiden kann, ob der Schreibzugriff zugelassen oder verhindert werden soll. Monitore erscheinen auf den ersten Blick ein sinnvolles Instrument der Virenbekämpfung zu sein, aber die ständige Aufforderung an den Benutzer zu entscheiden, ob ein Zugriff erlaubt sein soll oder nicht, empfinden viele Programmierer auf Dauer als störend, da sie häufig Programmdateien verändern.

## Welche Arten von Computerviren gibt es ?

Computerviren lassen sich nach Techniken klassifizieren, die sie benutzen.

Sehr viele Computerviren **fügen** den Virus an bestehende Programme **an**, indem sie die Programmdatei verlängern. Im Gegensatz dazu **überschreiben** einige Viren einen Teil des ursprünglichen Programmes, so daß dieses nicht mehr ablauffähig ist.

**Direct-Action-Viren** infizieren bei der Ausführung des infizierten Programmes sofort weitere Programmdateien und führen eine eventuell vorhandene Schadensroutine sofort aus (u.U. nur bei Eintreten bestimmter Bedingungen, wie Zeit/Datum, Zähler etc.). Nach der Ausführung übergibt der Virus die Kontrolle an das ursprüngliche Programm und entfernt sich aus dem Hauptspeicher. Der Virus führt





seine Aktion(en) direkt nach dem Programmstart aus.

Im Gegensatz dazu bleiben die meisten Viren im Hauptspeicher **resident**, um jederzeit das System zu kontrollieren, z.B. Festplattenzugriffe, Tastatureingaben, Druckeransteuerungen etc. Residente Viren bleiben also nach der Ausführung aktiv und können eine Schadensroutine oder weitere Infektionen zu späteren Zeitpunkten ausführen.

Der Benutzer wird zwischen der Ausführung des infizierten Programms und einem Schaden, der nach Beendigung des infizierten Programms auftritt, keinen Zusammenhang erkennen. Ein residenter Virus kann, vom Zeitpunkt seiner Aktivierung an, jederzeit neue Programmdateien infizieren. Schon das Kommando DIR führt bei einigen residenten Viren zu einer Infektion. Residenz ist die Voraussetzung für einige weitere Techniken.

**Stealth-Viren** versuchen ihre Anwesenheit im System zu verschleiern. Dazu überwachen sie z.B. Zugriffe auf Programmdateien und das Inhaltsverzeichnis.

Versucht das Betriebssystem, z.B. beim Befehl DIR, die Größe einer infizierten Programmdatei zu ermitteln, subtrahiert der Stealth-Virus von der tatsächlichen Dateilänge die Länge des Viruscodes und täuscht so eine korrekte Programmlänge vor. Wird eine Programmdatei nicht ausgeführt, sondern nur gelesen, z.B. von einem Virenscanner, entfernt der Virus aus der zu lesenden Datei den Viruscode, so daß der Virenscanner den Virus nicht in der Programmdatei finden kann.

Alle Stealth-Viren nutzen die Technik der Residenz, um die Zugriffe des Betriebssystems zu kontrollieren.

Viele Viren **verschlüsseln** inzwischen bei einer Infektion den ge-

samten Virus oder Teile davon (z.B. lesbare Zeichenketten). Dabei verwenden einige Viren bei jeder neuen Infektion neue Schlüssel zum Ver-/Entschlüsseln. Solche **polymorphen** Viren verhindern, daß Virenscanner nach einer speziellen, für den Virus typischen Bytefolge suchen können. Ein Beispiel hierfür sind Viren, die die sogenannte "Mutation Engine" enthalten, ein Modul, welches polymorphe Viren erzeugt.

Um Monitorprogramme zu umgehen, versuchen einige Viren sich zwischen BIOS und Monitorprogramm einzuklinken. Dazu unterwandern sie die Monitorprogramme mit einer Technik, die als **Tunneling** bezeichnet wird. Da solche Viren vor dem Monitorprogramm aktiv werden, kann ein Monitorprogramm ihre Aktivitäten nicht feststellen.

**Slow Viren** infizieren nur Programme, während diese geändert werden. Erzeugt ein Compiler ein Programm, so wird dieses noch während der Generierung durch den Compiler vom Virus infiziert. Da der Virus das Programm während der Generierung infiziert, kann ein Benutzer das infizierte Programm nicht mit einem Originalprogramm vergleichen.





Impressum

Universität Hamburg
Fachbereich Informatik
Virus-Test-Center
Vogt-Kölln-Straße 30
2000 Hamburg 54 (ab 1.Juli 1993 22527 Hamburg )

Telefon: ☎ 040 / 547 15 - 234
☎ 040 / 547 15 - 405

Fax: ☎ 040 / 547 15 - 226

Mailbox: ☎ 040 / 547 15 - 235

(In der Mailbox sind aktuelle Virenscanner zum Download verfügbar)

Spenden an das Virus-Test-Center bitte an die
Landeshauptkasse Hamburg, Kto-Nr. 101 600
Hamburgische Landesbank, BLZ 200 500 00
Stichwort: 34013 Prof. Brunnstein / FB Informatik