

Was ist eigentlich ein Virus?

Prof. Dr. Fred Cohen, der Erfinder des Computervirus, definierte ihn einmal so:

Ein Computervirus ist ein Programm, das andere infizieren und verändern kann, um möglicherweise veränderte Versionen von sich selbst hinzuzufügen.

Die heute übliche Definition lautet:

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.

Ein Computervirus ist also - genau genommen - kein eigenständiges Programm, sondern eine Abfolge von aneinander gereihten Zeichen, die für sich genommen nicht ausführbar ist. Im Gegensatz zu Würmern und Trojanern, die "echte" Programme (z.B. .exe-Dateien) sind, können Sie einen Virus im Dateimanager nicht aufspüren.

Hin und wieder taucht die Frage auf, ob ein Virus PC-Hardware beschädigen oder gar den Computer zerstören kann. Die Antwort ist ein klares Nein. Es ist kein Virus bekannt, der dazu in der Lage wäre. Meldungen, die besagen, dass ein Virus den Prozessor zerstört indem er eine x-te Potenz erzeugt oder das Druckerkabel zum Schmelzen bringt weil er die anliegende Spannung erhöht, sind technischer Unsinn. Solche Meldungen fallen in den Bereich der "Hoaxes" (s. weiter unten).

Viren können sich auf unterschiedlichen Wegen verbreiten. Früher war die Diskette der häufigste "Überträger", später erweitert um die CD-ROM und andere externe Datenträger. Zwar werden auf diesem Weg noch immer massenhaft Viren verbreitet, doch die größten "Virenschleudern" sind heute Netzwerke aller Art. Angefangen vom Firmen- oder Behördennetzwerk bis zum größten aller Netze, dem Internet. Unangefochtener Spitzenreiter ist dabei die Virenverbreitung über E-Mail.

Mittlerweile gibt es so viele verschiedene Virenarten, Variationen, Mischformen etc., dass eine sinnvolle Klassifizierung von Computerviren kaum noch möglich ist. Einige wenige Grundbegriffe sollen hier dennoch erläutert werden.

Was sind Bootsektorviren?

Ein Bootsektorvirus lagert die am Anfang der Festplatte (im Master Boot Record) gespeicherten Informationen, die für das Laden des Betriebssystems sorgen, auf eine andere Stelle auf der Festplatte aus. Diese Stelle markiert er als "fehlerhaft", so dass Betriebssystem und Programme nicht mehr in diesen Bereich schreiben. Neuere Bootsektorviren verschlüsseln den Original-Bootstrap oder die darin enthaltene Partitionstabelle. Dann nimmt der Virus die Stelle des Original-Bootstrap ein.

Bei jedem Hochfahren des PCs wird somit zunächst der Virus aktiviert und in den Arbeitsspeicher geladen. Der Virus "übernimmt" den PC und startet dann erst die eigentliche Bootroutine. Das geht so schnell, dass der User von all dem nichts merkt.

Der Virus bleibt die ganze Zeit über im Arbeitsspeicher und hat damit Zugriff auf alle an das System angeschlossenen Laufwerke, d.h. auf weitere Festplatten und vor allem auf das Diskettenlaufwerk.

Er kann jetzt jeden Bootsektor von nicht schreibgeschützten Disketten manipulieren und sich dadurch auf weitere (ungeschützte) Computer übertragen. Es müssen sich nicht einmal Programme oder Daten auf der Diskette befinden, denn auch eine scheinbar leere Diskette kann einen Bootsektorvirus enthalten.

Hat der Virus das Original-Masterbootprogramm beim Auslagern verschlüsselt, kann er nicht mehr entfernt werden. Ohne seine Entschlüsselungsroutine ist kein Zugriff auf die Daten auf den Disketten oder Festplatten möglich.

Bootsektorviren können auf allen möglichen Wegen auf den Computer eingeschleust werden. Da MS-DOS und die frühen "Windows"- Betriebssysteme heute aber nicht mehr als Serverbetriebssystem in Netzwerken eingesetzt werden und neuere Betriebssysteme die eigenständige Verbreitung dieser Viren verhindern, "vermehren" sich Bootsektorviren fast ausschließlich über externe Datenträger.

Was sind Hoaxe?

Hoaxe sind keine Viren, sondern Warnungen vor Viren (und anderen Schadprogrammen) - allerdings falsche Warnungen, vergleichbar mit Zeitungsenten. Was einmal als Scherz begann, hat sich mittlerweile zu einer regelrechten Plage entwickelt.

In diesen Hoaxen wird z.B. davor gewarnt, diese oder jene Datei oder eMail zu öffnen oder es wird empfohlen, unbedingt die Datei XY zu löschen. Meist wird dazu aufgefordert, diese Meldung an möglichst viele andere weiter zu leiten. Damit wird der Hoax auch noch zum digitalen Kettenbrief.

Es gibt Leute, die sich einen Spaß daraus machen, solche Falschmeldungen in die Welt zu setzen. Sie wollen Verwirrung stiften. Weniger erfahrene Computer-Nutzer können durch Hoaxe zu falschen Reaktionen verleitet werden (z.B. wenn sie der Aufforderung folgen, eine bestimmte Datei zu löschen).

Was sind Makroviren?

Makro-Viren werden in einer speziellen Programmiersprache geschrieben, die auf "BASIC" aufbaut. Beim Office-Paket der Firma Microsoft ist das "VBA" ("Visual Basic for Applications"). Diese Sprache ist nicht schwer zu erlernen, weshalb Makroviren noch immer zu den am weitesten verbreiteten Viren gehören.

Makros kommen überwiegend im Zusammenhang mit Office-Paketen zum Einsatz. Statt immer wieder die gleichen Arbeitsschritte abzuarbeiten, wird ein Makro erstellt, das diese Schritte "auf Knopfdruck" selbständig durchführt.

Bei dem Textverarbeitungsprogramm "Word" der Firma Microsoft wird die Datei "normal.dot" infiziert. Diese Datei hat die Aufgabe, die globalen Einstellungen dieser Textverarbeitung zu speichern. Von dort aus infiziert der Makrovirus alle .dot- und .doc-Dateien und verbreitet sich beim Austausch dieser Dateien. Das gilt analog für alle Programme eines Office-Paketes, die Makros verarbeiten können, also auch Tabellenkalkulationen oder Präsentationsprogramme. Verlassen Sie sich keinesfalls auf den in diese Programme integrierten "Makroviren-Schutz". Der kann von Viren relativ leicht umgangen werden.

Gegen Ende der 1990er Jahre machten Makroviren mehr als die Hälfte aller Viren aus. Heute sollte ihre Entdeckung einem modernen Virens scanner keine Probleme mehr bereiten. Ob die befallenen Dateien in jedem Fall auch wieder hergestellt werden können, steht allerdings auf einem anderen Blatt! Konnte sich ein Makro-Virus unbemerkt installieren, kann also u.U. die Arbeit von Wochen in Gefahr sein (etwa eine umfangreiche Diplomarbeit - möglichst noch ohne Backup).

Was sind TSR-Viren?

TSR heißt: "Terminate and Stay Resident" und bedeutet, dass sich diese Viren in den Arbeitsspeicher laden. Dort verbleiben sie, bis der Computer wieder ausgeschaltet wird. Als "speicherresident" bezeichnet man also keine bestimmte Virenart, sondern eine besondere Verhaltensweise ganz unterschiedlicher Viren.

Das klassische Beispiel für einen speicherresidenten Virus ist der Bootsektorvirus. Aber beinahe jede andere Virenart (z.B. Makroviren) kann diese spezielle Eigenschaft ebenfalls besitzen. Nichtresidente Viren werden nur aktiv, wenn das befallene Programm gestartet wird.

Einmal entdeckt, können sie deshalb relativ leicht "rückstandsfrei" entfernt werden. Im Gegensatz dazu haben TSR-Viren ganz andere Möglichkeiten. Sie können von sich aus Prozessaufrufe abfangen, externe Speichermedien manipulieren und allen erdenklichen Schaden im System anrichten, ohne dass der Anwender erst eine Aktion auslösen muss - und sie können, unter bestimmten Bedingungen, sogar die Formatierung (!) einer Festplatte "überleben".

Was sind Stealth-/Tarnkappen-Viren?

Virens Scanner legen für jedes Programm eine Prüfsumme an. Wird die Größe eines Programms (oder einer Datei) verändert, ändert sich sofort auch dessen Prüfsumme. Da Viren sich an ein Programm oder eine Datei anhängen, vergrößert sich das Wirtsprogramm bei einem Virenbefall automatisch.

Stealth-Viren versuchen nun, dem Virens Scanner vorzugaukeln, dass das befallene Programm gar nicht verändert sei, indem sie dem Scanner falsche Parameter übergeben.

Was sind Zeitzünder-/Trigger-Viren?

Das sind Viren, in die eine spezielle Routine einprogrammiert wurde, die den Virus erst bei Eintritt eines bestimmten Ereignisses oder dem Erreichen eines Datums aktiviert. Das kann das übernächste Hochfahren des Computers, ein bestimmter Tag oder auch erst ein Jahreswechsel sein.

"Reine" Zeitzünder-Viren gibt es nicht (das wäre auch ziemlich sinnlos). Viren, die über einen "internen Zähler" verfügen, besitzen immer auch andere Schadroutinen. Im Prinzip kann jede Virenart mit einem Zeitzünder versehen werden.

Was sind Zoo-Viren?

Zoo-Viren (auch Labor- oder Research-Viren genannt) sind, im Gegensatz zu ITW-Viren, nicht in freier Wildbahn anzutreffen, sondern in den Virenlaboren der Hersteller von Anti-Viren-Software. Sie werden zu Forschungs- oder Testzwecken erstellt. Der weitaus größte Teil aller Viren sind Zoo-Viren.

"Moderne" Viren vereinigen fast immer mehrere der o.g. Eigenschaften in sich. So ist der speicherresidente, polymorphe Tarnkappenvirus, der am nächsten Montag Ihre Festplatte formatiert, durchaus nichts Ungewöhnliches.

Zurzeit werden nur wenige wirklich neue Schadprogramme entdeckt. Die meisten aktuellen Schädlinge sind Variationen schon bekannter Viren, Würmer usw. Sie werden i.d.R. durch eine fortlaufende Buchstabenfolge gekennzeichnet, z.B. "Sobig", "Sobig.B", "Sobig.C" usw.

Was sind Würmer?

Computer-Würmer sind Programme zur Sabotage von Software, die sich oft in rasender Geschwindigkeit über die Computer-Netzwerke der Welt ausbreiten. Dabei unterscheiden sie sich vor allem in ihren Verbreitungsmöglichkeiten vom Computervirus: Während Viren für ihr zerstörerisches Werk immer einem "Wirt" anhängen müssen, haben Würmer ein eigenständiges "Fahrwerk".

Nur im Schlepptau gelangen Viren in andere Computer. Würmer hingegen können sich selbst auf den Weg machen. Dabei nutzen sie verschiedene Möglichkeiten. Die berühmt gewordenen Würmer "Melissa" oder "I love you" nutzten für ihre Verbreitung E-Mail Programme. Sie wurden aktiv, sobald der Adressat die E-Mail öffnete und schickten sich dann selbstständig an dessen Einträge im Adressbuch weiter. Der Wurm "Code Red" dagegen nutzte für sein Fortkommen Sicherheitslücken in Internet-Programmen, so genannte Verwundbarkeiten. Computer-Würmer der jüngsten Generation - wie etwa jetzt "Nimda" - stehen im Verdacht, sich über mehrere "Fahrwerke" zu verbreiten.

Was heißt Browser-Hijacker - 'Entführung' auf unerwünschte Suchmaschine

Das Entführen (das sogenannte Hijacking) auf nicht gewünschte Internetseiten ist nicht neu. Zweifelhafte Berühmtheit erlangt hierbei die 'Suchmaschine' Cool Web Search. Die hinter diesem Webangebot stehende Firma 'Coolwebsearch' (CWS) verbreitet immer neue Varianten trojanischer Pferde, mit dem Zweck den Surfer auf die eigene Seite umzuleiten.

Die erste Form des Hijacking's auf die Seiten von 'Coolwebsearch' wurde bereits im Mai 2003 entdeckt. Seit dem sind eine Vielzahl von Varianten hinzugekommen.

Dieses Hijacking nutzt eine Sicherheitslücke in veralteten Versionen der Virtual Machine von Microsoft aus. Daher ist auch nur der **Internet Explorer** von Microsoft hiervon betroffen.

Bei den meisten Hijacker-Varianten werden eine Reihe von Schlüsseln bzw. Werten in der Windows-Registrierung (Registry) geändert, die das Verhalten des Internet Explorers nachhaltig ändern. Da die Zahl der veränderten Schlüssel und/oder Werte ständig steigt verzichten wir an dieser Stelle auf eine Auflistung möglicher Veränderungen.

Neben den Änderungen im Internet Explorer wird häufig auch ein Trojaner installiert. Dieses sorgt dafür, dass die Veränderungen vom Anwender nicht ohne weiteres wieder rückgängig gemacht werden können. Änderungen, die der Anwender zurückstellt, sind nach einem Reboot des Systems wieder vorhanden. Ein anderer Trick der Browser-Hijacker ist es, sich bzw. die entführten Seiten in die Zone Vertrauenswürdigen Seiten des Internet Explorers zu legen. Hierdurch werden die Sicherheitseinstellungen der Zone Internet ausgehebelt, Javascript und ActiveX können ausgeführt werden, obwohl die Zoneneinstellungen korrekt sind. Ein weiterer möglicher unerwünschter Eingriff ist das Anlegen eines neuen Browser Helper Objects. Hierbei handelt es sich um ausführbare Programme die die Funktionen des Internet Explorers erweitern.

Mit dem BHO des Adobe Acrobat Readers ist der Internet Explorer zum Beispiel in der Lage, PDF-Dokumente direkt im Browserfenster anzuzeigen. Browser-Hijacker verwenden BHO's, um Internet-Anfragen auf eigene Seiten umzulenken.

Wie kann man das Browser-Hijacking vermeiden?

Am einfachsten ist es, in Zukunft auf den Internet Explorer von Microsoft zu verzichten. Dies hat zwei Gründe: Erstens wird der Internet Explorer von den weitaus meisten Anwendern benutzt, da er bei jedem einigermaßen aktuellen Betriebssystem von Microsoft automatisch mitinstalliert wird. Das wiederum hat zur Folge, dass gegen diesen Browser auch die meisten Angriffe unternommen werden. Zum Zweiten nehmen die Programmierer alternativer Web-Browser das Thema Sicherheit sehr ernst und haben ihre Browser wesentlich sicherer programmiert. Wie in den Hintergrundinformationen bereits beschrieben, ist es dort ohne aktive 'Unterstützung' des Anwenders nicht möglich, unerwünschte Programmiererweiterungen zu installieren.

Sicherere Alternativen zum Internet Explorer sind beispielsweise:

Mozilla (<http://www.mozilla.org>)
Mozilla Firefox (<http://www.mozilla.org>)
Opera (<http://www.opera.com>)
Firefox: <http://firebird-browser.de/>

Falsche, bzw. zu schwache Sicherheitseinstellungen in den Internetoptionen sind der Hauptgrund für die Ausführung dieser Schadprogramme. Hijacking ist zwar auch bei anderen Browsern wie z. B. Mozilla grundsätzlich möglich, es bedarf aber -im Gegensatz zum Internet Explorer- der aktiven "Unterstützung" durch den Surfer. Hier ist das gewollte Herunterladen und Installieren einer schädlichen Browsererweiterung (auch als PlugIn bekannt) erforderlich. Eine verborgene Installation aufgrund zu schwacher Sicherheitseinstellungen ist hier nicht möglich.

Wenn ein Browserwechsel nicht möglich oder nicht gewünscht wird

Viele Anwender scheuen sich nach wie vor, den Browser zu wechseln, oder sind beispielsweise aus beruflichen Gründen gezwungen, weiterhin den Internet Explorer zu verwenden. In solchen Fällen sollten zumindest die aktuellste Version (zur Zeit MSIE 6 inklusive Service Pack 1) verwendet und die Sicherheitseinstellungen überprüft und ggf. verstärkt werden. Hierzu stellt www.heise.de einen umfangreichen online Browser-Check (<http://www.heise.de/security/dienste/browsercheck/>) zur Verfügung. Zusätzlich sollte die Microsoft Java VirtualMachine gegen Java von Sun (<http://www.java.com/en/index.jsp>) ausgetauscht werden.

Das kostenlose englischsprachige Tool BHOdemon (http://www.pcworld.com/downloads/file_description/0,fid,23611,00.asp) kann den InternetExplorer vor unerwünschten Browser Helper Objects (BHO) schützen.

Einen Schutz gegen Veränderungen im laufenden Betrieb bietet das Tool Browser Hijack Blaster 1.0 (<http://www.majorgeeks.com/download.php?det=3786>). Das kostenlose englischsprachige Tool läuft im Hintergrund und meldet sich, wenn der Versuch unternommen wird, die IE Homepage, die IE Default Page, die IE Such Seite Page zu verändern, bzw. ein neues BHO zu installieren.

Das kostenlose englischsprachige Tool SpywareBlaster wurde -wie der Name schon sagt- in erster Linie zur Entfernung von Spy- und Adware entwickelt, kann mittlerweile aber auch die ungewollte Installation von vielen Browser-Hijackern verhindern, da es automatisch (ohne Benachrichtigung oder Nachfrage) die in der Datenbank aufgelisteten ActiveX-Elemente, Cookies und Webseiten blockt, sofern '*Enable all Protection*' ausgewählt wurde. Sollte das Blocken einzelner Seiten nicht gewünscht sein, braucht nur der Haken am Anfang der jeweiligen Zeile entfernt werden. (<http://www.javacoolsoftware.com/spywareblaster.html>)

Autovorschau von Outlook bzw. Outlook Express

Einige Browser-Hijacker werden über speziell präparierte HTML-Mails versandt. Benutzer von Microsoft Outlook bzw. Outlook Express sollten die Autovorschau deaktivieren. Bei aktivierter Autovorschau reicht das Markieren einer entsprechend präparierten Mail (zum Beispiel um sie zu löschen) aus, um das enthaltene destruktive Script auszuführen.

Was ist ein Trojanisches Pferd?

Trojanische Pferde sind Programme, die eine schädliche Funktion beinhalten. Nicht selten verfügen Trojanische Pferde über ein für Anwender sehr nützliche Funktion. Die schädliche Funktion läuft lediglich im Hintergrund ab, ohne dass dieses bemerkt wird.

Trojanische Pferde arbeiten nach verschiedenen Mustern. Zu einem gibt es Programme (Exe-Dateien), die keinerlei für den Anwender nützliche Funktionen aufweisen. Lediglich wird nach einem Start des vermeintlichen Programms ein Trojaner auf dem PC installiert. Damit kein Verdacht geschöpft wird, erscheinen Fehlermeldungen, dass eine bestimmte Datei nicht vorhanden ist, um das vorgegebene Programm zu starten.

Der Anwender löscht enttäuscht dieses unbrauchbare Programm und macht sich weiter keine Gedanken darüber.

Des Weiteren gibt es auch wesentlich "klügere" Trojanische Pferde, die sich hinter einem durchaus brauchbaren Programm verbergen. Wird das Programm installiert, kann es oft Monate dauern, bis ein Anwender bemerkt, dass sich ein schädliches Programm auf seinem System befindet.

Viele Trojaner installieren sich so auf dem System, damit dieses bei jedem Systemstart ebenfalls mitgestartet wird. - Somit läuft dieses Programm ständig im Hintergrund mit. Andere Trojanische Pferde starten erst, wenn ein bestimmter Vorgang (Start eines anderen Programms) auf dem System stattfindet.

Wozu sind Trojanische Pferde in der Lage, was können diese ?

Die meisten Trojaner sind darauf aus, Benutzerdaten eines Online-Dienstes auszuspähen, nicht selten nur von einem bestimmten Provider. Trojaner, die ständig im Hintergrund im betroffenen System mitlaufen, zeichnen mitunter sämtliche Tastaturfolgen auf. - Dieses bedeutet, alle Daten, die der Anwender über die Tastatur eingibt. - Hier nutzt es leider gar nichts, wenn der Anwender sein Passwort für einen Online-Dienst nicht abspeichert, sondern erst bei der Anmeldung eingibt. Die gesammelten Daten werden nach der Einwahl unbemerkt an den Autor des Trojanischen Pferdes geschickt.

Da die gesammelten Daten nach der soeben genannten Arbeitsweise, häufig viel zu gross und undurchsichtig für den Autor des Trojaners sind, arbeiten viele Trojanische Pferde weitaus intelligenter.

Die "besseren" Trojaner, zeichnen lediglich die Tastaturfolgen auf, die den "Hacker" interessieren. Dazu könnten Eingaben von Passwörtern für Online-Dienste/ Mail Accounts/ Webseiten/FTP/ Kreditkarten-Nr., Konten usw. gehören. - In einigen Fällen werden sogar Home-Banking-Programme überwacht und die Daten weitergeschickt. Für den Hacker hat es den Vorteil, er gelangt nur an die für ihn relevanten Daten und muss diese somit nicht aus einem riesigen "Datenberg" rausfiltern. Diese Arbeitsweise von Trojaner ist als sehr gefährlich einzustufen, da diese die Eigenschaften besitzen können, an sämtliche Daten eines Anwenders zu gelangen.

Des weiteren gibt es auch ein Vielzahl von Trojanischen Pferden, die nicht ständig im Hintergrund eines Systems mitlaufen: Diese Art von Trojanischen Pferden werden erst aktiviert, wenn der Anwender z.B. sein Programm für die Einwahl in einem Online-Dienst startet. Oder er ein sogenanntes Online-Tool verwendet, wenn er sich bereits online befindet.

Die dritte Art von Trojanischen Pferden nennt man auch ServerProgramme. - Diese Trojaner ermöglichen dem Hacker auf das betroffene System zuzugreifen. Diese Trojaner sind mit Abstand die gefährlichsten, die es zur Zeit gibt. Da diese Trojaner in Regel alle auf dieser Seite genannten Arbeitsweisen vereinen können.

Server-Programme sind zu folgendem in der Lage bzw. ermöglichen dem Hacker auf der "Gegenseite" zahlreichen Funktionen: Aufzeichnen der Tastaturfolgen, Auslesen von Passwörtern, herunter- und/oder hochladen von Dateien von/auf Dein System.

Der Hacker hat mitunter vollen Zugriff auf Deinen Rechner und kann fast alles machen, was er gerade möchte. Server-Programme bestehen aus einem Clienten (dieser wird benutzt um auf andere System zugreifen zu können) und dem eigentlichen Trojaner, dem Server.

Das Server-Programm öffnet auf Deinem System verschiedene sogenannter Ports, damit der Zugriff auf Dein System durch den Hacker möglich wird. Der Client ist dazu in der Lage nach aktiven "Servern" irgendwo im Internet zu scannen (suchen). Somit wird dem Hacker bekannt auf welche Systeme er zugreifen könnte.

Sie sehen, die Arbeitsweisen und Möglichkeiten eines Trojanischen Pferdes sind sehr breit gefächert. Auf alles bis in das letzte Detail einzugehen, würde den Rahmen dieser Seiten sprengen.

Wie macht sich ein Virus bemerkbar und wie verhalte ich mich.

Ist Ihr PC von einem Virus (oder einem anderen Schadprogramm) befallen, kann sich das auf unterschiedliche Weise bemerkbar machen - oder zunächst auch gar nicht! Hier folgt eine kurze, längst nicht vollständige Auflistung möglicher Anzeichen für einen Virenbefall.

Das **Booten** (Hochfahren) des Systems dauert länger als sonst. Einige Viren setzen sich so im System fest, dass sie bei jedem Booten mit gestartet werden. Bei leistungsfähigeren Computern fällt die Verzögerung aber nicht mehr auf.

Dateien werden verschoben, umbenannt oder in ihrer Größe verändert. Auch das wird man als "Normal-User" kaum bemerken.

Ungewöhnliche **Hintergrundaktivität**. Sie hören, dass auf die Festplatte zugegriffen wird, obwohl Sie in dem Augenblick gar nicht am PC arbeiten. Einige Programme nutzen jedoch solche "Arbeitspausen", um Scann- oder Sicherungsläufe durchzuführen.

Es steht insgesamt weniger als **640 KB** konventioneller DOS-Speicher zur Verfügung. Prüfen Sie diesen Wert, indem Sie den PC mit der Startdiskette booten und an der DOS-Eingabeaufforderung "MEM" (ohne Anführungszeichen) eingeben.

Ihr System stürzt noch häufiger ab als üblich. Beachten Sie aber, dass die Betriebssysteme der "Windows"-Reihe ganz allgemein gegen **"Abstürze"** und **"Einfrieren"** sowie deren Folgen nicht so gut geschützt sind wie andere Betriebssysteme, und dass es vielfältige Ursachen für diese Abstürze gibt.

Unsinnige oder nicht lesbare **Fehlermeldungen** oder **Schriftarten, Menüleisten, Icons** sind verändert oder vertauscht. Allerdings ist auch hier zunächst an Softwarefehler, missglückte Installationen, unvollständige Deinstallationen, Fehlbedienungen o.ä. zu denken.

Programme lassen sich nicht mehr starten oder beenden, der Computer reagiert auf Tastatureingaben oder Mausbewegungen nicht wie sonst. Aber auch hier werden überwiegend Software- oder Hardwarefehler vorliegen.

Mit einem Pop-Up-Fenster, einer Laufschrift o.ä. scheint sich ein Virus **selbst** zu melden. Doch nicht einmal das muss ein sicherer Beleg für die Anwesenheit eines Virus sein. Es gibt nämlich mehr oder weniger harmlose "Scherzprogramme", deren Programmierer meinen, dem Anwender einen Virenbefall (einen Hardwaredefekt, den Weltuntergang etc.) mitteilen zu müssen.

Diese Aufzählung ließe sich fortführen. Sie sehen, es ist beinahe unmöglich, ohne die Hilfe einer guten (aktuellen) Anti-Viren-Software einen Virenbefall im Vorfeld sicher festzustellen. Viele Viren sind völlig inaktiv, bis ein bestimmtes Ereignis eintritt oder ein Datum erreicht ist. Ob sich tatsächlich ein Virus auf Ihrer Festplatte befindet, der droht, in Ihrem System Schaden anzurichten, kann nur der Virens Scanner zweifelsfrei feststellen. Und der kann Ihnen diesen Plagegeist in aller Regel auch wieder vom Hals schaffen!

Die wichtigste Grundregel: Ruhe bewahren! Sie sind nicht der erste und auch nicht der letzte, dem das passiert. Ein Computervirus ist ein Ärgernis - aber solange der Computer nicht in Flammen steht, gibt es keinen Grund zur Panik. Das Schlimmste, das passieren kann ist, dass Sie Ihr Betriebssystem neu aufspielen müssen. Doch selbst das ist nur in wenigen Ausnahmefällen nötig (kommen Sie also um Himmels Willen nicht auf die Idee, bei der erstbesten Virenmeldung Ihre Festplatte zu formatieren!).

Handeln Sie also nicht vorschnell, wenn der Virens Scanner anbietet, den gefundenen Virus zu löschen. **Lehnen Sie dies zunächst ab.** Fahren Sie den PC **nicht herunter** und führen Sie auch **keinen Neustart** durch. Öffnen Sie **keine weiteren Programme.**

Wenn der Scanner die Möglichkeit bietet, den Virus in "Quarantäne" zu nehmen, sollten Sie diese Option nutzen. Der Virus wird dabei in ein besonderes Verzeichnis verschoben und jeder Zugriff auf ihn verhindert. Alternativ bietet mancher Scanner an, den Virus umzubenennen. Dabei wird die Dateierweiterung verändert, so dass der Virus nicht mehr aktiviert werden kann.

Wie Sie jetzt weiter vorgehen sollten, hängt im Wesentlichen von einer Frage ab: Wie aktuell und komplett ist Ihre Datensicherung?

Überlegen Sie daher zunächst in aller Ruhe, welche Daten Sie noch nicht in Ihre Datensicherung aufgenommen haben..

Möchten Sie auf bestimmte Daten, die Sie noch nicht gesichert haben, auf keinen Fall verzichten, sollten Sie diese Dateien jetzt auf externe Datenträger kopieren. Benutzen Sie dazu ausschließlich leere Datenträger, um nicht andere, bereits darauf befindliche Daten zu gefährden. Bedenken Sie, dass die Datensicherung, die Sie jetzt erstellen, virenverseucht sein könnte (markieren Sie diese Datenträger deshalb deutlich)! Dennoch ist es den Versuch wert, denn auch ein solches Backup ist mitunter noch zu retten.

Sind Sie nicht sicher, ob es sich tatsächlich um einen Virus handelt (vielleicht ist gerade Ihr Scanner für Fehlalarme "berühmt"), lassen Sie die verdächtige Datei zunächst in Quarantäne. Holen Sie für das weitere Vorgehen den Rat eines Fachmanns (oder einer Fachfrau!) ein. Das kann ein sachkundiger Bekannter oder auch die Hotline des Herstellers Ihres Virenschanners sein. Für Anfragen bei Hotlines gilt generell: Halten Sie alle nötigen Informationen bereit (welches Betriebssystem, welche Datei ist betroffen, bei welcher Aktion tauchte die Meldung auf, wie lautete die Meldung genau usw.).

Sie können sich auch bei Virenlisten im Internet, z.B. **Virenticker** oder **Viruslist** informieren. Mitunter hilft an dieser Stelle auch ein Blick in das Handbuch des Virenschanners.

Nachdem die Datensicherung abgeschlossen ist, und Sie sich vergewissert haben, dass es sich tatsächlich um einen Virus handelt, schalten Sie den Computer aus (keinen simplen Neustart, sondern tatsächlich für mindestens 10 Sekunden ausschalten!). Damit entladen Sie den Arbeitsspeicher, in dem sich möglicherweise noch Virencode befunden hat.

Ab der "Windows"-Version "WinME" sollten Sie vor dem Abschalten unbedingt die Funktion "Systemwiederherstellung" (unter: Systemsteuerung / System) deaktivieren. Ansonsten kann es passieren, dass "Windows" beim nächsten Booten, noch bevor Sie etwas unternehmen können, die reparierten Dateien wieder durch die ursprünglichen (verseuchten) ersetzt.

Starten Sie dann den Computer von der virenfreien und schreibgeschützten Startdiskette. Das ist wichtig, weil sich der Virus sonst u.U. gleich wieder in den Arbeitsspeicher laden würde und Sie würden diesen "Kameraden" nie los! Jetzt kann der Virenschanner seine Arbeit tun und den Virus entfernen. Zwar können alle modernen Virenschanner auch den Arbeitsspeicher prüfen, dennoch sollten Sie, um auf der sicheren Seite zu sein, den eben beschriebenen Weg einhalten!

Nachdem Sie Ihr System gesäubert haben, sollten Sie erneut einen "Kaltstart" durchführen, also den Computer für einen Moment ausschalten (vergessen Sie nicht, bei dieser Gelegenheit die Bootreihenfolge wieder umzustellen), und danach Ihre Festplatte noch einmal scannen - idealerweise zusätzlich durch einen zweiten Scanner. Insbesondere wenn es sich um einen Bootsektorvirus handelte, sollten Sie zusätzlich alle (es könnten mehrere befallen sein) externen Speichermedien auf Viren prüfen.

Konnten Sie den Infektionsweg nachvollziehen, informieren Sie ggf. denjenigen, der den Virus (in aller Regel ja unbeabsichtigt) weitergegeben hat.

Wenn Ihr Computer Teil eines Firmen- oder Behördennetzwerkes ist, ist die Vorgehensweise anders. Sie sollten den PC herunterfahren, also vom Netz nehmen, und sofort den Systemadministrator benachrichtigen. Versuchen Sie nicht, den Virus selbst zu löschen oder befallene Dateien/Programme zu desinfizieren. Da Sie i.d.R. nicht wissen können, welche Auswirkungen das auf das gesamte Netzwerk haben kann, überlassen Sie diese Arbeit dem Administrator! Der wird zwar nicht begeistert sein, aber wenn Sie durch eigene Reparaturversuche das Unheil noch vergrößern, könnten im Extremfall sogar Schadenersatzforderungen auf Sie zukommen.

Nach einem Virenbefall müssen Sie damit rechnen, dass das Schadprogramm unbemerkt Ihre Passwörter und andere geheime Login- oder Zugangsdaten über eine Online-Verbindung an andere übermittelt haben könnte. Ändern Sie deshalb sofort alle Passwörter (Sie sollten das ohnehin von Zeit zu Zeit tun)!

Schwieriger wird es, wenn der Virus auf Ihrem System aktiv ist, also schon ein Schaden entstanden ist oder gerade einer entsteht.

Sehen Sie den Virus bei der "Arbeit", ist der beste Rat wohl der: Schalten Sie den Computer unverzüglich aus und holen Sie auch hier sachkundigen Rat ein. Bei der Vielzahl der verschiedenen Viren, ihren unterschiedlichen Arbeitsweisen und Schadroutinen ist es unmöglich, für diesen Fall Patentrezepte bereitzuhalten.

An dieser Stelle noch mal nachdrücklich: Wenn Sie Ihr System regelmäßig scannen, der Hintergrundwächter ständig aktiviert ist, der Scanner durch Updates der Virendatenbanken aktuell gehalten wird und Sie sich für eine gute und bewährte Anti-Viren-Software entschieden haben, sollte es erst gar nicht so weit kommen!

Regelmäßig Windows Updates ausführen

Damit das Windows-Betriebssystem wenigstens mit den zur Verfügung gestellten Sicherheitspatches ausgestattet wird, ist ein regelmäßiges Windows Update (<http://windowsupdate.microsoft.com/de/>) erforderlich. Da Microsoft jeweils am zweiten Mittwoch im Monat neues Patches zur Verfügung stellt, sollte dies der maximale Zeitraum für den Besuch der Update-Seiten sein. Diese ist nur möglich aus dem Internet Explorer.