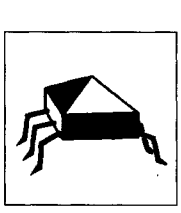


Computerviren – Technik, Vorbeugung, Bekämpfung

Thomas Hofer

Mit der zunehmenden Verbreitung der Informationstechnik und der fortschreitenden Vernetzung von Rechenanlagen wird es immer wichtiger, unberechtigten Zugang zu Programmen und Daten sowie mißbräuchliche Datenmanipulationen zu verhindern.

Problembewußtsein wecken

Dabei ist es dringend notwendig, neben der Entwicklung verbesserter Schutzmechanismen vor allem das Problembewußtsein bei den Anwendern zu schärfen und ihnen eine Hilfestellung zü geben. Dies gilt in besonderem Maße für die auf sich gestellten Benutzer der „Personal Computer", die schon seit geraumer Zeit in Angst und Schrecken versetzt werden, nicht zuletzt aufgrund einiger von den Medien aufgegriffener, durch Computerviren verursachter spektakulärer „Schäden"[1]. Festzuhalten ist, daß Computerviren eine wachsende Gefahr nicht nur für Programme, sondern vor allem für die in einem Computer gespeicherten Daten darstellen[2]. Dies schon deshalb, weil PCs – entsprechend ihrer schnell gestiegenen Leistungsfähigkeit – in zunehmendem Maße eingesetzt werden, um „sensible Daten" (etwa Finanz- und Rechnungsdaten, Unternehmensplanungen und Konstruktionspläne, vertrauliche Texte sowie Personaldaten) zu speichern. Die Zerstörung oder Verfälschung solcher Daten wie auch der Ausfall von Geräten oder Programmen würde solche Unternehmen empfindlich treffen.

Zur übereilten Panik oder zum Rückzug aus PC-Anwendungen – das darf schon jetzt gesagt werden – besteht keinerlei Anlaß. Grund für Ausfälle und Schäden, die durch Computerviren verursacht wurden, sind leider oft Unkenntnis und Nachlässigkeit im Umgang mit Computern beziehungsweise Programmen und Daten.

Praxisorientierte Hilfestellung

Nachdem in jur-pc 12/91, S. 1367 ff., bereits Wesen, Herkunft und Verbreitung von Computerviren sowie Möglichkeiten ihrer strafrechtlichen Erfassung und Bewertung dargestellt wurden, sollen die folgenden Ausführungen dazu dienen, dem Computeranwender eine praxisorientierte Hilfestellung bei der Konfrontation mit Computerviren zu geben.

A. Erscheinungsformen von Computerviren; Abgrenzung

„Programm-Anomalien"

Grundsätzlich ist jede Abweichung vom festgelegten (dokumentierten) „normalen Verhalten" des Computersystems als „anomal" zu bezeichnen. Als solches kann es entweder die vorgesehenen Leistungen nicht vollständig oder nicht korrekt erbringen, wofür als mögliche Ursachen Denk- oder Programmierfehler bei der Konzeption des Programms in Betracht kommen, oder es werden über den vorgesehenen Umfang hinaus zusätzliche „Leistungen" erbracht, die den Anwendern nicht bekannt und i. d. R. von diesen nicht gewollt sind. Derartige „Programm-Anomalien" werden bewußt geplant und programmiert, gegebenenfalls automatisch dem Programm von außen aufgeprägt[3].

I. Trojanische Pferde[4]

Keine Vervielfältigung

Die in jur-pc 12/91, S. 1368, vorgenommene allgemeine Beschreibung von Computerviren ist sehr vereinfachend, aber ausreichend, um die wesentlichen Unterschiede zwischen Computerviren i. e. S. und den sog. Trojanischen Pferden zu verdeutlichen: Unter „Trojanischen Pferden" versteht man in der Datenverarbeitung Programme oder Programmteile,

1 So die Warnungen der Medien vor dem Freitag, 13. Oktober 1989.

2 Im Rahmen des ersten Treffens europäischer Computerviren-Experten wurde Anfang Dezember 1990 geschätzt, daß Anfang 1992 die Zahl von 1.000 MS-DOS-Viren erreicht wird. Die Virus-Test-Zentren stellten inzwischen jedoch fest, daß diese Zahl bereits Mitte 1991 erreicht wurde.

3 Vgl. jur-pc 12/91, S. 1368.

4 Die Bezeichnung „Trojanisches Pferd" geht auf die griechische Sagenwelt zurück. Die Griechen bauten nach zehnjähriger Belagerung von Troja ein Holzpferd und füllten es mit Soldaten. Die Trojaner ließen sich durch den (scheinbaren) Abzug der griechischen Schiffe täuschen. Sie zogen das Holzpferd trotz der Warnung Lakoons in die Stadt, um der Göttin Athene ein Opfer zu bringen. Durch diese List konnten die Griechen Troja erobern.

Häufige Tarnung: Utility oder Spielprogramm

die angeblich eine bestimmte Aufgabe lösen, in Wirklichkeit aber im verborgenen – zusätzlich oder statt dessen – etwas ganz anderes tun, zumeist etwas Unerwünschtes. Im Gegensatz zu den Computerviren i. e. S. fehlt ihnen die Vervielfältigungseigenschaft, weshalb Programme dieser Art nicht als Computerviren bezeichnet werden sollten.
Meist als nützliche Utilities oder unterhaltende Spielprogramme getarnt[5], finden sie Zugang zum Rechner, nachdem sie von ihrem Konstrukteur an einer bestimmten Stelle in ein Rechnersystem bzw. Programm eingebracht wurden, wo sie auch verbleiben, solange sie existieren[6]. Dadurch ist der Ort der Manipulation auch der Ausgangspunkt ihrer Wirkung, was – verglichen mit Viren – die Bekämpfung wesentlich erleichtert.

II. Kennzeichnung und Arbeitsweise von Computerviren im engeren Sinne

„Echte" Computerviren

Programme, die man als echte Computerviren bezeichnen kann, bestehen grundsätzlich aus zumindest zwei, funktionell voneinander getrennten, Komponenten, einem Vervielfältigungsteil und einem Effekt- oder Schadensteil.

Vervielfältigungsteil

„Sich vermehren" heißt für ein Programm ganz allgemein: Es kann Kopien von sich erzeugen. Entscheidend ist aber nicht die Tatsache, daß Kopien erzeugt werden, sondern das Wie. Der Vervielfältigungsteil eines Computervirus umfaßt alle Funktionen, die für seine Weiterverbreitung erforderlich sind. Dies beinhaltet die Suche nach nichtinfizierten Programmen, Veränderungen solcher Programme, Installation im Speicher, eventuell auch Tarnung. Vermehrung ist somit beim Virusprogramm immer die Fähigkeit, andere Programme zu infizieren, das heißt, eine Kopie von sich selbst in ein anderes Programm irgendwie einzufügen. Dieser einfache Mechanismus führt dazu, daß jedes einmal infizierte Programm sofort selbst den „Virus" weiterverbreitet, und zwar solange, bis alle erreichbaren Wirtsprogramme verseucht sind. Je häufiger verseuchte Programme aufgerufen werden, desto schneller geht die Ausbreitung vonstatten[7]. Damit kann sich eine Infektion genau wie bei biologischen Viren lawinenartig in einem DV-System ausbreiten.

Schadensteil

Der Effekt- bzw. Funktionsteil wird im Regelfall erst nach Abarbeitung des Vervielfältigungsteils aktiv. Als Funktion bzw. Wirkung eines Computervirus kommt all das in Frage, was sich als Programm niederschreiben läßt. Ob ein Programm von 1 bis 1.000.000 zählt, um die Leistung eines PCs herabzusetzen, oder ob es bei jedem Aufruf eine Datei auf der Platte löscht, hängt allein von der Phantasie des Virusprogrammierers ab. Fast immer ist in diesem Teil des „Virus" eine ganz eindeutige Auslösebedingung (Trigger) festgelegt, die gleich zu Beginn überprüft wird. Trifft sie nicht zu, endet die Abarbeitung des Schadensteils, und es passiert nichts Auffälliges. Dies erklärt auch, warum „Virusinfektionen" häufig über einen längeren Zeitraum hinweg unentdeckt bleiben können – das „Virus schläft", bis der festgelegte Zeitpunkt eintritt.
Wird die Auslösebedingung jedoch wahr, tritt der eigentliche Sabotagecode in Aktion. Programmtechnisch ist ein Auslöser nichts anderes als eine Bedingung („if ... then"-Abfrage); der prinzipielle Aufbau des Virusprogramms wird durch diesen sehr einfachen Zusatz kaum verändert. Zeitsteuerungen oder Zähler werden auch eingesetzt, um den Grad der destruktiven Wirkung von Aufruf zu Aufruf zu steigern.

Bekannte Auslösebedingungen

Es seien an dieser Stelle lediglich exemplarisch einige bekannte Auslösebedingungen und Schadensfolgen genannt:

- Erreichen einer bestimmten Uhrzeit oder eines bestimmten Systemdatums
- Ausführen einer bestimmten Programmfunktion, z. B. Abspeichern
- Erreichen eines bestimmten Systemzustandes (z. B. Bitfolge 110 im Paritätszähler bei Ambulance-Virus) oder eines vorgegebenen Wertes des Infektions- oder Schadenszählers
- Abwesenheit eines bestimmten Ereignisses.

Schadensfolgen nach Computervirenbefall

Die für den PC-Anwender direkt oder indirekt feststellbaren Wirkungen von Computerviren sind sehr unterschiedlich. Sie reichen von mehr oder weniger makabren Scherzen (meist als transiente Schäden bezeichnet) über die Zerstörung einzelner Files oder der gesamten Festplatte bis zur gezielten Veränderung von Dateien (= permanente Schäden). Computerviren

5 Für PCs sind vor allem die Trojanischen Pferde AIDS und 12Tricks bekannt.

6 Vgl. dazu Dierstein, Von Viren, trojanischen Pferden und logischen Bomben (I), NJW-CoR 4/90, S. 26.

7 Konsequenz: In einem ruhenden System kann sich kein Virusprogramm mehr fortpflanzen.

sind in gewissem Sinne immer schädlich, weil sie zumindest andere Programme verändern und zusätzlichen Speicher und Rechenzeit beanspruchen.
Die Wirkung von Computerviren richtet sich – im Gegensatz zu ihrer Vermehrung – nicht nur auf andere ausführbare Programme, sondern beispielsweise auch gegen gespeicherte Daten. Der PC-Anwender bemerkt die Anwesenheit von Computerviren meist erst durch die Folgen ihrer destruktiven Aktivitäten. Als solche sind bisher bekanntgeworden:

Schadenswirkung nicht auf ausführbare Programme beschränkt

- Zerstören von Files (z. B. Jerusalem) — *Jerusalem-Virus*
- Totalverlust aller Daten auf Festplatten oder Disketten durch Auslösen der Neuformatierung (Datacrime und Ogre) — *Datacrime und Ogre*
- Manipulationen der Tastatureingabe (z. B. Fu Manchu und Fumble) — *Manchu und Fumble*
- Manipulationen der Druckerausgabe (z. B. Typo und Mix1) — *Typo und Mix1*
- Verringern des verfügbaren Plattenspeicher oder Feststellen neuer „Bad Sectors" (alle Boot-Viren, z. B. Stoned-Virus) — *Stoned-Virus*
- Verändern von Datei-Verzeichnissen und/oder FAT
- Permanenter Warmstart (z. B. Vienna) — *Vienna-Virus*
- Reduzierung der Verarbeitungsgeschwindigkeit (Jerusalem)
- Akustische Signale (z. B. Oropax und Yankee Doodle) — *Oropax und Yankee Doodle*
- Nachrichten auf dem Bildschirm (z. B. Denzuk) — *Denzuk*
- Veränderung der Bildschirmanzeige: Buchstaben fallen vom Bildschirm (Ping Pong und Herbst); ein Krankenwagen fährt über den Bildschirm (Ambulance) — *Ping Pong, Herbst und Ambulance*
- Veränderung von Datenbeständen (Änderung von Zahlen in einer Tabellenkalkulation, Produktion falscher Rechenergebnisse[8], Änderung von Texten durch Einfügen fehlerhafter Zeichen). — *Subtile Schäden*

Festzuhalten ist jedenfalls, daß nicht alle Computerviren von gleicher Gefährlichkeit für den Datenbestand des Benutzers sind. Neben den vom Virenprogrammierer beabsichtigten Wirkungen können aber auch durch Programmierfehler oder Unverträglichkeiten zwischen Computerviren und Anwendungsprogrammen weitere unvorhersehbare Effekte oder Schäden auftreten.

B. Einzelne Erscheinungsformen – Techniken[9]

Aktivierung
2 Gruppen von DOS-Viren

Computerviren führen – ebenso wie alle Programme in einem Computer – ihre Aufgabe (Reproduktion und Funktionen) erst aus, wenn sie aufgerufen werden. Diese Aktivierung erfolgt durch den Aufruf des sie umgebenden Programms[10], in das sie eingepflanzt wurden, oder nach einem Befall von Teilen des Betriebssystems. Im Prinzip lassen sich die DOS-Viren in zwei große Gruppen aufteilen, die sich durch ihre Angriffspunkte unterscheiden.

I. Bootsektor-Viren

Funktionsweise

Der Bootsektor-Virus nutzt den Umstand aus, daß beim Einschalten eines MS-DOS-Computers ein Teil des Betriebssystems erst noch von der Diskette oder Festplatte in den Arbeitsspeicher des PCs geladen werden muß. Diesen Teil sucht der Computer im Boot-sektor (= hierfür abgeteilter Bereich auf der Platten- bzw. Diskettenoberfläche) der Festplatte oder Bootdiskette in Laufwerk A:.

8 Z. B. der „dBase-Virus": Er verändert die Datendateien des weitverbreiteten Datenbankprogramms „dBase", das oftmals für die Bearbeitung wichtiger Finanzdaten verwendet wird, so, daß der Anwender anfangs keine Notiz von der Manipulation nimmt, denn auf dem Bildschirm erscheinen stets die korrekten Zahlen – die Berechnungen aber werden mit den manipulierten Daten ausgeführt.

9 Es sei hinsichtlich der nachfolgenden Ausführungen angemerkt, daß Verwender des Betriebssystems DOS wegen dessen hoher Verbreitung im Markt die beliebtesten Ziele der Virenprogrammierer darstellen. Dies ist auch der Grund, weshalb sich diese Darstellung auf Computerviren bzw. Mechanismen beschränkt, die für diese Systeme anwendbar sind.

10 Häufig Wirtsprogramm genannt.


Der Computervirus ersetzt den ursprünglich vorhandenen Bootsektor durch sich selbst und speichert ersteren an einer anderen Stelle des Datenträgers. Wird der Computer das nächste Mal gebootet, übernimmt der Computervirus die Steuerung und bleibt im Arbeitsspeicher. Er lädt dann den Original-Bootsektor, so daß augenscheinlich alles wie gewohnt funktioniert. Auf diese Weise kann das Virusprogramm von jetzt an jede neu eingelegte Diskette ohne Schreibschutz[11] infizieren.
Ähnliches passiert, wenn sich keine Diskette im Laufwerk befindet und von der Festplatte gestartet wird.

Verbreitung

Zugriffe auf andere Platten oder Disketten lösen dann die Weiterverbreitung aus. Auch eine infizierte, im Laufwerk vergessene Datendiskette kann beim Bootvorgang einen Computervirus einschleusen, da jede Diskette zumindest einen Bootsektor aufweisen muß, auch wenn kein Betriebssystem darauf vorhanden ist. Unangenehm an allen Varianten dieses Computervirustyps ist, daß sie aufgrund ihrer Bauweise bereits vor allen üblichen Virenwächtern geladen und aktionsbereit sind, wodurch sich das Abblocken von Bootsektor-Viren als schwierig erweist[12].

II. Programmviren

Ausführbare Dateien als Wirtsprogramme

Die zahlenmäßig größere Gruppe ist die der Programm- bzw. Dateiviren, die Programmdateien unter Verwendung des DOS-Filesystems verändern. Sie infizieren ausführbare Programmdateien, die normalerweise die Attribute „.com" oder „.exe" besitzen, manchmal aber auch Overlay-Files sowie Bildschirm- und Druckertreiber, was bereits angesprochen wurde.
Hier unterscheidet man zwischen zwei grundsätzlich verschiedenen Gruppen, den überschreibenden und den nichtüberschreibenden Computerviren.

Überschreibende Computerviren

Überschreibende Computerviren zerstören Programme bereits durch ihren Verbreitungsmechanismus: Hier bleibt die ursprüngliche Programmlänge erhalten, da der Computervirus einen Teil des Programms selbst – meist den Anfang – mit sich überschreibt. Da durch den Überschreibvorgang ein Teil des Programmcodes beschädigt wird, zeigt sich der Computervirenbefall i. d. R. in Fehlfunktionen des Programms. Folglich ist diese Art der Dateiviren relativ leicht zu entdecken; Verbreitungsgefahr und praktische Bedeutung sind relativ gering.

Nichtüberschreibende Computerviren

Virenprogrammierer achten daher heute darauf, daß ihr Machwerk derartige Symptome vermeidet – es kopiert also den Programmteil, bevor es ihn überschreibt, an eine unbenutzte Stelle des jeweiligen Datenträgers und flickt ihn bei jedem Programmstart wieder ein.
Bei nichtüberschreibenden Computerviren enthält eine neu infizierte Programmdatei dann eine Kopie des Computervirus, gewöhnlich am Ende der Datei (seltener am Beginn eines Originalprogramms). Ein erster Verdacht ist immer dann angesagt, wenn die Länge des Programms nicht mehr mit der Länge auf der Originaldiskette übereinstimmt. Diese Sorte von sog. Link-Viren sind mithin für den Anwender besonders gefährlich, da ihre Präsenz sich mit den genannten Methoden nicht so leicht erkennen läßt (das Programm bleibt trotz der Infektion voll lauffähig) – es sei denn, man erkennt die Infektion unmittelbar nach Veränderung der Dateilänge, so daß eine Weiterverbreitung noch nicht stattfinden konnte.Die meisten Dateiviren unter DOS arbeiten nach diesem Schema, Unterschiede ergeben sich dann vor allem beim Verbreitungsmechanismus bzw. bei den Schadensfunktionen, worauf noch einzugehen ist.

Speicherresidente Computerviren

Wird das infizierte Programm dann aufgerufen, so nistet sich der Computervirus vielfach resident im Arbeitsspeicher ein und hängt sich von diesem Zeitpunkt ab solange an jedes ausgeführte Programm, bis der Computer ausgeschaltet wird. Computerviren, die diese Art der Verbreitung benutzen, können das System mehr oder weniger kontrollieren und verbreiten sich sehr schnell[13].
Andere Derivate wiederum suchen nach neuen, noch nicht infizierten Programmdateien, die sie dann verseuchen.Es gibt Computerviren, die nach beiden Methoden zugleich arbeiten.Die meisten aber versuchen, eine bestehende Infektion zu erkennen, so daß eine Datei, die schon verseucht ist, nicht erneut vom Virus manipuliert wird.

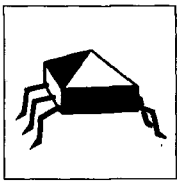
Hybridformen

In den letzten Monaten verfließen die Grenzen zwischen Dateiviren und Bootsektor-Viren

11 Schreibschutz-Kleber bei 5,25"-, Schieber bei 3,5"-Disketten.

12 Als besonders gefährlicher Vertreter dieser Gattung sei hier der „Disk-Killer"-Virus genannt: War ein infiziertes System etwa zwei Tage in Betrieb und fand in dieser Zeit keine Vervielfältigung des Virus mehr statt, verschlüsselt Disk-Killer die gesamte Festplatte, Spur für Spur. Leider wird die Entschlüsselung nicht mitgeliefert.

13 Hier werden in der Literatur durch die Begriffe „direct action" und „indirect action" noch weitere Unterscheidungen getroffen, auf die aber im Rahmen dieser Einführung verzichtet werden soll; vgl. PC+Technik 3/91, S. 147.



zunehmend. Es sind mittlerweile einige Hybridformen bekanntgeworden, die sowohl Boot- und Partitionssektoren als auch Programmdateien befallen. Selbst wenn alle infizierten Programmdateien gelöscht bzw. neu installiert werden, ist der Computervirus nach dem nächsten Bootvorgang wieder im Speicher und befällt die gerade installierten Programme aufs neue[14].

Neue Generation: „Stealth-Viren"

Erschwerend kommt neuerdings das Phänomen hinzu, daß sich eine große Anzahl von Mutationen bekannter Computervirenstämme herausgebildet hat, sowie die Tatsache, daß eine neue Generation sog. Stealth-Viren[15] in Erscheinung getreten ist, die neben den bereits genannten Funktionen die Eigenschaft besitzt, sich ausgezeichnet zu tarnen[16]. Dazu gehört auch die Fähigkeit, sich selbst zu chiffrieren (unter Verwendung ständig wechselnder Chiffrierschlüssel) bzw. sich selbst zu mutieren. All dies hat natürlich zur Folge, daß der gleiche Computervirus auf jedem befallenen Programm völlig anders aussieht und daher viel schwerer zu lokalisieren und zu entfernen ist[17].

Heutige Computerviren schöpfen bei weitem nicht das Schadenspotential aus, das in dieser Technik enthalten ist. Um so schlimmer ist, daß man schon die heutigen „Anomalien" nur begrenzt bekämpfen kann. In dieser Situation ist ein baldiges Abflauen der Computervirenwelle nicht zu erwarten.

III. Schlußfolgerungen

Grenzen der Computervirenverbreitung

Nach Schilderung der Möglichkeiten, wo sich Computerviren festsetzen können und wie sie arbeiten, ergeben sich folgende technische Grenzen der Computervirenverbreitung:

- In einem ruhenden System kann sich kein Virusprogramm mehr fortpflanzen.
- Das Virusprogramm muß i. d. R. eine Schreibberechtigung im System besitzen. Wo nicht geschrieben werden darf oder kann, ist auch keine Vermehrung von Computerviren möglich[18]. Damit wird einsichtig, warum PCs und Workstations von der Computervirengefahr weit mehr bedroht sind als Rechenzentren im herkömmlichen Sinne, wo nur einige wenige Mitarbeiter berechtigt sind, Systemprogramme oder systemnahe Programme zu ändern. Am PC oder Arbeitsplatzsystem ist dagegen jeder Benutzer sein eigener Systemprogrammierer, Operator, Anwendungsprogrammierer, Sicherheitsbeauftragter und Auftraggeber in einer Person, d. h., er allein entscheidet, welche Diskette eingelegt oder welche Software auf welchen Wegen beschafft und eingesetzt wird. Konsequenz: Schreibgeschützte Datenträger bleiben vor Computervirenbefall verschont, denn innerhalb der Laufwerke (gleich welchen Typs oder Formats) wird die Spannungszufuhr zum Schreibkopf hardwaremäßig getrennt, so daß es physikalisch unmöglich ist, die Informationen auf der Diskette zu verändern.

Ohne Schreibberechtigung keine Computervirenvermehrung

- Ein Virus kann keinen Computer infizieren, der nicht zuvor mit einer verseuchten Diskette gebootet oder auf dem ein infiziertes Programm aufgerufen wurde.
- Das Auslesen von reinen Datendateien, z. B. Texten, von einer computervirenverseuchten Diskette verursacht nach heutigem Kenntnisstand keine Infektion des Rechners. Die Vervielfältigung des Computervirus setzt die Ausführung eines Programms voraus, womit Datendateien als Infektionsquellen ausscheiden. Es ist somit nicht möglich, daß Computerviren das eigene System durch reinen Datenaustausch infizieren. Es muß allerdings darauf hingewiesen werden, daß auch als Text-Files gespeicherte Quellprogramme, die mit einem Interpreter, wie z. B. BASIC, dBASE oder LISP, abgearbeitet werden, in diesem Sinne als ausführbare Programme betrachtet werden müssen.

Reine Datendateien verursachen keine „Infektion".

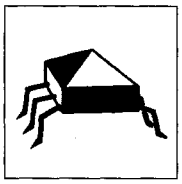
14 Vertreter dieser schwer zu entfernenden Sorten von Computerviren sind z. B. Omicron, das 1253-Virus und Invader.

15 Benannt nach dem gleichnamigen Stealth-Bomber.

16 So werden z. B. vergrößerte Dateien mit der Originalgröße ausgegeben, da der Virus die Größenangaben korrigiert.

17 Zu dieser neuen Gattung von Computerviren gehören u. a. das 4096-Virus (alias Frodo), V2000, Cameleon und Whale. Letzterer verdient sicher besondere Bemerkung – nicht nur, weil er das bisher größte DOS-Virus ist (mehr als 10 KB Größe!). Mehr als die Hälfte dieser Monstrosität dient dazu, einerseits, den Virus möglichst gut zu verbergen, und andererseits, das Disassemblieren sehr aufwendig und mühsam zu gestalten.

18 Das ist auch der Grund dafür, daß Computerviren um so gefährlicher sind, je näher sie am System oder Systemkern (COMMAND.COM) eingesetzt werden.



Computerviren imbatteriegepufferten CMOS-RAM?

- Ein Computervirus kann sich nicht im CMOS-RAM eines Rechners einnisten: ATs und 386-Systeme speichern System-Parameter in einem kleinen CMOS-Speicher. Eine Batterie sorgt nach dem Ausschalten des PCs dafür, daß dessen Inhalt nicht zerstört wird. Der Inhalt dieses Speichers besteht aus reinen Daten, die durch den Prozessor nicht ausführbar sind. Hinzu kommt, daß die Größe dieses Speichers bei den meisten Rechnertypen sehr beschränkt ist und zum überwiegenden Teil bereits verwendet wird. Es existieren allerdings Computerviren, die die im CMOS-RAM abgelegten Konfigurationsparameter eines Rechners verändern oder zerstören und das System dadurch außer Funktion setzen, jedoch können sie niemals bewirken, daß ein im CMOS-RAM eventuell befindliches Programm automatisch gestartet wird[19]. Eine Ausnahme ist lediglich für die Speicher einiger Laptops zu machen, bei denen durch eine Pufferung des Arbeitsspeichers im Standby-Modus oder bei Absinken der Akkuspannung Datenverlust verhindert werden soll.

Computerviren sind betriebssystemspezifisch.

- Ein Virus kann nicht von einer Computergattung auf eine ganz andere portiert werden, z. B. von Apple Macintosh auf IBM-PC oder MS-DOS auf UNIX. Computerviren müssen zur Ausführung der ihnen zugedachten Aufgaben Zugang zur Systemebene haben und setzen dafür immer einen bestimmten Prozessor, eine Betriebssystem-Version oder eine spezielle Chip-Kennung voraus. Ein Computervirus kann in PCs mit unterschiedlichen Betriebssystemen nicht aktiv werden. „Universal-Viren", die unter verschiedenen Betriebssystemen gefährlich werden, sind bisher nicht bekanntgeworden.
- Hardwareschäden an den heute üblichen PCs sind zwar theoretisch denkbar, z. B. durch extreme Steuerbefehle des Controllers an die Schreib- und Leseköpfe der Massenspeicher, bisher allerdings noch nicht bekanntgeworden.

C. Maßnahmen zur Vorbeugung gegen Befall und zur Beseitigung von Computerviren

I. Computervirenprophylaxe

Damit es erst gar nicht zum Ernstfall – der Verseuchung von Programmen oder Zerstörung von Daten – kommt, können geeignete und von jedem Anwender leicht zu realisierende Maßnahmen zur „Computervirenprophylaxe" getroffen werden:

Vorsicht vor Programmen unbekannter Herkunft.

1. Die Vermeidung von Computerviren muß beim Einbringen neuer Programme einsetzen. Daher gilt: Wer Computerviren nicht erst in sein System gelangen lassen will, sollte Programme meiden, deren Herkunft nicht bekannt ist (sprich Raubkopien), zumindest aber solche aus Schulen, Hochschulen[20] und Computer-Clubs sowie „günstige Angebote" auf Messen nicht in PCs übernehmen, die für die Verarbeitung wichtiger Programme und Daten verwendet werden. Für das Testen dieser Programme sollte immer ein „isolierter" PC verwendet werden, der nicht für „produktive" Arbeiten eingesetzt wird bzw. auf dem keine wichtigen Daten verarbeitet werden.

Neue Disketten mit Computervirenscannern prüfen

2. Alle eingehenden Disketten, auch die Lizenzprogramme renommierter Hersteller, vor und nach der Installation mit der aktuellen Version eines guten Computervirenerkennungsprogramms auf Computervirenbefall überprüfen (vgl. dazu unten D. II. 2.).

Schreibschutz bei Disketten aktivieren

3. Neue Programme immer nur von schreibgeschützten Kopien der Originaldisketten auf der Festplatte installieren. Bei versiegelter Software ist darauf zu achten, daß der Verschluß unbeschädigt ist.

Besonderheiten bei Schreibschutzaufklebern

Wichtig: Bei 5,25"-Disketten stets Schreibschutzaufkleber aus Alufolie oder festem schwarzen Papier verwenden, denn Diskettenlaufwerke dieses Formats arbeiten mit einer Lichtschranke, die prüft, ob ein Schreibschutzaufkleber angebracht ist oder nicht. Rote Aufkleber sind lichtdurchlässig und sollten deshalb zum Verschließen der Schreibschutzkerbe

19 Fazit: Notieren Sie sich die Einstellungen Ihres CMOS-RAMs, damit Sie sie im Falle einer Beschädigung oder Veränderung schnell restaurieren können.

20 Diese sind wegen der Vielzahl der an den Geräten tätigen Personen und der Tatsache, daß diese vielfach eigene Software mitbringen, in hohem Maße gefährdet. Hinzu kommt, daß dort Computer in immer größerem Umfang zu lokalen und internationalen Netzwerken zusammengeschlossen werden. So können Computerviren, die über die Diskettenlaufwerke der Arbeitsstationen eingeschleust werden, den zentralen Server befallen und damit schnell ein ganzes Netzwerk lahmlegen.

ebensowenig verwendet werden wie Tesafilm, denn die Lichtschranke leuchtet ebenfalls durch diese Materialien, wird so getäuscht und ermöglicht den Schreibvorgang.

4. Führen Sie ein Inhaltsverzeichnis der aktuellen Programme und Daten auf den wichtigen Datenträgern, nicht bloß der Festplatte. Notieren Sie jeweils das Datum ihrer Erzeugung oder Installation sowie die Länge der jeweiligen Dateien.

Programmgrößen notieren

5. Setzen Sie regelmäßig eines der bewährten Computervirensuchprogramme zur Überprüfung des vorhandenen Daten- und Programmbestandes (vor allem der Festplatte!) ein.

Regelmäßige Computervirensuche

6. In regelmäßigen und möglichst kurzen Abständen Sicherheitskopien des Daten- (nicht des Programmbestandes) anfertigen und drei Generationen von Sicherungen aufbewahren. Andernfalls besteht die Gefahr, daß zusammen mit den Programmen auch Computerviren konserviert werden. Programme gehören nicht in die Datensicherung, sondern in das Programmarchiv. Ein regelmäßiges Backup hat darüber hinaus weitere Vorteile, die man spätestens bei einem hardwarebedingten Datenverlust, z. B. durch Headcrash, Überspannung, entsprechend zu würdigen weiß. Hierzu gehören auch schreibgeschützte Kopien der wichtigsten Programme, die man möglichst an einem getrennten Ort aufbewahrt. Diese Maßnahme ist in ihrer Bedeutung nicht hoch genug einzuschätzen und wird leider von vielen – meist privaten – Anwendern vernachlässigt[21].

Regelmäßige Datensicherung

7. Je nach schadenstiftender Funktion benötigt ein Computervirus für seine „Tätigkeit" eine im System vorgeschriebene Erlaubnis, d. h. in der Regel eine Schreibberechtigung. Gerade diese Tatsache („ohne Schreiben keine Vermehrung") kann vor allem in Netzwerken der Schlüssel für eine Abwehr und Bekämpfung jeglicher Art von Programmanipulationen (auch Sabotage) sein, mit der ein beträchtlicher Teil der Computervirengefahr unter Kontrolle gebracht werden kann[22]. Neue Programme oder neue Versionen von Programmen dürfen in LANs nur vom Systembetreuer unter Beachtung besonderer Vorsichtsmaßnahmen eingebracht werden.

Präventivmaßnahmen in LANs

8. Wird der Computer von mehreren Personen benutzt, sollten geeignete Schutzmaßnahmen getroffen werden, damit nur autorisierte Personen an wichtigen Programmen und Daten arbeiten (z. B. durch Paßwortschutz), auch aus Gründen des Datenschutzes.

Zugangssicherung

II. Anhaltspunkte für eine Computervirenaktivität[23]

Sollten die eben beschriebenen Vorbeugemaßnahmen nicht oder nur unvollständig beachtet worden sein und funktioniert das System überraschend nicht mehr wie gewohnt, gibt es einige Erkennungsmerkmale, die einen Computervirenbefall indizieren. Diese frühzeitig zu erkennen ist um so wichtiger, als rechtzeitig Gegenmaßnahmen eingeleitet werden können und sich mögliche Schäden auf diesem Weg in Grenzen halten lassen.

Die folgende Aufzählung kann nicht den Anspruch auf Vollständigkeit erheben. Sie gibt lediglich eine Reihe von Symptomen wieder, die für bekannte Computerviren typisch sind:

Typische Symptome

- Es dauert etwas länger als gewöhnlich, ein Programm zu laden und der Rechner arbeitet spürbar langsamer[24].
- Programme passen plötzlich nicht mehr in den Arbeitsspeicher, obwohl sich weder an der Zahl der speicherresidenten Programme noch an der physikalischen RAM-Kapazität etwas geändert hat.
- Speicherresidente Programme versagen plötzlich ihren Dienst und tun nicht, was man von ihnen erwartet.
- Neue (unbekannte) Programme befinden sich im Hauptspeicher.
- Programme greifen ohne erkennbaren Nutzen auf Disketten oder Festplatte zu und das zu Zeiten, an denen das früher nie aufgefallen ist.
- Es häufen sich ungewöhnliche Fehlermeldungen (z. B. „Schreibschutz von Diskette entfernen", obwohl gar nicht geschrieben werden sollte).

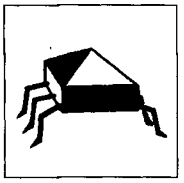
---

21 Der Zeitaufwand hierfür hält sich in Grenzen, setzt man eines der neueren marktgängigen BACKUP-Programme oder einen Streamer ein.

22 Vgl. Fußnote 20.

23 Selbstverständlich gibt es auch andere Ursachen für derartige Fehler. Dazu zählen Hardware-, Software- und Bedienungsfehler.

24 Jerusalem-Virus.

- Ausführbare Programme sind (verglichen mit dem computervirenfreien Original) länger geworden[25]. Der freie Plattenspeicher wird kleiner, obwohl keine neuen Dateien aufgenommen bzw. bereits vorhandene geändert wurden.
- Ein Prüfsummen-Programm meldet Veränderungen.
- Programme oder andere Dateien verschwinden „spurlos".
- Ein Kaltstart von einer Festplatte ist nicht mehr möglich.
- Es kommt zu Systemabstürzen ohne erkennbaren Anlaß (d. h. Änderung der Rechnerkonfiguration in CONFIG.SYS bzw. AUTOEXEC.BAT).
- Manipulationen des Bildschirmspeichers: Bespielsweise fallen Zeichen herunter und sammeln sich am unteren Bildschirmrand[26].
- Unvermittelt werden Töne aus dem Lautsprecher des PCs ausgegeben: Der PC spielt ein Lied[27].

III. Computervirenbefall – was nun?

Wurden die bereits empfohlenen Datensicherungen durchgeführt, besteht kein Anlaß zur Panik oder zu unüberlegtem Handeln.

Kein Datenaustausch mit Dritten

Selbstverständlich sollte nun keine Diskette, die in dem vermutlich infizierten PC benutzt wurde, auf einem anderen Rechner verwendet oder an Dritte weitergegeben werden. Des weiteren sollten Kollegen, mit denen Programm- und Datenaustausch betrieben wurde, umgehend gewarnt werden.

Computerviren aus dem Hauptspeicher entfernen

1. In einem ersten Schritt muß erreicht werden, daß der Hauptspeicher von Computerviren befreit wird:

Bei Verdacht auf Befall von Computerviren (vgl. Symptome) ist daher der Computer sofort auszuschalten (Kaltstart), damit auch der resetfeste Speicher neu aufgebaut wird. Ein Warmstart genügt nicht, denn es ist möglich, Computerviren zu entwickeln, die einen Warmstart – und sogar einen Hardware-Reset überstehen! Wenn der Arbeitsspeicher beim Start nicht initialisiert wird, kann sich der Virus im Hauptspeicher halten, und es ist ein leichtes, ihn sodann zu aktivieren.

Will man aber sichergehen, daß sich keine Computerviren mehr im Arbeitsspeicher befinden, ist das System ganz aus- und erst nach einigen Sekunden wieder einzuschalten. Dadurch werden alle momentan im Arbeitsspeicher des PC vorhandenen Computerviren zerstört.

Danach ist vor allen Arbeiten zur Erkennung und Bekämpfung von Computerviren das System mit einer schreibgeschützten und mit Sicherheit computervirenfreien Kopie der Originalbetriebssystemdiskette wieder hochzufahren. Es kann nun davon ausgegangen werden, daß zumindest der Arbeitsspeicher computervirenfrei ist, nicht aber die Festplatte oder weitere Disketten, die ohne Schreibschutz benutzt wurden.

2. Die weitere Vorgehensweise unterscheidet sich danach, welcher Virustyp – File- oder Boot-Virus – vorliegt.

Beseitigung von File-Viren

a) Die Beseitigung von reinen File-Viren ist relativ einfach:

- Physikalisches Löschen aller infizierten Dateien[28].
- Ersetzen aller gelöschten Files durch die Originale von computervirenfreien Disketten.
- Abschließend mit einem aktuellen Computerviren-Erkennungsprogramm prüfen, ob tatsächlich alle Computerviren beseitigt wurden.

Beseitigung von Bootsektor-Viren

b) Die Beseitigung von Bootsektor-Viren und Hybridformen ist bedeutend aufwendiger:

1. Alternative: Formatierung und Neuinstallation

Die sicherste, aber auch zeitintensivste Methode, die Festplatte von Computerviren zu säubern, besteht in einer Neuformatierung[29]. Der DOS-Befehl „FORMAT" überschreibt nur

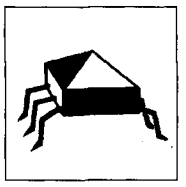
25 Intelligente Computerviren verhindern die Anzeige (leicht) erkennbarer Veränderungen, wie z. B. der Programmlänge.

26 Herbst-Virus.

27 Oropax-Virus.

28 Dadurch kann verhindert werden, daß nach einem logischen Löschen mit der DOS-Funktion DEL oder ERASE von einem Dritten mit einem Dateiwiederherstellungsprogramm die infizierte Datei wieder restauriert und aktiviert werden kann.

29 Im Interesse der Computervirenforschung kann aber zuvor noch eine Sicherung der Platte angefertigt und einem zuverlässigen Spezialisten oder einem Institut, wie dem Hamburger Virus Test Center, zur Analyse zur Verfügung gestellt werden.



Disketten und löscht damit auch Boot-Viren. Im Gegensatz dazu wird von FORMAT auf Festplatten nur die Directory und die FAT gelöscht. Boot-Viren (z. B. Stoned, Tequila), die sich in den Partition-Record kopieren, werden nicht zerstört. Derartige Computerviren können nur durch eine physikalische (low-level) und anschließende logische Formatierung der Festplatte dauerhaft zerstört werden[30], wobei allerdings sämtliche Programme und Daten verlorengehen. Hier spätestens erweist es sich als äußerst vorteilhaft, wenn man dem Rat gefolgt ist, regelmäßig Sicherungen auf verschiedenen Datenträgersätzen anzulegen, so daß man i. d. R. zumindest auf ein computervirenfreies und nicht zu altes Backup zurückgreifen kann. Ist dies nicht geschehen, bleibt dem Anwender nur, sämtliche Programme und Daten von schreibgeschützten Originaldisketten bzw. Sicherungskopien zu reinstallieren.

Nach dem Zurückspeichern des Backups bzw. der Reinstallation von Originaldisketten sollte die restaurierte Festplatte erneut auf Computerviren überprüft werden.

Falls die Betriebssystemdiskette, von der der Kaltstart durchgeführt wurde, das Backup und alle Originaldisketten noch nicht befallen waren, ist der PC nun wieder computervirenfrei.

2. Alternative: Computervirenscanner und Antivirus-Programme

Eine stetig wachsende Zahl von Unternehmen hat in der eingangs beschriebenen Situation die Zeichen der Zeit erkannt: Sie entwickeln Hilfsmittel, die vor Computerviren schützen oder sie bekämpfen sollen. Leider stehen die Angaben einiger Anbieter in ihrem Werbematerial nicht im Einklang mit den tatsächlichen Leistungen der angekündigten Produkte. Viele PC-Anwender können beim Studium solcher Prospekte nur schwer zwischen einem soliden Werkzeug und einem Luftschloß unterscheiden. Letztlich kann aber eine scheinbare Sicherheit vor einem Computervirenbefall zu geringerer Sorgfalt verleiten und beträchtliche Schäden verursachen. Deshalb soll in diesem Zusammenhang auch auf einige preiswerte und bewährte Produkte hingewiesen werden.

Funktionsweise von Computervirenscannern

Viele Anticomputerviren-Programme untersuchen einen PC (Disketten, Festplatte und Hauptspeicher) auf die Anwesenheit von Computerviren. Diese Programme werden als Computerviren-Erkennungsprogramme oder Computerviren-Scanner bezeichnet. Die meisten dieser Programme versuchen, sich dabei die Vorgehensweise vieler Computerviren bei ihrer Reproduktion zunutze zu machen:

Während seiner Verbreitung versucht ein Computervirus herauszufinden, ob das Wirtsprogramm, in das er sich gerade einpflanzen will, schon einmal infiziert worden ist oder nicht. Die einfachste Form einer solchen kontrollierten Vermehrung ist die Suche nach einem Kennzeichen bzw. einer Markierung. Denn indem jedem Computervirus ein bestimmtes Kennzeichen (z. B. die Zeichenfolge „ABCD" am Anfang) mitgegeben wird, kann der „Virenkonstrukteur" verhindern, daß übermäßiger Speicherbedarf, überraschendes Anwachsen der Programmlängen (vgl. oben) und ähnliche Unregelmäßigkeiten den Benutzer Verdacht schöpfen lassen und auf die mögliche Anwesenheit des Computervirus in seinem System vorzeitig aufmerksam machen.

Suche nach „Viren-Signaturen"

Computervirenkiller-Programme suchen dementsprechend nach derartigen „Signaturen" bzw. ganz bestimmten Zeichenfolgen eines Computervirus, indem sie die Programmcode-Folgen mit den Computervirencodes in ihrer Bibliothek vergleichen. Aus dem Auffinden eines solchen Computervirencodes wird dann auf den Computervirusbefall des Systems geschlossen. Denn ist erst einmal die Gestalt eines Computervirus in Form des ihn charakterisierenden Kennzeichens bekannt, kann man sich diese Tatsache auch bei Bekämpfung und Abwehr zunutze machen. Diese Technik ist überall dort sehr wirksam und einleuchtend, wo der Computervirus im Wirtsprogramm ein Kennzeichen setzt, um eine Mehrfachinfektion und damit eine vorzeitige Entdeckung zu verhindern, nicht aber den Typen, die mit einer Chiffrierfunktion ausgestattet sind und so ihr Erscheinungsbild ständig wandeln.

Hat ein solches Antivirus-Programm einmal einen Computervirus erkannt, wird es sogleich dessen Beseitigung anbieten können[31].

Danach kann man i. d. R. weiterarbeiten, auch ohne die Festplatte zu formatieren.

30 Vorsicht bei den in jüngerer Zeit am weitesten verbreiteten IDE-Festplatten (AT-Bus): Hier führt eine low-level-Formatierung bei einigen Fabrikaten zu einem Verlust plattenspezifischer Informationen (Bad-tracks-Liste). Außerdem schließen einige Plattenhersteller ihre Gewährleistung aus.

31 Die Beseitigung eines Computervirus an der Stelle seiner Entdeckung bringt so gut wie gar nichts. Greift man nicht zu weiterreichenden Reinigungsmaßnahmen, ist auch ein eben gesäubertes Wirtsprogramm nach kurzer Zeit von neuem verseucht.

Nachteile

Abwehrprogramme der beschriebenen Art können naturgemäß nur bei bereits bekannten Computerviren funktionieren; gegen neu auftretende Typen oder Varianten sind sie in der Regel wirkungslos. Aus diesem Grund hinken sie der Entwicklung aber immer hinterher: Erst wenn ein neuer Computervirus entlarvt ist, kann der Hersteller sein Programm anpassen (weshalb auf lange Sicht auch den schon genannten Vorbeugemaßnahmen große Bedeutung zukommt). Andererseits werden selbst manche neuen Versionen bekannter Computerviren „übersehen".

Das Prüfsummenverfahren

Diesen Nachteil suchen viele Hersteller durch die Bildung von Prüfsummen zu kompensieren: Mit einem Algorithmus wird z. B. nach Erhalt der Originaldiskette vom Anwender eine Prüfzahl für jedes Programm berechnet und als Vergleichszahl aufbewahrt. Ergibt zu einem späteren Zeitpunkt der gleiche Algorithmus eine abweichende Prüfsumme, so wurde möglicherweise in das betreffende Programm ein Computervirus eingepflanzt. Derartige Prüfsummenprogramme können Infektionen zwar nicht verhindern, aber im Gegensatz zu Computervirenscannern auch neue Computerviren feststellen. Welche Anforderungen sind an ein gutes Antiviren-Programm – abgesehen von dessen Aktualität – zu stellen?

BSI: Mindestanforderungen an Antiviren-Tools

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn hat einen Forderungskatalog erarbeitet, in dem Mindestanforderungen an Computerviren-Suchprogramme aufgestellt werden[32] Der Markt stellt eine Vielzahl von Antiviren-Tools – sowohl kommerzielle[33] wie solche aus dem Shareware-Bereich – bereit.

Zwei bekannte und bewährte Shareware-Vertreter (McAfee ViruScan; F-PROT) und ein kommerzielles Produkt (Turbo-Antivirus) sollen hinsichtlich ihrer unterschiedlichen Konzeption kurz vorgestellt werden.

Die Programme von John McAfee ...

Die Shareware-Programme von John McAfee werden getrennt in vier Modulen angeboten.

... werden rasch aktualisiert.

Die Programme werden mit DOS-Befehlen gestartet und mit Aufruf-Parametern gesteuert. Das Erkennungsprogramm SCAN gehört zu den wenigen Programmen, die schnell ergänzt und erweitert werden. Das Entfernen der mit SCAN erkannten Computerviren erfolgt – soweit dies überhaupt möglich ist – mit dem Programm CLEAN.

Netzwerkversion

Wie schon mehrfach erwähnt, breiten sich MS-DOS-Viren auch in Netzwerken aus. Deshalb wurde unter dem Namen NetScan eine Netzwerkversion von SCAN entwickelt, die auch virtuelle Laufwerke bearbeiten kann.

Fridrik Skulasons Shareware-Paket F-PROT

Das Shareware-Paket F-PROT von Fridrik Skulason besteht aus einem leistungsfähigen Programm, das alternativ aus einer komfortablen Oberfläche oder direkt gestartet werden kann. Auch die Computervirenbeschreibungen können direkt abgerufen werden. Zusätzlich wird mit F-PROT das Programm VIRSTOP geliefert, das einen residenten Scanner enthält. Wird es aktiviert, so wird jedes Programm das aufgerufen wird, automatisch auf bekannte Computerviren überprüft.

TNT Turbo AntiVirus aus Israel

Das Lizenzprogramm TNT Turbo AntiVirus wurde in Israel entwickelt. Das Programm, das Computerviren entdecken und – falls möglich – entfernen kann, wird über eine leistungsfähige Oberfläche bedient. Der Aufruf kann aber auch über die DOS-Ebene erfolgen. Das Paket enthält auch das Programm TSAFE, das ähnlich wie VIRSTOP bei F-PROT zur residenten Überwachung geladen werden kann. Mit der aktuellen Version wird auch ein Programm zur Bildung von Prüfsummen geliefert. Alle genannten Produkte unterliegen ständiger Programmpflege und besitzen einen Update-Service.

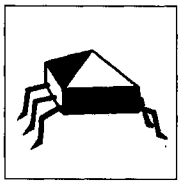
Folgende Punkte verdienen unabhängig vom jeweils eingesetzten Antiviren-Produkt Beachtung:

- Verwenden Sie keine alten Computerviren-Erkennungsprogramme.
- Beziehen Sie Ihr Computerviren-Erkennungsprogramm nur von einem autorisierten Distributor oder Händler. Verzichten Sie auf Computervirenscanner von guten Freunden. Einige Versionen wurden sofort nach deren Erscheinen gezielt verseucht und hatten so beim gutgläubigen Anwender gerade die entgegengesetzte Wirkung[34], ebenso ist es leicht möglich, daß bei einer vorhergehenden Untersuchung eines PCs eine solche Diskette infiziert wurde.

32 Abgedruckt in Personal Computer 9/91, S. 156, und in „Trojanische Pferde, Viren und Würmer – eine ernstzunehmende Gefahr für PC-Anwender?" hrsg. v. G. Mußtopf, S. 47 f., sowie Anhang F, S. 102 ff., perComp-Verlag Hamburg, 3. Auflage 1991.

33 Regelmäßig führen auch Computerzeitschriften Tests bekannter Computervirenscanner durch, die einen gewissen Anhalt für deren Brauchbarkeit geben können.

34 Vgl. Personal Computer 2/91, S. 118.



- Computerviren-Erkennungsprogramme können durchaus auch Falschmeldungen ausgeben. In diesem Fall ist eine Gegenprobe mit einem anderen Produkt durchzuführen.

Wenn einem Computervirus auch mit einem solchen Hilfsprogramm nicht beizukommen ist, bleibt als letzter Ausweg noch, sich an Experten zu wenden, die Erfahrung mit diesen Schädlingen haben[35].

Internationale Computervirenbekämpfung

In jüngster Zeit haben sich auch Organisationen und Institutionen (EICAR[36]; CARO[37]; CERT[38]; OKIS[39]) formiert, um die internationale Zusammenarbeit von Computerviren-Forschungsgruppen, Anwendern und Herstellern von Anti-Computerviren-Produkten mit dem Ziel einer schnelleren und zuverlässigeren Entdeckung und Analyse von „Computer-Anomalien" zu fördern.

Resümee

Es gibt kein Allheilmittel, das gegen alle denkbaren Computerviren unter allen Umständen hilft, und es wird auch keines geben, das eine vollständige Restaurierung infizierter Programme oder zerstörter Dateien in jedem Fall sicherstellen kann. Das Wissen und die Sorgfalt von PC-Anwendern stellen nach wie vor wichtige Voraussetzungen für eine erfolgreiche Vorbeugung und eine Begrenzung möglicher Schäden dar. Die heute sichtbare Entwicklung sollte für alle PC-Anwender Anlaß genug sein, vorbeugende Schutzmaßnahmen nicht nur zu planen, sondern auch in der täglichen Praxis zur Selbstverständlichkeit werden zu lassen.

Weiterführende Literaturhinweise:

Burger, Ralf:
Computervirenbuch, 5. Auflage 1990, Data-Becker.

Brunnstein, Klaus:
Computerviren-Report, 2. Auflage 1991, WRS-Verlag, Planegg-München.

Dierstein, Rüdiger:
Von Viren, trojanischen Pferden und logischen Bomben, NJW-CoR 4/90, S. 8 ff., 5/90, S. 26 ff., 1/91, S. 26 ff.

Mußtopf, G. (Hrsg.):
Trojanische Pferde, Viren und Würmer – Eine ernstzunehmende Gefahr für PC-Anwender?, perComp-Verlag GmbH, 3. Auflage 1991.

Schöneburg/Heinzmann/Namyslik:
Computerviren – Gefahren und Schutzmöglichkeiten, Mark & Technik 1989.

35 Das Virus Test Center der Universität Hamburg unter der Leitung von Prof. Dr. Brunnstein und das MicroBIT Virus Center der Universität Karlsruhe sind hier an erster Stelle zu nennen. Ein Nachweis aller wichtigen Adressen findet sich bei Mußtopf, a. a. O., S. 95 ff. (Anhang E).

36 European Institute for Computer Anti-Virus-Research.

37 Computer Anti-Virus Research Organization.

38 Computer Emergency Response Team.

39 Offener Kreis für Information und Sicherheit.