Dipl.-Ing
Erich H. Franke
DK6II
Lenaustraße 20
D-7535 Königsbach-Stein 2
Tel 07232-5160
FAX 07232-1647

Unheimliche Begegnungen der Elektronischen Art

Computerviren und was man dagegen tun kann

Beitrag zur 35. UKW-Tagung 1990 in Weinheim

Königsbach, im Juli 1990

1 Computerviren als Problem für alle Computeranwender

Für den reinen Anwender, für den der Computer einfach ein Stück Werkzeug mehr darstellt, sind heutige Computersysteme wahrlich schon kompliziert genug.

Im Zeitalter kommerzieller Nutzung von Computern entsteht bereits ein hoher wirtschaftlicher Schaden dadurch, daß Computer nicht genutzt werden können oder Datenbestände unbefugt zerstört oder verändert werden.

Jeder Anwender hat schon einmal, vor allem unter Termin- und Kostendruck mit 'abstürzender' Soft- und Hardware gekämpft und war sich doch nie ganz im Klaren, ob da nun einfach Bedienungsfehler, unzuverlässige Hardware, Programmfehler oder ob da doch mehr dahintersteckt.

Mit diesem 'mehr' wollen wir uns heute beschäftigen und zwar mit einer besonderen Art von Programmen, die unliebsame Zeitgenossen aus vielerlei Motiven heraus in Umlauf bringen und die den Betrieb von Computern recht erheblich stören können.

Wir sprechen von dem, was in der Regenbogenpresse als 'Killer-Programm' und im sonstigen

Computer-Chinesisch klangvoll mit Virus, Wurm, trojanischem Pferd oder logischer Bombe bezeichnet wird.

Wir wollen uns anschauen, wie diese Systeme arbeiten, wie man sie erkennt und was man dagegen tun kann. Wir wollen auch sehen, wo **keine** Gefahren bestehen, um einer Virus-Paranoia vorzubeugen.

2 Wer ist betroffen

Viren und ihre Abarten gibt es für praktisch alle Computer, die über ausreichend Speicherplatz verfügen und deren Software auf Datenträgern transportiert werden kann. Es gibt keine mir bekannten Viren für KIM-1 oder AIM-65, wohl aber für CP/M-Systeme, APPLE II, C-64 [1], ATARI ST [2], AMIGA [3], Mac's und MS-DOS-Rechner. Selbstverständlich bleiben auch andere Rechner diverser Hersteller nicht verschont (UNIX-Rechner, VAX, IBM etc.).

Betroffen ist hierdurch eigentlich jeder Computer-Anwender der mit anderen Anwendern kommuniziert und Programme austauscht. Wir sprechen hier durchaus nicht von sogenannten 'Raubkopien', also illegal kopierter Pakete, sondern auch von im Rahmen von Projekten erstellten Programmen Shareware oder Public-Domain[1)]-Software. Das Vogel-Strauß-Argument 'bei mir nicht' erscheint in diesem Zusammenhang ein wenig weltfremd. Aber sehen Sie selbst...

3 Von Viren, Würmern und Trojanischen Pferden

Hinter diesen klangvollen Namen steht eine ganze Legion verschiedener Computer-Störprogramme mit teilweise recht unterschiedlichen Eigenschaften. Diese sollte jeder Computeranwender kennen, da sich aus dieser Kenntnis heraus eine wirksame Diagnose und Prophylaxe ableiten läßt.

3.1 Der 'klassische' Virus

> "**Viren** (Einz. Virus)[zu lat. virus "Schleim, Saft, Gift"]... V. sind in Proteinhüllen verpackte Stücke genet. Materials, die den biochem. Apparat geeigneter Wirtszellen auf Produktion neuer V. derselben Art umprogrammieren können."

So definiert Meyers Neues Lexikon [4] den Begriff des organischen Virus. Diese Definition läßt

---

[1)] Nicht-Kommerzielle, frei kopierbare Software

sich mit ein wenig Phantasie auf sein elektronisches Äquivalent übertragen.

Im Computersinne ist ein Virus mithin ein ablauffähiges Programmstück, daß in der Lage ist, sich in bereits vorhandene 'Wirtsprogramme' einzunisten. Allerdings programmieren Computerviren das befallene Programm in der Regel nicht dazu neue Viren zu produzieren. Das Wirtsprogramm wird meist als Träger mißbraucht, um den Viruscode in einen Computer hineinzubringen und zumindest kurzzeitig die Kontrolle über den Prozessor zu erhalten.

Ist dies geschehen, so gibt es zwei Möglichkeiten. Einmal gibt es die sogenannten 'direct action'-Viren. Sie führen ihr Fortpflanzungs- und mögliches Zerstörungswerk direkt beim Ausführen des infizierten Programmes durch.

Die andere Virenklasse installiert eine lauffähige Kopie im Hauptspeicher des Rechners und klinkt sich in die normalen Mechanismen des Betriebssystems ein. Diese Viren sind weitaus heimtückischer, vor allem wenn sie mit einer Art Zeitzünder versehen sind. 'Residente' Viren überleben geschützt in einer Ecke des Hauptspeichers und können sich je nach Typus auf jede gewechselte Diskette übertragen. Dies ist besonders perfide, wenn der Fortpflanzungsmechanismus zum Beispiel an den Betriebssystemaufruf 'Datei öffnen' gekoppelt ist.

Viren bestehen in der Regel aus drei prinzipiellen Teilen:

- Fortpflanzungsteil
- Trigger-Auswertung
- Wirkteil

Der Fortpflanzungsteil enthält Code zum Transport des Viruscodes und zur Infektion von Wirtsprogrammen oder Systemteilen. Dieser Code ist darauf angelegt, möglichst unauffällig zu agieren, damit der Fortpflanzungsvorgang nicht bemerkt und der Virusbefall vorzeitig erkannt wird.

Aus Virus-Sicht ist der Fortpflanzungsteil deshalb auch so angelegt, daß möglichst keine Schäden am Wirtsprogramm oder den anderweitig befallenen Systemresourcen auftreten.

Bei der Fortpflanzung achten die meisten Viren darauf, eine Datei nicht mehrfach zu verseuchen. In der Regel prüfen Viren eine Datei vor der Fortpflanzung, ob bereits der selbe Virus bereits eingebaut wurde. Dies verhindert eine Explosion des Wirtes.

Manche Viren führen eine Aufdatierung vor. Wenn sie ein Programm vorfinden, das mit dem gleichen Virus älterer Version behaftet ist, so entfernen sie diesen und installieren dafür sich selbst.

Die zweite Stufe wird wirksam, wenn der Virus 'an Ort und Stelle' ist. Die meisten Viren warten mit Aktionen, bis ein bestimmtes Ereignis eingetreten ist. Ist das Ereignis nicht gegeben, so übergibt der Virus wieder die Kontrolle an das eigentliche Wirtsprogramm und bleibt selbst

passiv.

Die Möglichkeiten der Auslösung[2)] sind vielfältig. Es kann das Erreichen eines bestimmten Datums sein (Herbstlaub, 170x), es kann nach einer bestimmten Anzahl von Programmaufrufen sein. Dann startet der bis dahin scheinbar inaktive Virus seinen Wirkteil.

Der Wirkteil enthält die eigentliche Aktion des Virus. Hier haben die Virus-Programmierer ihre Phantasie bereits genügend strapaziert. Mögliche Aktionen beginnen mit dem, programmiertechnisch anspruchslosen Formatieren der Festplatte, Löschen von Dateien oder sonstigen Zerstörungen bis hin zum Abspielen von Musikstückchen oder Verändern der Bildschirmausgabe.

Auf jeden Fall kann man davon ausgehen, daß die Aktionen des Wirkteils aus Anwendersicht unerwünscht sind.

Neben den Programmviren gibt es sogenannte Bootsektor-Viren, die wie schon der Name sagt, in denn Boot-Sektoren von Disketten lauern und durch einen Computer-Kaltstart aktiviert werden. Dazu aber später mehr.

In diversen Veröffentlichungen wird zwischen 'harmlosen' und 'gefährlichen' Viren unterschieden. Ich teile diese Auffassung jedoch nicht. Jeder Virus und sei er noch so harmlos in seinen gewünschten Effekten, verändert doch das befallene Wirtsprogramm. Er muß dies tun, um an die CPU-Resource heranzukommen. Die Erfahrung zeigt, daß zahlreiche Viren von ziemlich schlechten Programmierern erstellt wurden und bedingt durch Programmierfehler Schäden verursachen, die das Opfer Zeit und Geld kosten können.

3.2 Da ist der Wurm drin

Im Gegensatz zu Viren bezeichnen wir mit dem Begriff 'Wurm'[3)] Programme, die speziell dafür konstruiert sind, sich über Netzwerke hinweg auszubreiten und damit verschiedene Computer ohne menschliches Zutun quasi vollautomatisch zu verseuchen.

Würmer sind in ihrem Aufbau Viren recht ähnlich. Der Fortpflanzungsteil muß dabei die Transportfunktion über Netzwerke mit der dazu notwendigen Ermittlung und /oder Umgehung von Passworten oder anderen Schutzmaßnahmen enthalten. Würmer die in heterogenen Netzen, d.h. Netzen die aus unterschiedlichen Rechnersystemen aufgebaut sind, wirksam sein sollen, enthalten meist den Code für verschiedene CPU-Typen, zum Beispiel VAX und 68000 unter UNIX. Dieser Code wird dann als Daten zum Zielsystem übertragen und ggf. dort mit dem

---

[2)] engl. trigger

[3)] engl. Worm

systemeigenen Compiler übersetzt, gelinkt und ausgeführt. Frech aber wirksam...

Mit Würmern haben Freizeitanwender in der Regel weniger zu tun. Professionelle Nutzer können häufig ohne intensive Vernetzung nicht mehr arbeiten, vor allem, wenn Daten verarbeitet werden, die an räumlich getrennten Orten erfaßt werden, wie dies im Bankwesen, wissenschaftlich-technischen Bereich, und in der Luft- und Raumfahrt notwendig ist.

Hier gibt es eine Reihe internationaler Netzwerke, häufig auf der Basis von UNIX- oder IBM-spezifischen Protokollen. UNIX-Netze sind in diesem Fall besonders gefährdet, da der Zugang, vor allem im Universitätsbereich recht einfach ist.

Hier gibt es die Geschichte vom 'Internet-Wurm', der von einem Studenten geschrieben und freigesetzt wurde und innerhalb weniger Tage weltweit Rechner verseucht hatte [5].

Dieser Fall ist ziemlich ärgerlich, da er den Befürworter restriktiver Maßnahmen beim Datenaustausch (leider) notwendige Argumente liefert und dem freien Umgang mit Netzwerken entgegensteht.

Fairerweise muß man jedoch anmerken, daß der zweifelhafte 'Erfolg' des Internet-Wurms großteils auf den laschen Umgang der Netzknotenbetreiber mit ihren Passworten zurückzuführen ist.

Und natürlich auf dokumentierte und zumindest Insidern bekannten Schwächen und Programmierfehlern des unterlegten Betriebssystems UNIX.

Über Infektionsgefahren beim Benutzen von Mailboxen werden wir uns gleich eingehender unterhalten...

3.3 Galoppierende Seuchenherde

Viele von uns kennen aus Homers "Ilias" die Geschichte vom Ausgang des Trojanischen Krieges [6]. Bis zum 10. Kriegsjahr war es der Griechischen Streitmacht unter Agamemnon nicht gelungen, die befestigte Stadt einzunehmen. Erst eine List des Odysseus brachte die Entscheidung. Die Griechen zogen zum Schein ihre Truppe vor der belagerten Stadt ab, ließen jedoch ein hölzernes Pferd zurück.

Die Sage berichtet, daß die Verteidiger unter Hektor und Äneas unvorsichtigerweise dieses obskure Geschenk in die Stadt brachten. Es kam wie es kommen mußte. Das Pferd war nämlich hohl und in der Nacht entstiegen ihm 30 griechische Kämpfer, die des nachts die Tore der Stadt öffneten um ihre Gefährten einzulassen; Troja wurde ein Raub der Flammen...

Aus dieser Geschichte heraus ist der Vergleich mit einem speziellen Vertreter der Virenszene offensichtlich.

Als 'Trojanisches Pferd' wird ein Programm bezeichnet, daß nach außen hin zunächst einmal ganz gut aussieht, etwa eine Datenverwaltung oder ein Rechenprogramm. Das Trojanische Pferd arbeitet auch ganz normal und führt die beschriebenen Aufgaben richtig durch. Daneben jedoch besitzt es bestimmte und ganz sicher unerwünschte Nebeneffekte, beispielsweise das Einpflanzen eines eigentlichen Virus oder die Veränderung gespeicherter Daten.

Von klassischen Viren unterscheiden sich Trojanische Pferde dadurch, daß sie vom Programmierer bewußt bereits mit diesen 'Nebeneffekten' programmiert und nicht erst später verseucht wurden.

Systembedingt findet man Trojanische Pferde zuweilen in Public-Domain-Software. Dies ist insbesondere ärgerlich, da dieser Umstand den Public-Domain-Gedanken von freier Software in Verruf bringt.

Eines der bekanntesten Trojanischen Pferde ist *AIDS*[4)], der von Kriminellen in erpresserischer Absicht in Umlauf gebracht wurde und die Datenbestände auf der Festplatte verschlüsselt. Gegen ein Lösegeld sollte man dann ein 'Gegenmittel' bekommen. AIDS war übrigens als SexWare verpackt, wohl um die 'Infektionsbereitschaft' der Klientel zu steigern. Ich weiß nicht, was aus der Angelegenheit wurde, habe jedoch der Tagespresse entnommen, daß man die Täter in Großbritannien gefaßt habe.

Nur ganz ahnungslose Computerbenutzer lassen jede fremde Software ohne vorherige Schutzmaßnahmen laufen. "Never accept software from strangers". Dieser Satz stand bereits 1986 im Sicherheitshandbuch eines amerikanischen Computerherstellers [7], also lange bevor Computerviren Allgemeingut wurden.

Trojanische Pferde haben definitionsgemäß keinen eigenen Fortpflanzungsteil, da sie sich ja per Mimikry hinter harmlos aussehenden Applikationen verstecken. Allerdings sind Abarten denkbar, die beim Aufruf ihrerseits Viren freisetzen. Für sich gesehen sind Trojanische Pferde unbeweglich und müssen vom Anwender in das System geholt werden.

Trojanische Pferde sind in Multiuser-Umgebungen gefährlicher, wenn sie benutzt werden, um fremde Paßworte, private Dateiinhalte oder einen Superuser-Status zu erhalten. Diese Gefahren sind für reine PC-Anwender (noch) nicht von Bedeutung.

3.4 Sprengstoff im Hauptspeicher

Die 'logische Bombe' ist ein weiterer Vertreter von Zerstörungsprogrammen.

[4)] nicht zu verwechseln mit dem AIDS-Virus-Programm. Siehe dazu auch in Kap. 0.

Hiermit bezeichnet man Programme, die im Rechner bewußt eingebaut werden und auf ein Auslöseereignis hin bestimmte, aus Sicht des Rechnerbetreibers unerwünschte, Aktionen vornehmen.

Die logische Bombe kommt ursprünglich aus dem kommerziellen Bereich. Sie kennen vielleicht die Geschichte eines angestellten Programmierers, der nach erfolgter Kündigung ein Programm in die Startup-Sequenz des Rechners seines ursprünglichen Arbeitgebers einbaut, das nach einer bestimmten vorgegebenen Zeit die Datenbestände löscht. Die logische Bombe unterscheidet sich von Viren und Trojanischen Pferden dadurch, daß sie bewußt und absichtlich in den Zielrechner eingeschleust wird und nicht 'von selbst' oder durch Unachtsamkeit in den Rechner gerät.

Sie als PC-Besitzer können mit logischen Bomben durchaus konfrontiert werden, zum Beispiel auf Messen wie dieser, wenn am Ausstellungsstand auf einmal jemand unbedingt 'ein tolles Programm' in Ihrem Rechner anschauen will. Hier herrscht Alarmstufe Eins!

Um zu demonstrieren, wie trivial eine logische Bombe sein kann, folgt ein praktisches Beispiel. Dies ist allerdings nicht zur Nachahmung bestimmt...

Wenn Sie einem anderen PC-Besitzer unbemerkt folgende Anweisung in seine AUTOEXEC.BAT-Datei eintragen können:

```
DEL *.*
ECHO Hahaha!
```

Abb. 1:Beispiel einer logischen Bombe

haben Sie sicherlich einen neuen Freund gewonnen...

4 Mechanismen der Ansteckung

Kann ich meinen Rechner vor unerwünschten Programmen sichern? Dies scheint eine zentrale Frage unter Computerbenutzern zu sein. Ganz klar, wie im organischen Äquivalent muß ein Virus, Wurm oder Trojanisches Pferd erst in den Computer gebracht werden bzw. anderweitig hineingelangen.

Und es muß zumindest kurzzeitig die **Kontrolle** über die CPU erhalten, das heißt es muß fremder Maschinencode ausgeführt werden. Von ganz wenigen Ausnahmen einmal abgesehen kann man ein virusverseuchtes Programm kopieren, löschen, ansehen oder ausdrucken und ist

(ziemlich) sicher, solange man das Programm oder Teile daraus nicht ausführt.

4.1 Infektion durch Viren

Bei Viren unterscheidet man grob zwei Arten an Hand der Methode, mit der sie die Kontrolle über die CPU erhalten: Die sogenannten Link-Viren und die Bootsektor-Viren.

4.1.1 Bootsektor-Viren

Letztere sind ein wenig harmloser, sofern man in diesem Zusammenhang überhaupt von 'Harmlosigkeit' sprechen kann.

Wie der Name bereits vermuten läßt, befallen Bootsektor-Viren den sogenannten Boot-Sektor von Floppies und Festplatten. Der Boot-Sektor ist ein Plattenbereich, der vom normalen Betriebssystem nicht benutzt wird. Er wird kurz nach dem Einschalten des Rechners von dessen ROM-residenten Kaltstartprogramm in den Speicher geladen und ausgeführt. Seine Aufgabe ist, das eigentliche Betriebssystem (DOS) in den Speicher (RAM) zu laden und zu starten. Dieser stufenweise Einschaltvorgang wird seit der Frühzeit der Computerei als 'Bootstrap' bezeichnet. Daher also Boot-Sektor...

Sowohl auf Disketten als auch auf Festplatten ist der Boot-Sektor recht klein. Er umfaßt bei heutigen Systemen meist nur 512 Byte. Dieser Platz genügt meist gerade so für das Boot-Programm, glücklicherweise praktisch jedoch nicht für ein zusätzliches Virus-Programm.

Ein Virus, der den Boot-Sektor infizieren will, muß also das ursprünglich dort liegende Boot-Programm zunächst einmal wegschaffen.

Die Möglichkeiten dazu sind vielfältig:

1. Der Virus markiert einen freien Sektor des Speichermediums als 'Bad' und kopiert den ursprünglichen Boot-Sektor dorthin. Sich selbst kopiert er in den nun freien Boot-Sektor.

2. Der Virus kopiert den Boot-Sektor in eine unbenutzte Spur, z.B. Spur 40 auf 360 Kbyte-Disketten

3. Der Virus legt eine geschützte Datei an (Hidden, System) und kopiert das ursprünglichen Boot-Programm dort hinein und merkt sich die absolute Lage.

Alle drei Methoden sind, wenn man den Mechanismus kennt, vom Anwender auch ohne viele Hilfsprogramme aufzuspüren bzw. abzustellen. Näheres dazu später.

Gestartet wird der Bootsektor-Virus wie bereits erwähnt, durch den Kaltstartlader im ROM des Computers. Der Virus-Code installiert sich an den bereits zu diesem Zeitpunkt vorhandenen rudimentären Betriebssystemsschnittstellen. Danach übergibt er die Kontrolle an den weggeschafften alten Boot-Sektor, der treu und brav das eigentliche Betriebssystem aktiviert. Zu diesem Zeitpunkt ist der Boot-Sektor-Virus jedoch bereits in den Tiefen des Speichers verschwunden und lauert auf das Eintreten der Triggerbedingung...

4.1.2 Link-Viren

Neben den Bootsektor-Viren spielen die sogenannten Link-Viren die weitaus größere und gefährlichere Rolle.

Der Name Link-Virus kommt von dessen Fortpflanzungsverhalten. Der Link-Virus 'befällt' ausführbare Wirtsprogramme, indem er sich in dieses Programm einklinkt[5)].

Um den Vorgang zu verstehen muß man die Art und Weise kennen, in der MS-DOS und viele andere Betriebssysteme auch, ihre ausführbaren Programme verwalten.

So gibt es beispielsweise unter MS-DOS zwei häufig auftretende Typen von ausführbaren Programmen und einige weniger bekannte Abarten.

'Normale' ausführbare Programme enden mit der Dateikennung .COM oder .EXE.

.COM-Dateien werden beim Programmaufruf generell in den Hauptspeicher an die feste Adresse 0x100 (hex 100) geladen. Die Ausführung des Programms beginnt an der ersten Anweisung im Maschinencode. Die Länge eines .COM-Programmes ist durch das Betriebssystem auf 64 Kilobyte fest begrenzt.

.EXE-Dateien können im RAM an verschiedenen Stellen geladen werden und besitzen dazu in der Datei eine 'Verschiebe-Information' (engl. relocation information). Diese Verschiebeinformation sagt dem Lader, welche Anweisungen auf die Ladeadresse umgerechnet werden müssen um ausführbar zu werden.

Das Betriebssystem erkennt an Hand eines Verwaltungseintrags im Kopf der Datei (file header) wie lange der zu ladende Maschinencode ist, wo sich der Verschiebeanteil befindet und wo nach erfolgter Adress-Umrechnung das Programm zu starten ist.

[5)] engl. to link

Die Infektion erfolgt in der Regel durch Verlängern der jeweiligen Programmdatei um die Länge des Virus-Codes und durch 'Verbiegen' der Programm-Startadresse, so daß nach dem Laden der Virus als erstes aufgerufen wird. Hierdurch wird das Wirtsprogramm durch die Infektion nicht beschädigt, so daß der Virusbefall nur durch die geänderte Länge erkennbar ist. (Bei besonders tückischen Viren nicht einmal das!)

Es gibt nur wenige primitive Viren, die das Wirtsprogramm überschreiben und damit Teile daraus zerstören. Sie können deshalb vergleichsweise leicht erkannt werden.

Schauen wir uns einmal typische Infektionsmuster näher an.

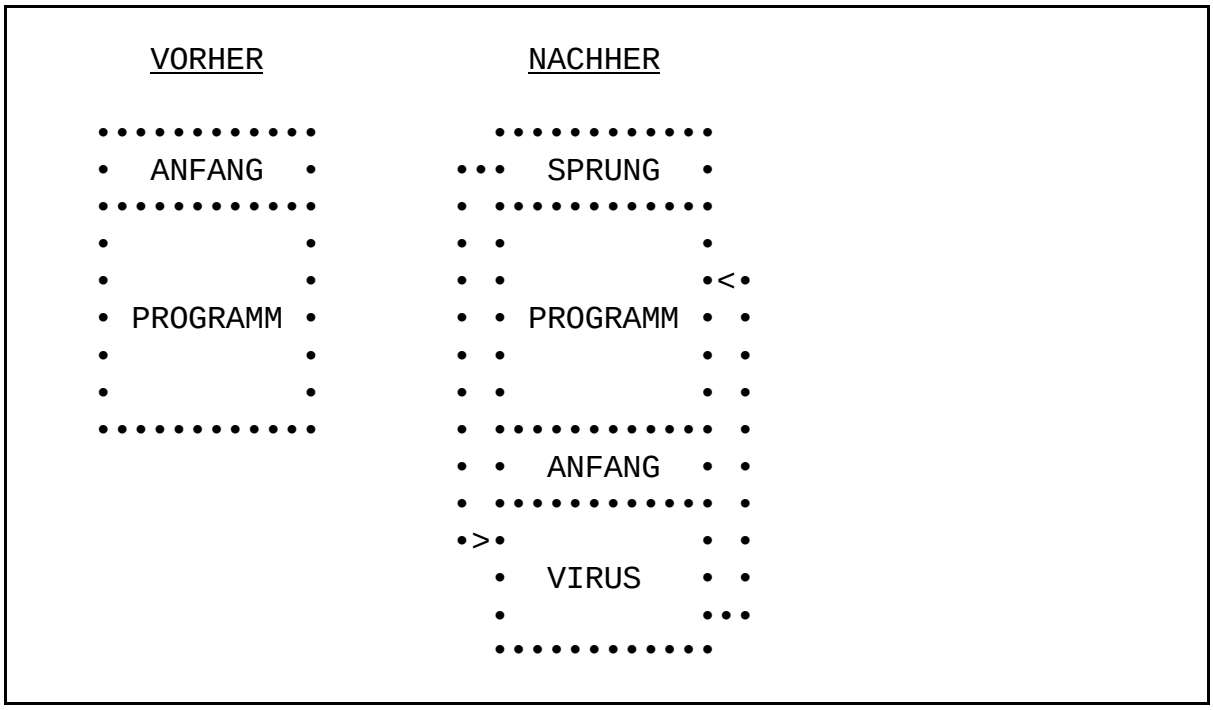

Abb. 2:Infektion einer COM-Datei

COM-Dateien haben für Viren zwei Einschränkungen. Sie sind nicht verschieblich und ihre Startadresse liegt immer bei 0x100. Das Ziel einer möglichen Virus-Attacke liegt demnach am Ende der Datei. Der Virus verlängert die bestehende COM-Datei durch seinen eigenen Code und trägt am Programmanfang einen Sprung auf seinen Anfang ein. Am Ende seiner eigenen Verarbeitung übergibt der Virus die Kontrolle an das Wirtsprogramm zurück.

Bei EXE-Dateien haben es Viren fast leichter. Sie können ihren Code direkt vor den Anfang des Wirtes packen und eigene 'Relocate'-Information mitbringen und diese in den Verschiebeteil kopieren.

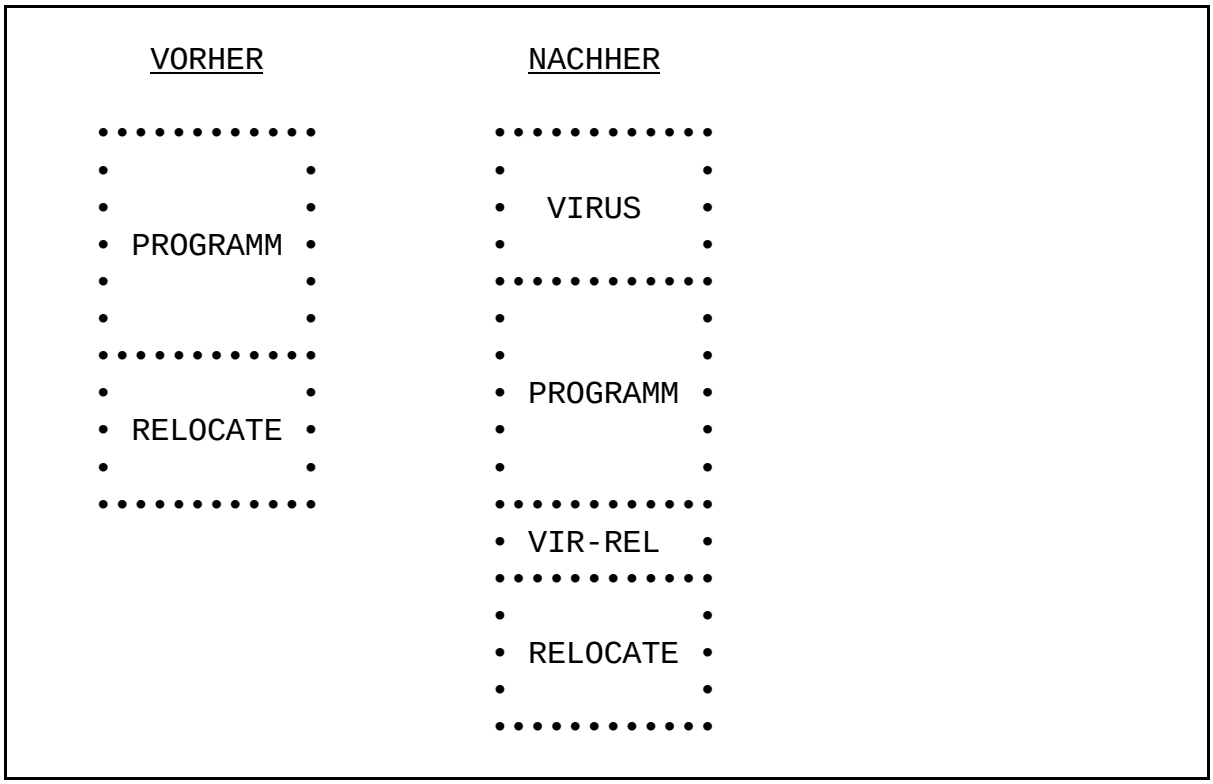

Abb. 3:Typische Infektion einer EXE-Datei

Auf diese Weise gelangt der Virus an die CPU und führt, je nach Typ, seine vorbestimmten Aktionen aus. Danach gibt er die Kontrolle an das Wirtsprogramm weiter, das sich dann scheinbar normal verhält. Bis auf eine unmerkbare Verzögerung beim Programmaufruf ist für den Anwender kaum etwas zu bemerken.

In unsere Überlegungen müssen wir aber auch diejenigen ausführbaren Programmdateien einbeziehen, die nicht direkt als 'ausführbare Programme' bekannt sind. Dies sind zum einen Gerätetreiber, die die Endung .SYS besitzen, aber auch andere Programmteile, sogenannte 'Overlays', die vor allem bei größeren Programmpaketen zu finden sind und Endungen wie .OVL oder .OVR besitzen.

4.1.3 Virus-Aktionen

Wir haben nun gesehen, wie ein Virus auf die Platte bzw. in eine Datei kommt und wie er die Kontrolle über die CPU erhält. Was danach kommt, ist von Virus zu Virus unterschiedlich:

Man unterscheidet hier wiederum ganz grob zwei Unter-Arten:

- 'direct-action'-Viren
- 'deferred-action'-Viren

Erstere prüfen sofort den Trigger und führen ggf. sofort das Wirkteil aus. Die Wirkung kann, sofern erkennbar, dem infizierten Programm zugeordnet werden.

'Direct Action'-Viren sind deshalb in ihren Fortpflanzungsmöglichkeiten auch auf die Datenträger beschränkt, die zur Laufzeit des Infizierten Programmes zugreifbar sind.

Im Gegensatz dazu stehen die 'deferred action'-Viren, die sich selbst als TSR-Programm (engl. Terminate and Stay Resident) im Computer installieren und sich in die Schnittstellen des Betriebssystems einschalten.

'Deferred action'-Viren sind besonders tückisch, da ihre Wirkung erst lange Zeit nach dem Aufruf eines infizierten Programmes auftreten können und da ihre Fortpflanzungsfähigkeit keiner zeitlichen Beschränkung unterliegt.

Die Tatsache, daß sich die 'deferred action'-Viren in die Betriebssystemsschnittstellen einschalten hat zur Folge, daß sie direkten Einfluß auf die Arbeitsweise später gestarteter Programme nehmen können.

Ein Beispiel hierfür ist die Mimikry mit der sich ein bestimmter Bootsektor-Virus tarnt. Dieser Virus erkennt über bestimmte BIOS-Aufrufe, daß der Boot-Sektor der Diskette gelesen werden soll. Erkennt der Virus diesen Befehl, so gibt er statt des Bootsektor-Inhaltes, in dem sein Code gespeichert ist, den Inhalt des zwischengespeicherten Original-Bootsektors wieder. Dieses Verhalten schützt ihn vor Entdekung durch Disketten-Suchprogramme.

Diese Manipulation ist durch das rufende Programm nicht erkennbar. Ein einfacher Virus-Sucher, der einfach den Boot-Sektor liest und damit Viren sucht, wird hierdurch getäuscht!

Eine ähnliches Mimikry-Verhalten zeigt ein anderer Link-Virus. Dieser überwacht die Befehle 'findfirst' und 'findnext' und manipuliert den Längeneintrag der Datei von der aus er aktiviert wurde dahingehend, daß dem rufenden Programm (also z.B. DIR) die Dateilänge minus der Viruslänge gemeldet wird.

Ein geeigneter Virus in einem File-Server eines Unternehmens kann einen nicht abzuschätzenden wirtschaftlichen Schaden verursachen.

Wir wissen nun, welche prinzipiellen Möglichkeiten es für einen Virus gibt, in ein System einzudringen und sich zu etablieren. Wir wollen nun sehen, wie man einen Virenbefall erkennen und was man dagegen unternehmen kann.

4.2 Infektion mit anderen Störprogrammen

Im Gegensatz zur Virusinfektion, die ja quasi selbstätig verläuft, spielen für PC-Anwender die Infektionsgefahren durch andere Störprogramme in der Regel eine geringere Rolle.

4.2.1 Trojanische Pferde

Wie bereits gesagt, holt sich der Benutzer derartige Störer SELBST in den Rechner. Das heißt, hier erfolgt die Infektion durch Unkenntnis, Unachtsamkeit oder schlichte Dummheit.

Der bekannteste 'Trojaner' der Neuzeit ist wohl das AIDS-Programm (nicht zu verwechseln mit dem AIDS-Virus), der eine Daten-Manipulation in erpresserischer Absicht im Rechner der Opfer vornimmt.

Trojanische Pferde sind meist als Tools oder Utilities[6)] oder als Spiele getarnt.

Besondere Beachtung sollte auch Programmen aus Datenbanken (Mailboxen) geschenkt werden. Sie können Texte aus Mailboxen in der Regel gefahrlos ausdrucken und ansehen. Falls Sie jedoch ein Programm aus der Mailbox in Ihren Rechner laden[7)] und zur Ausführung bringen, besteht Gefahr. Gleiches gilt für BASIC-Programme mit eingestreuten Maschinensprachen-Anteilen, deren Funktion nicht zweifelsfrei bekannt ist. Ein Beispiel sei der BHP-Virus für den C-64 [8].

4.2.2 Würmer

Würmer 'leben' wie bereits erwähnt von Netzwerken, in denen automatisierter Daten- und vor allem Programmausführungs-Betrieb möglich ist.

Die Teilnahme an reinen Daten-Netzwerken, beispielsweise der Paket-Radio-Betrieb sind (heute noch) vollständig gefahrlos.

---

6) engl. Hilfsprogramme

7) Download

Netzknotenbetreiber sollten jedoch bereits heute die Infektion automatischer Netzknoten in Betracht ziehen und diese durch geeignete Paßworte und andere Schutzmaßnahmen absichern.

Auch hier liegt die eigentliche Gefahr in der Komplexität der Systeme und - oftmals - der mangelhaften Systemkenntnisse der Benutzer und Betreiber.

4.2.3 Logische Bomben

Bomben werden in der Regel bewußt gelegt, sei es nun von 'Spaßvögeln', frustrierten Mitarbeitern oder Saboteuren. Man kann hier nicht direkt von 'Infektion' sprechen.

Auch die Erkennung und Abwehr solcher Sprengstoffpakete gestaltet sich anders und erfordert mehr logistische und organisatorische als elektronische Maßnahmen.

5 Maßnahmen für die Erkennung

Wie aus den vorangegangenen Abschnitten abzuleiten ist, kommt gerade der Früherkennung eines Virenbefalles große Bedeutung zu.

Die Erkennung Trojanischer Pferde, logischer Bomben und Würmer spielt im Gegensatz dazu für reine PC-Anwender glücklicherweise eine geringere Rolle, wenn die grundlegenden Sicherheitsmaßnahmen eingehalten werden.

Virenprogrammierer verwenden in der Regel große Mühe darauf, daß sich der Fortpflanzungsvorgang und damit die Infektion des Zielsystems im Stillen abspielt, damit der Benutzer nicht vorzeitig gewarnt wird.

Hierdurch soll eine möglichst große Verbreitung sichergestellt werden. Viele Viren triggern ihre Aktion auch erst nach einer bestimmten 'Inkubationszeit' oder nach einer bestimmten Anzahl von Generationswechseln. Hierdurch will der Virenprogrammierer sicherstellen, daß auch Backup-Kopien verseucht sind, damit eine Restauration zusätzlich erschwert wird.

Eines der wichtigsten Erkennungsmittel sind Virensuchprogramme, wie sie zum Beispiel in /4/ beschrieben sind.

Hier gibt es im Public-Domain wie im kommerziellen Bereich inzwischen einige mehr oder minder wirksame Produkte. Zur Beschreibung derselben hat sich eine eigene Terminologie entwikelt:

- Virensucher
- Erkennen von Veränderungen
- Viren-'Killer'
- Anti-Viren
- Alarmanlagen
- Gesunder Menschenverstand

Diese Verfahren wollen wir nun diskutieren.

5.1 Viren-Sucher

Virensucher sind Programme, die Viren aktiv suchen. Das heißt, sie durchsuchen die Platte/Diskette dateiweise oder direkt und vergleichen die Inhalte mit gespeicherten Mustern (Signaturen) bekannter Viren.

Das Verfahren ist an sich recht wirksam, vor allem bei 'alten Bekannten' aus der Virenszene. Verschiedene Personen und Gruppen bieten inzwischen unterschiedlich gute und schnelle Virensucher an. Leider merken dies aber auch die Virenprogrammierer. Zur Umgehung des Schutzes ist es für diese recht einfach einige wenige Bytes zu ändern, um zumindestens die einfachen Suchprogramme, die mit direkten Vergleichen arbeiten, zu unterlaufen. Diese künstlichen Mutanten haben dann eine andere Signatur und ggf. auch ein anderes Verhalten.

Bessere, jedoch auch aufwendigere Programme arbeiten mit verschlüsselten Muster-Daten und suchen durch Korrelation statt Vergleich und teilen nicht mehr den Namen des gefundenen Virus mit, um dem Virenprogrammierer sein Anti-Anti-Viren-Werk zu erschweren. Das Ganze erinnert stark an Nachrüstung und Anti-Anti-Raketen...

5.2 Erkennen von Manipulationen

Eine andere brauchbare Methode umgeht dieses Manko. Sie beruht darauf, alle Programmdateien der Festplatte zu untersuchen und sich die daraus resultierende Signatur zu merken. Diese Signatur ist so angelegt, daß man durch sie erkennen kann, ob sich Programmteile irgendwie verändert haben.

Zur Signaturbildung können herangezogen werden:

- Prüfsummen
- CRC-Polynome[8)]
- Dateilänge

Gute Prüfprogramme legen das Verfahren nicht offen. Und das aus gutem Grund: Ein 'intelligenter' Virus, bzw. ein hartnäckiger Virusprogrammierer, könnte den sich so ergebenden Schutz aufheben, indem er dem Virus 'Korrekturinformationen' mitgibt, die dem Prüfer eine korrekte Dateilänge oder Prüfsumme vorgaukelt.

Sehr gute Prüfprogramme lassen die Eingabe einer willkürlichen Schlüsselzahl durch den Benutzer zu, die zur Signaturerstellung mit eingerechnet wird. Hier haben Viren (fast) keine Chance.

Ein Nachteil der Methode ist, daß der Benutzer AKTIV werden muß, der Prüfvorgang Zeit kostet und deshalb (Schlampi, Schlampi) gerne vernachlässigt wird.

Außerdem führen bestimmte Kopierschutzverfahren bzw. selbstmodifizierende Programme ggf. zu Fehlauslösungen.

5.3 Viren-'Killer'

Kombiniert mit Virensuchern werden auch martialisch anmutende sogenannte 'Virenkiller' angeboten. Diese sollen, zumindest gemäß Herstellerangaben, bekannte Viren erkennen und entfernen.

Wie man sich aus dem vorangegangenen Kapiteln leicht überlegen kann, ist dies bei Bootsektor-Viren sicherlich auch zu machen. (Für den Hausgebrauch reicht dort aber auch schlichtes Neuformatieren!)

[8)] Cyclic Redundancy Check.

Linkviren zu eliminieren ist jedoch ein anderes Geschäft. Zum einen sitzen sie in den Dateien nicht immer dort, wo man sie vermutet. Zum anderen muß ja zumindest der alte Dateianfang wieder restauriert werden, sonst ist das derart operierte Wirtsprogramm hinterher nicht mehr arbeitsfähig. Weiterhin darf der Virus bei seinem Aufenthalt keine Schäden hinterlassen haben und der 'Killer' muß vorsichtig zu Werke gehen, sonst heißt es hinterher 'Operation gelungen, Programm tot'!

Erkannte Linkviren beseitigt man besser mit Stumpf und Stiel, indem man das befallene Programm von den (sicheren!) Originalen neu installiert. So man hat, aber das ist eine andere Geschichte!

5.4 Antiviren und Impfstoffe

Antiviren, zum guten Schluß, sind vor allem im Hinblick auf Boot-Sektor-Viren entwickelt worden. Sie residieren selbst im Boot-Sektor (vor allem bei Maschinen mit DOS im ROM, wie z.B. ATARI ST), sind also selbst eine Art Virus ohne Wirkteil. Antiviren prüfen, ob sie durch irgendwelche Einflüsse verändert worden sind und melden etwaige Angriffe.

5.5 Alarmanlagen

Alarmprogramme sind ein recht ordentlicher Schutz bei der Früherkennung bzw. bei der Analyse verdächtiger fremder Programme. Sie wirken bei Viren gleichermaßen wie bei etwaigen logischen Bomben, Würmern und Trojanischen Pferden. Zumindest so lange, wie diese über die Betriebssystemsschnittstellen agieren.

Alarmprogramme sind selbst speicherresidente Programme, die sich wie ein Virus in mögliche Betriebssystemsschnittstellen einklinken und alle Aufrufe überwachen. Bei verdächtigen Aktivitäten schlagen sie nun Alarm. Verdächtig ist in hohem Maße: Absolutes Lesen und Schreiben (vor allem in den Boot-Sektor), Formatieren, Öffnen bestimmter Dateien wie IBMBIO.COM etc. Je nach Programm erscheint dann ein Fenster, daß die angeforderten Betriebssystemsfunktionen anzeigt und um Erlaubnis für die Ausführung nachfragt. So können unerwünschte Datenveränderungen - zumindest von geschultem Personal - recht sicher und früh erkannt werden.

5.6 Andere Verfahren

Was aber tun, wenn man (noch) kein geeignetes Virensuch, -kill, oder sonstiges Programm besitzt? Dann hilft der gesunde Menschenverstand und ein wenig Nachdenken schon erstaunlich

weit.

Ein sehr hilfreiches Werkzeug gibt es bei Toolboxen wie NORTON UTILITIES, den PC-TOOLS oder deren Verwandten. Es heißt meistens **MI** (Memory Information) und zeigt die Hauptspeicher- (RAM)-Belegung an.

In der Liste sind alle im Hauptspeicher stehenden Programme und deren Länge angegeben. So zum Beispiel das Betriebssystem selbst, Der Befehlsprozessor, die Tastaturtreiber und andere speicherresidente Programme.

```
Memory Info v5.8
Copyright 1989 Central Point Software, Inc.   All rights
reserved.

Conventional memory.  Total:  640k
Largest executable program:    92k

Type  Paragraphs  Bytes     Owner
----  ----------  -----  -------------
Prog  0FFC-10BEh   3120  0FFCh <itself>
Prog  10D8-1146h   1776  10D8h <itself>
Prog  1148-12A2h   5552  1148h <itself> C:\SYSTEM\KEYB.COM
Prog  12AD-1327h   1968  12ADh <itself> C:\UTIL\DOSEDIT.COM
Prog  1333-17FFh  19664  1333h <itself> C:\PCTOOLS\PC-CACHE
Prog  180A-882Eh    449k 180Ah <itself> C:\WP51\WP.EXE UKW9
Prog  883C-88FEh   3120  883Ch <itself> C:\COMMAND.COM
Prog  8917-9FFFh     92k 8917h <itself> C:\PCTOOLS\MI.COM
```

Abb. 4:Beispiel für einen Hauptspeicher-Auszug

Falls Sie ein geeignetes Programm dazu besitzen, sollten Sie sich nach dem Booten von einer sicheren Diskette einen Ausdruck der Speicherbelegung herstellen udn diesen über Ihren Arbeitsplatz hängen.

Während der Sitzung, vor allem nach dem Betrieb 'unsicherer' Software sollten Sie die aktuelle Liste mit dem Ausdruck vergleichen. Taucht auf einmal ein TSR-Programm[9)] auf, das nicht in der Liste steht, so besteht zumindest der Verdacht auf einen Angriff.

Eine weitere Früherkennungsmaßnahme besteht darin, die Liste durch CHKDSK auszudrucken

---

[9)] Abk. f. Terminate and Stay Resident. Speicherresidente Betriebssystemerweiterung

und von Zeit zu Zeit nachzukontrollieren. Tauchen 'auf einmal' Bad Sectors auf der Festplatte oder Diskette auf, besteht zumindest der Verdacht auf einen Bootsektor-Virus.

```
Volume CBM_PC40(1) created 24 May 1989 19.37

 33384448 bytes total disk space
    45056 bytes in 3 hidden files
   159744 bytes in 69 directories
 31012864 bytes in 1664 user files
    81920 bytes in bad sectors
  2084864 bytes available on disk

   655360 bytes total memory
   556896 bytes free
```

Abb. 5:Beispiel für eine CHKDSK-Liste

Bootsektor-Viren anderweitig zu erkennen ist an sich gar nicht so einfach! Hier hilft vor allem 'Sauberkeit' am Rechner. Das 'Booten' von einer fremden Diskette sollte tunlichst unterlassen werden! Das Risiko durch selbst-bootende Spielprogramme muß jeder Anwender selbst tragen.

Ansonsten gehört eine schreibgeschützte Systemdiskette zur Grundausstattung jedes Rechners. Meistens werden Original-Systemdisketten bereits ab Werk ohne Schreibkerbe geliefert. Diese sind zu bevorzugen.

Sie sollten immer dann, wenn Sie eine Diskette formatieren vorher von einer - ebenfalls schreibgeschützten - Kopie der Systemdiskette booten. Natürlich aus dem Kaltstart heraus, also durch Abschalten des Rechners oder Drücken der RESET-Taste sofern man hat. Der 'Affengriff' CTRL-ALT-DEL, der den Warmstart auslöst, kann von Viren softwaremäßig 'umgebogen' werden, die, wie Beispiele zeigen, dann nur (leise lachend) einen Warmstart vortäuschen, selbst jedoch geschützt überleben.

Falls man ein Werkzeug wie NORTON UTILITIES oder PC-TOOLS besitzt, kann man mit diesem auch den Boot-Sektor anschauen. Diese Methode ist nicht immer wirksam, wenn ein Virus den Boot-Sektor nur vortäuscht.

Link-Viren beim Eindringen zu erkennen ist ohne Hilfsmittel praktisch nicht möglich. Außer über mögliche Wirkungen kann man jedoch das Fortpflanzungsverhalten als Erkennungsmaßnahme benutzen.

Eine mögliche Erkennungsmethode ohne fremde Hilfsmittel ist die 'Methode Fliegenfänger'. Man nehme ein ausführbares Programm bekannter Länge und kopiere es zweimal auf die oberste Directory-Ebene. Eine Kopie nenne man zum Beispiel **FANG.EXE**. Die zweite Kopie **FXXX.XYZ**. Die Programme sollten nicht zu kurz sein, so um die 32 kByte herum, jedoch

nach Möglichkeit nicht lange rechnen und nicht viel Ein/Ausgabe produzieren. Ein kurzes PASCAL, C oder anderes Programm genügt vollauf.

Nun baue man sich eine Kommandodatei auf, z.B. **F.BAT** und füge die folgenden zwei Zeilen ein:

```
FANG
COMP FANG.EXE FXXX.XYZ
```

Abb. 6:Beispiel für einen 'Fliegenfänger'

Bauen Sie eine ähnliche Datei für .COM-Files auf.
FANG bildet einen Köder für mögliche Viren. Es ist ausführbar, ist lang genug (manche Viren meiden zu kurze Programme wg. Entdeckungsgefahr) und wird verführerisch oft aufgerufen.

Dafür müssen Sie selbst sorgen, indem Sie **F** von Zeit zu Zeit starten. Die AUTOEXEC-Datei ist nicht unbedingt der beste Ort hierfür, da zum Zeitpunkt des AUTOEXEC-Laufes die meisten Programme noch nicht gelaufen sind und ein möglicher Link-Virus noch garnicht aktiv werden konnte.

Lauert jedoch ein 'deferred action' Virus im Speicher, bekommt er mit einiger Wahrscheinlichkeit Appetit auf das unschuldige **FANG.EXE** und/oder **FANG.COM** und versucht es zu infizieren. Der folgende Vergleich mit dem für den Virus aufgrund des willkürlich gewählten Namens nicht erkennbaren Referenzprogrammes bringt eine mögliche Abweichung ans Licht, gegen die der Virus eigentlich nicht gefeit ist.

Einen kleinen Nachteil hat diese Methode. Bestimmte Viren haben einen zeitgesteuerten Fortpflanzungsmechanismus und entwickeln dadurch nur gelegentlich Appetit auf unseren Köder.

Selbstverständlich muß der Köder ABSOLUT virenfrei sein. Die meisten Viren erkennen sich selbst und infizieren ein Programm nicht zweimal. Wäre nun **FANG** bereits selbst verseucht, hätten wir keinen Fliegen-Fänger sondern eine Viren-Schleuder!

5.7 Weitere Verdachtsmomente

Hier folgen ein paar Symptome und mögliche virusbedingte Ursachen. Doch Vorsicht: Nicht jeder Systemfehler ist ein Virusinfekt. Bitte keine Virus-Paranoia entwickeln...

Symptom: Auf der Diskette/Festplatte befinden sich (auf einmal) 'Bad Sectors'.
Verdacht: Es hat sich ein Boot-Sektor-Virus eingeschlichen, der den eigentlichen Boot-

Sektor in einem 'Bad Sector' zwischengelagert hat.
Maßnahme: Von einer sicheren Quelle booten. Neue Diskette formatieren (/S). Daten dateiweise kopieren. (kein sog. Track-Kopierer, kein DISKCOPY!). Festplatte sichern, low-level-formatieren und dateiweise neu einrichten...

Symptom: Die Anzahl bzw. Größe von 'Hidden Files' oder Dateien mit dem 'System'-Attribut hat sich (von alleine) verändert.
Verdacht: Ausgelagerter Virus-Code.
Maßnahme: wie oben.

Symptom: Ein Programm bekannter Länge hat diese (von selbst) verändert.
Verdacht: Link-Virus am Werk!
Maßnahme: Siehe unten

Symptom: Im Speicher befindet sich ein TSR-Programm das vorher noch nicht da war.
Verdacht: Ein 'deferred action'-Virus hat sich eingeschlichen.
Maßnahme: Booten von sicherer Diskette. Analyse von AUTOEXEC.BAT und CONFIG.SYS. (s.u.)

Symptom: Beim Aufruf eines Programmes von einer schreibgeschützten Diskette erscheint auf einmal eine 'Write protected'-Fehlermeldung, die früher nicht erschienen ist.
Verdacht: Ein 'deferred action'-Virus versucht sich auf Diskette fortzupflanzen und hatte dabei Pech...
Maßnahme: Booten von sicherer Diskette. Analyse von AUTOEXEC.BAT und CONFIG.SYS. (s.u.)

Symptom: Ihr Rechner spielt Musikstückchen ab, Buchstaben bewegen sich auf dem Bildschirm von selbst, Ihre Festplatte formatiert sich von Zeit zu Zeit, Programme verschwinden, andere tauchen auf, der Inhalt Ihrer Festplatte ist auf einmal verschlüsselt...
Verdacht: Sie haben sich bereits einen Virus eingefangen.
Maßnahme: Nicht ärgern, Rechner abschalten, Kaffee trinken gehen...

6 Weitergehende Maßnahmen

Wir haben von einigen Maßnahmen gesprochen, um Viren zu erkennen. Hier noch ein paar Hinweise zum Aufspüren.

Nehmen wir einmal an, Sie hätten die Auswirkung eines LINK-Virus entdeckt, zum Beispiel den Versuch der Fortpflanzung auf eine schreibgeschützte Diskette.

Sinnvoll aber langwierig wäre nun, die Platte neu zu formatieren und sämtliche Programme von den (sicheren!) Originaldisketten neu zu installieren. Backup-Kopien sind verdächtig, vor allem, wenn man nicht den genauen Zeitpunkt der Infektion bezüglich des letzten Backup-Zeitpunktes kennt.

Reine Datendateien sind nicht unbedingt verdächtig, wohl aber das AUTOEXEC.BAT und CONFIG.SYS, die auf unbekannte (und ggf. unerwünschte) Kommandos hin untersucht werden sollen (logische Bomben drohen hier).

Mit einem gewissen Risiko kann man feststellen, welche Programme verseucht sind. Zum einen dürften dies die Programme sein, die über die Datei AUTOEXEC.BAT aufgerufen werden wie Tastaturtreiber, Bildschirmschoner, residente Programme und ähnliches.

Sicherlich sollten auch sämtliche Betriebssystemsprogramme von der Originaldiskette neu überspielt und das System mit SYS nochmals kopiert werden.

Bei anderen Programmen ist es schwieriger. Es ist wichtig, alle infizierten Programme auf der Platte möglichst sicher aufzuspüren. Und das geht folgendermaßen:

Falls Sie den Virus rechtzeitig erkannt haben, ist es durchaus möglich ihn zu analysieren. Hierbei können Listen wie die in Kapitel 7 dieses Beitrags recht nützlich sein. Es hilft aber auch etwas Handwerksarbeit wie folgt.

Sie benötigen dazu ein Werkzeug, das eine Stringsuche direkt auf der Platte ermöglicht (z.B. NORTON UTILITIES, PC-TOOLS o.ä.) sowie einen Debugger wie DEBUG.

Nun fangen Sie den Virus ein ('Fliegenfänger'), indem Sie ihn zur Infektion eines bekannten, ggf. speziell für diesen Zweck präparierten Programmes verleiten.

Stellen Sie durch Vergleichen der verseuchten Datei (z.B **FANG.EXE**) mit der Referenz (**FXXX.XYZ**) fest, wo sich der Virus eingenistet hat. Man findet den Viruscode oft sofort durch bewußten 'Single Step' vom Programmanfang her, da der Virus ja möglichst sofort die CPU-Kontrolle haben will.

Notieren Sie sich ein gehöriges Stück des Virus-Codes in Hex-Schreibweise.

Starten Sie nun die Plattensuche und suchen Sie binär die gesamte Platte nach dem Stückchen Viruscode ab. Das Referenzstückchen sollte nicht zu groß sein! Nehmen Sie ruhig ein paar Fehlalarme in Kauf! Das Suchprogramm stoppt beim Auffinden des Virus-Stückchens und zeigt (meistens) den Namen der Datei an, in der es gefunden wurde.

LÖSCHEN SIE DANN DIESE DATEI UMGEHEND. Perfektionisten mögen nach

vollständiger 'Entwanzung' der Platte einen COMPRESS-Lauf mit Löschung der so freigewordenen Stellen durchführen und einen BAD-BLOCK-Check ausführen.

Falls Sie einen Virus-Verdacht haben und ein Symptom nachweisen können, zum Beispiel das Auftauchen eines unbekannten Blockes in der Speicherbelegungsliste oder ein unplanmäßiger Zugriff auf die Diskette und dieses Symptom auch reproduzieren können, ist es möglich, gezielt auf Virenjagd zu gehen.

Booten Sie von einer 'sicheren' Diskette (schreibgeschützte Originaldiskette). Die dort vorhandene AUTOEXEC.BAT- und CONFIG.SYS-Datei sollten nur die minimal notwendigen Befehle enthalten, deren Programmdateien alle von schreibgeschützten, sicheren Originalen stammen.

Prüfen Sie das Symptom. Es darf noch nicht auftreten! Beginnen Sie nun, Programm für Programm aus AUTOEXEC.BAT aufzurufen (von Platte natürlich) und prüfen jedesmal das erkannte Symptom. Meist wird man ziemlich bald fündig und kann dann aus dem als infiziert erkannten Programm durch Absuchen der Festplatte wie bereits beschrieben eine 'Entwanzungsaktion' durchführen.

Manchmal ist dies die einzige Art und Weise ohne zuverlässiges Virensuchprogramm größere Programmbestände zu säubern.

7 Eine abschließende Bemerkung

Der vorliegende Beitrag stützt sich auf den aktuellen Stand der (Viren)-Technik, wie er in der einschlägigen Fachliteratur dargelegt oder auf eigenen Erfahrungen beruht.

Dieser Beitrag soll vor allem den Anwendern die Angst vor Virusprogrammen nehmen und darstellen, daß man einen Schutz mit relativ einfachen vorbeugenden Maßnahmen und Methoden durchaus erzielen kann.

Er soll weiterhin den Schleier des Geheimnisvollen und der Pseudo-Romantik bei Virus-Erzeugern und bei -Jägern zu lüften helfen um die Attraktivität der Computer-Sabotage[10)] herabzusetzen.

Ich hoffe für die Vielzahl der Anwender, daß das Erzeugen und Freisetzen von Viren oder anderen Störprogrammen möglichst bald 'außer Mode' kommt.

[10)] §§303a und §§303b StGb

8 Checkliste zur Prophylaxe:

Anbei nochmals eine Zusammenfassung der wichtigsten vorbeugenden Maßnahmen:

- Niemals von einer fremden Diskette 'booten'! Dies ist bei der überwiegenden Anzahl von Programmen auch NICHT notwendig.

- Bei der Benutzung fremder Programme bzw. selbst-bootender (Spiel-)Programme möglichst Festplatte hardwaremäßig stillegen.

- "Never accept software from strangers". Jedes Programm unbekannter Herkunft ist verdächtig mehr zu tun, als es den Anschein hat.

- Nach der Benutzung fremder Programme den Computer ABSCHALTEN. Ein Warmstart (CTRL-ALT-DEL genügt nicht!).

- Muß fremde Software (auch käufliche) installiert werden, so sollte sie zuvor mit einem Virus-Erkennungsprogramm untersucht werden.

- Einrichten eines 'Fliegenfängers' bekannter Größe und periodische Prüfung desselben.

- Originaldisketten kommerzieller Softwareprodukte vor dem ersten Einbringen IMMER mit Schreibschutz versehen. Vor der Installation von einer SICHEREN Diskette booten. Originaldisketten sofort kopieren, noch bevor andere Programme aufgerufen wurden.

- Originaldisketten gehören in den Panzerschrank! Schutz vor Zerstörung und unberechtigter Manipulation.

- Fremde, unbekannte Software NIEMALS an einem vernetzten PC testen. Geschickterweise hält man für besonders harte Haker einen unvernetzten, festplattenlosen 'Spiel'-PC bereit...

- Niemals auf Software-Schreibschutzmaßnahmen vertrauen. Jeder Software-Schreibschutz kann softwaremäßig umgangen werden!

- Ein lohnendes Ziel für jeden Virus ist der Befehlsprozessor COMMAND.COM selbst. Der Befehlsprozessor ist wohl das am häufigsten laufende Programm auf dem PC überhaupt und kann die Infektion so weit tragen. Halten Sie eine Kopie des Befehlsprozessors unter einem nicht erkennbaren Namen bereit und vergleichen von Zeit zu Zeit.

- Prüfen Sie AUTOEXEC.BAT und CONFIG.SYS auf Ihnen unbekannte Einträge. Drucken Sie sich möglichst den Inhalt der letzten (bekannten) Version aus und vergleichen Sie. Auch (scheinbare) **REM**-Einträge sind verdächtig! Das Trojanische Pferd AIDS schreibt zum Beispiel die Zeile <u>REM .EXE</u> nach AUTOEXEC. Das

Leerzeichen ist in Wirklichkeit jedoch das nicht druck- und anzeigbare Sonderzeichen ALT-<255> ! Die mit **REM** beginnende Zeile wird von COMMAND.COM nicht als Kommentar- sondern als Befehlszeile aufgefaßt. Der 'Trojaner' hatte nun vorher die Datei mit dem 'hidden'-Attribut als REM<255>.EXE[11)] auf die Festplatte geschrieben. Dieses wird nun gestartet, bumm...

- Mißtrauen Sie Virensuchern unbekannter Herkunft! Es ist denkbar, daß es Trojanische Pferde darunter gibt!

- Prüfen Sie von Zeit zu Zeit die Speicherbelegung und mißtrauen Sie unbekannten Einträgen.

- Zeigt die Platte 'Bad Blocks' so sollte sie mit SPINRITE oder einem ähnlichen Tool 'gereinigt' werden. Geht danach der Boot-Vorgang schief, so hat man sich mit großer Wahrscheinlichkeit einen Bootsektor-Virus eingefangen.

- Ihnen sollte nichts verborgen bleiben. Suchen Sie alle Dateien mit 'hidden' und 'system' Attribut und verifizieren Sie deren Inhalt! Zwei 'system'-Dateien gehören zum Betriebssystem. Es sind 'MSDOS.SYS' und 'IO.SYS' bzw. 'PCDOS.SYS' und 'IBMBIO.SYS' je nach Betriebssystem.

9 Glossar

Im vorangegangenen Beitrag werden Abkürzungen und Begriffe verwendet, die im folgenden näher beschrieben werden sollen.

BIOS Basic Input Output System. Grundlegende Ein-/Ausgabefunktionen, die bereits teilweise im Festwertspeicher (ROM) gespeichert sind.

BOOT eigentlich 'Bootstrap'. Kaltstartvorgang des Computers, bei dem das Betriebssystem (DOS) von einem Massenspeicher in den Hauptspeicher geladen wird. Schutzmaßnahmen sind in dieser Zeit kaum gegeben.

DOS Disk Operating System. Betriebssystem des Computers, das (gewöhnlich) von Platte geladen wird. Residiert im ->RAM.

HIDDEN Dateien im Inhaltsverzeichnis[12)] können Attribute besitzen. Das 'hidden'-Attribut verhindert eine Anzeige bei 'DIR'.

[11)] <255> soll dabei ein Zeichen der Codierung 0x255 darstellen!

[12)] engl. directory

LINKVIRUS Virus, der sich in ein anderes ausführbares Programm einnistet

MIMIKRY Die Fähigkeit, sich zu tarnen und seiner Umwelt eine andere Gestalt vorzutäuschen.

PUBLIC DOMAIN nicht-kommerzielle Programme, die frei kopiert werden dürfen und gewöhnlich auf Selbstkostenerstattungsbasis weitergegeben werden.

RAM Random Access Memory. Synonym für den Hauptspeicher des Computers in den Programme geladen werden und der nach dem Abschalten wieder leer ist.

ROM Read-Only Memory. Festwertspeicher. Synonym für die fest gespeicherten Grund-Programme des Computers, die durch Software nicht verändert werden können. (Firmware)

SYSTEM siehe sinngemäß bei 'HIDDEN'.

TSR 'Terminate and Stay Resident'. Eine Methode der Erweiterung von Betriebsystemsfunktionen die auch von Viren gerne genutzt wird.

10 Beispiel für eine Virus-Liste

VIRUS CHARACTERISTICS LIST V56[13)]
Copyright 1989, McAfee Associates
408 988 3832

The following list outlines the critical characteristics of the known IBM PC and compatible viruses.

[13)] entnommen aus Quelle /**Fehler! Textmarke nicht definiert.**/

```
Infects Fixed Disk Partition Table------+
Infects Fixed Disk Boot Sector--------+ |
Infects Floppy Diskette Boot -------+ | |
Infects Overlay Files-------------+ | | |
Infects EXE Files---------------+ | | | |  Increase in
Infects COM files-------------+ | | | | |   Infected
Infects COMMAND.COM---------+ | | | | | |   Program's
Virus Remains Resident----+ | | | | | | |     Size
Uses Self-Encryption----+ | | | | | | | |      |
                        | | | | | | | | |      |
Virus                   V V V V V V V V V      V        Damage
-----------------------------------------------------
--------------
Taiwan                  . . . x . . . . .     708       p
Chaos                   . x . . . . x x .     N/A       B,O,D,F
Virus-90                . x . x . . . . .     857       P
Oropax                  . x . x . . . . .    2773       P,O
4096                    . x x x x x . . .    4096       D,O,P,L
Devil's Dance           . x . x . . . . .     941       D,O,P,L
Amstrad                 . . . x . . . . .     847       P
Payday                  . x . x x x . . .    1808       P
Datacrime II-B          x . x x x . . . .    1917       P,F
Sylvia/Holland          . x . x . . . . .    1332       p
Do-Nothing              . . . x . . . . .     608       p
Sunday                  . x . x x x . . .    1636       O,P
Lisbon                  . . . x . . . . .     648       P
Typo/Fumble             . x . x . . . . .     867       O,P
Dbase                   . x . x . . . . .    1864       D,O,P
Ghost Boot Version      . x . . . . x x .     N/A       B,O
Ghost COM Version       . . . x . . . . .    2351       B,P
New Jerusalem           . x . x x x . . .    1808       O,P
Alabama                 . x . . x . . . .    1560       O,P,L
Yankee Doodle           . x . x x . . . .    2885       O,P
2930                    . x . x x . . . .    2930       P
Ashar                   . x . . . . x . .     N/A       B
AIDS                    . . . x . . . . .    Overwrites Program
Disk Killer             . x . . . . x x .     N/A     B,O,P,D,F
1536/Zero Bug           . x . x . . . . .    1536       O,P
MIX1                    . x . . x . . . .    1618       O,P
Dark Avenger            . x x x x x . . .    1800       O,P,L
3551/Syslock            x . . x x . . . .    3551       P,D
VACSINA                 . x . x x x . . .    1206       O,P
Ohio                    . x . . . . x . .     N/A       B
Typo (Boot Virus)       . x . . . . x x .     N/A       O,B
Swap/Israeli Boot       . x . . . . x . .     N/A       B
```

1514/Datacrime II	x	.	.	x	x	.	.	.	.	1514	P,F
Icelandic II	.	x	.	.	x	.	.	.	.	661	O,P
Pentagon	.	.	.	.	.	.	x	.	.	N/A	B
3066/Traceback	.	x	.	x	x	.	.	.	.	3066	P
1168/Datacrime-B	x	.	.	x	.	.	.	.	.	1168	P,F
Icelandic	.	x	.	.	x	.	.	.	.	642	O,P
Saratoga	.	x	.	.	x	.	.	.	.	632	O,P
405	.	.	.	x	.	.	.	.	.	Overwrites	Program
1704 Format	x	x	.	x	.	.	.	.	.	1704	O,P,F
Fu Manchu	.	x	.	x	x	x	.	.	.	2086	O,P
1280/Datacrime	x	.	.	x	.	.	.	.	.	1280	P,F
1701/Cascade	x	x	.	x	.	.	.	.	.	1701	O,P
1704/CASCADE-B	x	x	.	x	.	.	.	.	.	1704	O,P
Stoned/Marijuana	.	x	.	.	.	.	x	.	x	N/A	O,B,L
1704/CASCADE	x	x	.	x	.	.	.	.	.	1704	O,P
Ping Pong-B	.	x	.	.	.	.	x	x	.	N/A	O,B
Den Zuk	.	x	.	.	.	.	x	.	.	N/A	O,B
Ping Pong	.	x	.	.	.	.	x	.	.	N/A	O,B
Vienna-B	.	.	.	x	.	.	.	.	.	648	P
Lehigh	.	x	x	.	.	.	.	.	.	Overwrites	P,F
Vienna/648	.	.	.	x	.	.	.	.	.	648	P
Jerusalem-B	.	x	.	x	x	x	.	.	.	1808	O,P
Yale/Alameda	.	x	.	.	.	.	x	.	.	N/A	B
Friday 13th COM	.	.	.	x	.	.	.	.	.	512	P
Jerusalem	.	x	.	x	x	x	.	.	.	1808	O,P
SURIV03	.	x	.	x	x	x	.	.	.		O,P
SURIV02	.	x	.	.	x	.	.	.	.	1488	O,P
SURIV01	.	x	.	x	.	.	.	.	.	897	O,P
Pakistani Brain	.	x	.	.	.	.	x	.	.	N/A	B

B - Corrupts or overwrites Boot Sector
O - Affects system run-time operation
P - Corrupts program or overlay files
D - Corrupts data files
F - Formats or erases all/part of disk
L - Directly or indirectly corrupts file linkage

HINWEIS: Diese Liste ist nicht vollständig! Angaben ohne Gewähr!

11 Hilfstruppen

Es gibt eine Reihe von Organisationen oder Firmen, die bei akuten Virenproblemen weiterhelfen können. Die Liste ist naturgemäß nicht vollständig:

MicroBIT Virus Center
Universität Karlsruhe
Rechenzentrum
Zirkel 2
D-7500 Karlsruhe

Virus Test Centrum
Universität Hamburg
Fachbereich Informatik
Schlüterstraße 70
D-2000 Hamburg 13

Forschungsinstitut für
Mikroprozessortechnik
Johannes Kepler Universität
A-4040 Linz
Österreich

Zentralstelle für Sicherheit
in der Informationstechnik
Am Nippenkreuz 19
D-5300 Bonn 2

12 Quellenangaben und Literatur

Zum Virenthema sind zahlreiche Veröffentlichungen in Fachzeitschriften erschienen, darunter auch [9] und [10].

1. 64'er; Ausgabe 3; März 1989; Markt&Technik Verlag, D-8013 Haar

2. "Angst vor Computer-Viren"; c't, Heft 7, 1988; Verlag Heinz Heise GmbH; D-5000 Hannover

3. Commodore Computing; Heft 10, 1988

4. Meyers Neues Lexikon; Band 8 Te-Zz; Bibliographisches Institut AG;

Mannheim; 1981

5. "The Worm Story"; The INTERNET Worm, Crisis and Aftermath; Communications of the ACM; No.6, Vol.32, June 1989

6. Schwab, G. Sagen des Klassischen Altertums; 1. Auflage 1968; Droemer Knauer

7. Security Managers Handbook; Digital Equipment Corporation; Maynard, Mass. USA

8. Bayrische Hackerpost; D-8000 München

9. MS-DOS Viren erkennen und bekämpfen; CHIP SPECIAL Best Nr. 1064; 1. Auflage 1990; Vogel Verlag Würzburg

10. "Keine Angst vor Viren"; PC Magazin Plus; Heft 9/89; Markt&Technik-Verlag; D-8013 Haar

13 Abbildungsverzeichnis

Abb. 1: Beispiel einer logischen Bombe 7
Abb. 2: Infektion einer COM-Datei 11
Abb. 3: Typische Infektion einer EXE-Datei 12
Abb. 4: Beispiel für einen Hauptspeicher-Auszug 19
Abb. 5: Beispiel für eine CHKDSK-Liste 20
Abb. 6: Beispiel für einen 'Fliegenfänger' 21