RZ info

UNIVERSITÄT DES SAARLANDES

Anwenderinformation des Rechenzentrums der Universität des Saarlandes

2. Jahrgang, Nr. 5 Juli 1989

Herausgeber: Rechenzentrum der Universität des Saarlandes
A. Schmitt, M. Schneider

Inhalt

Benutzermitteilungen:

- *MS-DOS-Kurse im Wintersemester* S. 2
- *Neue Version von CKOMM* S. 2
- *Boot-Virus auf Atari-Rechnern* S. 2
- *Rechnerzugang zum BS2000-Rechner 7.570 P* S. 3

Netzzugang über Wählanschlüsse S. 4
Programmabbruch im Dialog S. 5
HP-Plotter Master Draft II im RZ S. 6
Leitfaden für die Software-Nutzung S. 8
Urheberrechtsschutz für Software S. 10
Sabotage: Minen, Würmer, Viren und andere Arten von Vandalismus-Software S. 12

Computerviren auf der Spur:

- Teil 1 S. 13
- Teil 2 S. 17

Neue technisch-wissenschaftliche Anwendersoftware für BS2000 S. 23

Benutzermitteilungen

MS-DOS-Kurse im Wintersemester

Für den Herbst und das Wintersemester bietet das RZ wieder eine Reihe von MS-DOS-Kursen an. Die Kurse werden diesmal sowohl in Homburg als auch in Saarbrücken abgehalten.

Für die Kurse in Saarbrücken sind folgende Termine geplant:

dBase III	2.-4.10.89
MS-DOS	6.-8.10.89
MS-Word	9.-10.10.89
MS-Chart	16.-18.10.89
MS-Windows	13.-15.11.89
Multiplan	27.-29.11.89

In Homburg werden folgende Kurse abgehalten:

MS-DOS	2.-4.10.89
dBase III	8.-10.1.90
MS-Word	15.-17.1.90
MS-Chart	22.-24.1.90
MS-Windows	29.-31.1.90
Multiplan	5.-7.2.90

Der Ort für die Saarbrücker Kurse wird noch bekanntgegeben.

Interessenten melden sich bitte wie gewohnt bei der Anwenderberatung des RZ an, Tel. 302-3602.

Neue Version von CKOMM

Ab sofort ist die Version 2.01 des Kommunikationsprogramms CKOMM erhältlich, mit dem auf dem Campus installierte Atari-Rechner ins CANTUS-Netz eingebunden werden können. Mit dieser neuen Version ist nun auch ein bildschirmorientierter Dialog mit den zentralen UNIX-Rechnern möglich.

Kopien sind wie üblich auf 3 1/2 Zoll Disketten in der Anwenderberatung zu erhalten. (Bitte formatierte Leerdiskette mitbringen).

Boot-Virus auf Atari-Rechnern

Aus gegebenem - wenn auch nicht mehr ganz aktuellem - Anlaß möchte das RZ auf einen Virus hinweisen, der vor einiger Zeit auf den im RZ aufgestellten Atari-Rechnern entdeckt wurde. Der Virus wurde zufällig entdeckt, als mit einem dafür konzipierten Programm die Atari-Rechner des RZ auf das Vorhandensein von Viren untersucht wurden. Ansonsten hatte er sich nicht bemerkbar gemacht.

Bei diesem Virus handelt es sich um einen sogenannten 'Bootvirus', der sich im Bootsektor einer Diskette einnistet. Der Virus ist als Public-Domain-Virus bekannt und als harmlos einzustufen; er kopiert sich lediglich auf bisher 'saubere' bootfähige Disketten, zerstört jedoch keine Files und macht sich auch ansonsten nicht negativ bemerkbar.

Es ist nicht auszuschließen, daß der Virus bei der Weitergabe von Kopien des CKOMM-Programms, das Atari-Rechner ins Cantus-Netz einbindet und das seit etwa einem Jahr vom RZ an die Benutzer verteilt wird, auch auf Benutzerdisketten gelangt ist. Nach der Entdeckung des Virus wurden zwar sofort alle Disketten mit Programmkopien, die in der Benutzerberatung zur Verteilung bereitstehen, auf ihre 'Sauberkeit' hin untersucht; alle untersuchten Disketten waren in Ordnung. Möglich ist jedoch, daß einem Benutzer, dem das CKOMM-Programm auf eine mitgebrachte Diskette von der Festplatte des in der Benutzerberatung aufgestellten Ataris

kopiert wurde, unbeabsichtigt auch der Virus mitgegeben wurde.

Zur Behebung dieses Problems gibt es ein Public-Domain-Programm mit dem bezeichnenden Namen **'Sagrotan'**, mit dem Disketten auf Boot- und auch auf Link-Viren hin untersucht werden können (siehe auch den Artikel über Computer-Viren in diesem Heft). Boot-Viren werden von Sagrotan beseitigt; bei einem Befall durch Link-Viren müssen die befallenen Programme gelöscht werden.

Befallene Bootsektoren werden von Sagrotan dadurch gereinigt, daß Sagrotan einen eigenen Bootsektor schreibt, der nichts anderes bewirkt als bei Systemstart die Meldung "Kein Virus im Bootsektor" auszugeben. Durch das Überschreiben des - möglicherweise infizierten - usprünglichen Bootsektors wird ein evtl. dort vorhandener Virus beseitigt. Mit Sagrotan kann außerdem laufend die Größe der auf einer Platte gespeicherten Dateien kontrolliert werden. Ein unerklärliches Anwachsen der Dateigröße ist u.U. ein Indiz für einen Virusbefall.

Eine Kopie des Programms SAGROTAN V4.05 ist im RZ bei Rainer Blau, Tel. 2529 erhältlich.

Zugang zum BS2000-Rechner

Vor einigen Wochen stellte eine ganze Reihe von Anwendern verwundert fest, daß der BS2000-Host 7.570 P auf den Versuch des Anwenders, auf die gewohnte Weise ins System zu gelangen, durchaus ungewöhnlich reagierte: der übliche Zugang wurde verweigert und der Anwender mit einer Meldung wie etwa 'user has been severed' abgewiesen.

Auf einen mehr oder weniger empörten Anruf bei der Benutzerberatung hin konnte der Anwender erfahren, daß in der Zwischenzeit zusätzliche Kontrollen für den Zugang zum Produktionsrechner errichtet worden waren. Diese waren notwendig geworden aufgrund eines Hacking-Falles, bei dem ein unbefugter Benutzer sich in unrechtmäßiger Weise Zugang zum Produktionsrechner verschafft hatte. Der Betreffende konnte überführt werden.

Um eine Wiederholung zu vermeiden, wurden die Zugangskontrollen auf dem BS2000-Rechner 7.570 P erweitert.

Zum einen wurde der Zugangsschutz beim *LOGON*-Kommando dadurch verbessert, daß das System die logische Verbindung zur Datenstation abbricht, falls bei der Eingabe des *LOGON*-Kommandos falsche Angaben gemacht werden (z.B. falsches Paßwort, ungültige Abrechnungsnummer oder falsche User-ID). Dabei wird vom System nach jeder falschen Eingabe eine längere Pause bis zur nächsten Eingabemöglichkeit erzwungen. Auf diese Weise werden maschinelle *LOGON*-Versuche wesentlich erschwert.

Zur Verbesserung des Zugangsschutzes beim Rechnerzugang von außen wurde vom Systemverwalter eine Datei BEN.WAEHL auf der Kennung derjenigen Benutzer angelegt, die über Datex-P, einen Wählanschluß, von Endgeräten, die überwiegend von Kursteilnehmern genutzt werden oder über das Dialogprogramm TELNET ins System gelangen wollen. Die Datei BEN.WAEHL enthält ein zusätzliches Paßwort, das beim Einloggen abgefragt wird. Dieses Paßwort muß mit dem Systemverwalter vereinbart werden und kann mithilfe der Prozedur $DO BEN.WAEHL wieder abgeändert werden.

Zum andern werden Kennungen, die nicht mit einem Paßwort versehen sind, beim Systemstart automatisch gesperrt.

Es stellte sich im Rahmen dieser Maßnahme heraus, daß eine erschreckend große Zahl von Benutzern auf ihrer BS2000-Kennung überhaupt keinen Paßwortschutz vorgesehen hatte. Damit wurde eine wesentliche Möglichkeit, Unbefugten das Eindringen in die eigene Kennung zu verwehren, nicht genutzt.

Da die Verantwortung für etwaige Sicherheitseinbrüche aber zuerst beim RZ gesucht wird, sah sich das RZ veranlaßt, die Benutzer dazu zu bringen, die Schutzmechanismen, über die sie selber Einfluß haben, erst einmal voll auszuschöpfen. Aus diesem Grund werden seit dem 2. Mai alle Kennungen täglich überprüft, ob sie ein Kennungspaßwort enthalten. Wenn dies nicht der Fall ist, wird die Kennung automatisch gesperrt und nur nach Rücksprache mit dem Systemverwalter wieder freigegeben.

Das Paßwort zum Schutz der Benutzerkennung ist eine Zeichenfolge von bis zu 8

Zeichen) oder von bis zu 16 Sedezimalzeichen. Damit können 2^{64} verschiedene Paßwörter definiert werden. Wenn vernünftig gewählte, achtstellige Paßwörter verwendet werden, ist das Vorhaben, ein solches Vorhaben durch systematisches Ausprobieren zu 'knacken', langwierig und schwierig, auch wenn dies maschinell versucht wird.

Weil kurze Zeichenfolgen dazu verführen, einfache Begriffe als Paßwort zu wählen, sind Folgen aus nur 4 oder noch weniger Zeichen unter Sicherheitsaspekten zu kurz, besonders dann, wenn nur Ziffern oder nur Buchstaben für das Paßwort gewählt werden.

Eine Mischung aus 8 Ziffern, Buchstaben und Sonderzeichen wird dringend empfohlen, zumal hier an der Universität die User-ID aus dem Institutionenschlüssel abgeleitet ist. Eine solche Mischung erschwert das Erraten auch dann, wenn das Paßwort für den Berechtigten 'sinnvoll' und leicht merkbar aufgebaut ist.

Weitere Informationen zum Thema Rechnerzugang sind über das Informationssystem mittels der Prozedur DO $INFO.INFO erhältlich (Datei-Stichwort *Rechnerbenutzung.Prn.Nok*).

Netzzugang über Wählanschlüsse

MEDUSA abgeschaltet

Mittlerweile werden auch die letzten Anwender es bemerkt haben: seit April dieses Jahres ist das MEDUSA-Netz endgültig abgeschaltet. MEDUSA, der Vorläufer des jetzigen CANTUS-Netzes, war eines der ersten heterogenen Rechnernetze in Europa. Es wurde in den Jahren 1977 bis 1980 von den RZ-Mitarbeitern Frick und Berberich entwickelt. Über MEDUSA waren mehrere Hosts (TR440, VAX-Rechner, damals noch unter VMS, und Siemens-Rechner) und ca. 600 Terminals bzw. PCs miteinander verbunden.

Anschließbar an MEDUSA waren billige, herstellerunabhängige Peripheriegeräte für verschiedene Großrechner (Terminals, Drucker, Plotter, auch PCs). Im Laufe seiner Betriebszeit hatte sich dieses Netz als außerordentlich stabil erwiesen. Aus diesem Grund wurde es auch nach dem Abschluß der CANTUS-Installationsarbeiten weiterbetrieben. Mittlerweile ist die dem MEDUSA-Netz zugrundeliegende Technologie von der technischen Entwicklung jedoch überholt und veraltet.

Neue Modem-Anschlüsse an CANTUS

Die letzten Geräte, die noch über MEDUSA angeschaltet waren, waren die Telefon-Modems. Seit April gibt es neue Telefonmodems an CANTUS. Seit dieser Zeit nimmt das RZ an einem Feldversuch mit der Deutschen Bundespost teil. Bei diesem Versuch werden Hochgeschwindigkeitsmodems am Telefonnetz erprobt. Diese Modems erlauben den direkten Zugang zum CANTUS-Netz und damit den Zugang zu den an CANTUS angeschlossenen Hosts.

Bei dem neuen Modemtyp handelt es sich um den *Trailblazer Logem T2000* der Firma `kabelmetal elektro`. Folgende Übertragungsraten werden unterstützt:

V.21	300 Baud	vollduplex
V.22	1200 Baud	"
V.22bis	2400 Baud	"
PEP	18000 Baud	quasi-vollduplex

Das PEP-Verfahren *(Packetized Ensemble Protocol)* ist eine Multi-Carrier-Transmission, die z.Z. nur von diesem Gerät unterstützt wird. Alle anderen Verfahren sind von der CCITT genormt und sollten mit allen Geräten funktionieren, die eine FTZ-Nummer für das betreffende Verfahren haben. Außerdem können die MNP-, UUCP-, X-Modem- und Kermit-Protokolle unterstützt werden.

Sollte es bei bestimmten Parameter-Kombinationen zu Schwierigkeiten kommen, melden Sie sich bitte entweder bei der Anwenderberatung (Durchwahl: 3602) oder direkt bei Alfred

Neisius (Durchwahl: 2566). Eine genaue Beschreibung der neuen Modems und ihrer Möglichkeiten ist in der Benutzerberatung einzusehen.

Die Telefonnummern der Anschlüsse lauten:

0681/ 380 76 an CANTUS

0681/ 380 77 "

0681/ 380 78 "

0681/ 380 79 an SFBVAX

Um einem Mißbrauch der Anschlüsse vorzubeugen, muß jeder Benutzer explizit die Möglichkeit eines Dialoges von außen auf seiner User-ID erlauben. Im Falle des BS2000-Rechners muß unter seiner Kennung die Datei BEN.WAEHL vorhanden sein (siehe auch unter der Kennung $INFO die Datei 'Rechnerbenutzung', Kap. 2.1.1.6.2 'Zugang von außen' bzw. der Punkt 'Rechnerzugang' in den Benutzermitteilungen in diesem Heft).

Wird via Modem ein Anschluß an die Rechner UNIVAX bzw. SFBVAX gewünscht, ist in **jedem** Fall der zuständige Systemverwalter zu befragen (UNIVAX: Bernd Färber, Tel. 3623; SFBVAX: Bernhard Sieloff, Tel. 2434).

Durch diese explizite Erlaubnis kann sichergestellt werden, daß ein Zugang von außen nur auf den eigenen Wunsch des Benutzers möglich wird, und in diesem Fall auch noch zusätzliche Zugangsprüfungen stattfinden

Eine dringende Bitte an alle Modem-Benutzer:

Bitte versuchen Sie nicht, fremde User-IDs auszuspähen und zu benutzen und auf diese Weise unberechtigt Zugang zum Netz zu erhalten; schon der Versuch kann strafrechtlich verfolgt werden!

An dieser Stelle ist der Hinweis angebracht, daß jeder Modem-Benutzer bemüht sein sollte, sich nach einem Gespräch ordnungsgemäß auszuloggen und keine offenen Dialoge zu unterhalten. Wird ein Dialog nicht ordnungsgemäß beendet, kann der nächste Benutzer, der über die Nummer, auf der ein früherer Dialog noch besteht, auf die Kennung des Vorgängers gelangen; diese ist für den folgenden Anwender dann quasi ein 'offenes Buch'.

Für den Fall, daß einmal die Telefonverbindung unterbrochen wird, wird folgendes Vorgehen empfohlen:

- Versuchen Sie, die gleiche Wähl-Nummer erneut anzuwählen und beenden Sie Ihr früheres Gespräch.

- Sollte diese Wähl-Nummer besetzt sein, so wählen Sie eine andere Nummer an, eröffnen ein neues Gespräch und beenden Sie ihren alten Dialog (mithilfe des cancel-Kommandos o.ä.).

Programmabbruch im Dialog

Hin und wieder - bei unerfahrenen Benutzern meist etwas häufiger - tritt der Fall ein, daß ein im Dialog ablaufendes Benutzerprogramm in eine Endlosschleife gerät. Der auf diese Weise überraschte Benutzer wird meist verzweifelt nach dem berühmten Knopf zum Abstellen suchen. Falls dies nicht gelingt, werden leicht hohe Rechenzeiten verbraucht (beim jüngsten derartigen Fall waren es 100 CPU-Stunden!), Kapazitäten blockiert und nicht zuletzt unnötige Kosten verursacht. Aus diesem Grund sei an dieser Stelle auf eine Reihe von Kommandos hingewiesen, mit denen man solche Programme abbrechen kann.

Es spielt dabei keine Rolle, ob man einen lokalen Dialog mit der Siemens-Anlage führt oder sich über Datex-P von außen auf der Produktionsanlage 'eingelogged' hat.

Zur Programmunterbrechung, die vor dem *logoff* auf jeden Fall versucht werden sollte, stehen folgende Möglichkeiten zur Verfügung:

a) *Bei 9750-Bildschirmen:*

Drücken Sie die **K2-Taste**! Damit wird ein Break erzeugt.

b) *Bei einer Rechnerverbindung über CANTUS:*

Unterbrechen Sie das Programm durch Eingabe des CSAV-Vermittlerkommandos **#xan** oder durch eine **leere Eingabe (Line Feed)**. Durch Eingabe von #xan wird ein laufendes Programm, das sich im Zustand des Rechnens befindet, unterbrochen.

c) *Beim X.29-Zugang von außen über Datex-P* :

Gehen Sie durch Eingabe von **CTRL-P** in den PAD-Vorrangmodus und schicken Sie das Kommando **BREAK** ab.

Nach diesen Eingaben sollte das System wieder mit dem Eingabeaufforderungszeichen / antworten, worauf mit ***/logoff*** der Dialog ordnungsgemäß beendet werden kann.

Zum Abbruch eines Datex-P-Dialogs kann außerdem noch das CSAV-Kommando **#xen** abgeschickt werden; dieses Kommando bewirkt einen Verbindungsabbruch, jedoch im Falle einer Endlosschleife keinen Programmabbruch. Dieser wird nur erreicht, wenn ein neuer Dialog eröffnet wird, von dem aus der alte Dialog mit dem noch laufenden Programm beendet werden kann (cancel-Kommando). Deshalb sollte das Kommando #xen nicht benutzt werden zum Abbruch eines normalen (nicht Datex-P-)Dialogs.

Eine Aufstellung und genauere Charakterisierung der anderen CSAV-Vermittlerkommandos wird im nächsten RZ-INFO erscheinen.

Neuer Plotter HP Masterdraft II im RZ

Ab Juni 1989 steht den Anwendern des Rechenzentrums der Universität des Saarlandes ein *Hewlett-Packard MASTER DRAFT II Plotter* zur Verfügung. Standardmäßig ist der Plotter eingestellt für Zeichnungen im DIN A1 Format mit 8 Farben. Auf besonderen Wunsch - in Absprache mit den Operateuren - (Tel. 3554) kann der Plotter umgerüstet werden für Zeichnungen im DIN A0 Format mit 8 Farben.

Der Plotter ist an der BS2000-Anlage 7.570 P angeschlossen und wird über den Spoolout versorgt.

Logisch ist der Plotter als 'Drucker' für die Ausgabe von HPGL - Dateien anzusehen. ***HPGL*** ist die Hewlett-Packard Grafik Language, für die mehr oder weniger modifiziert auf den meisten Computer-Systemen ein Treiber existiert.

Es können - wo auch immer erzeugt - HPGL - Dateien, die über File-Transfer auf die BS2000-Anlage gebracht oder auf der BS2000-Anlage erzeugt wurden, mittels der Prozedur ***$DO.HPDRAFT*** auf den Plotter übertragen werden.

Plottinformation sollte mit dem HPGL - Kommando ***PLOTTER ON*** (ESC.Y oder ESC.( )) beginnen und mit dem Kommando ***PLOTTER OFF*** (ESC.Z oder ESC.()) enden. ESC steht für Escape (im EBCDIC Code X'27' oder 39 dezimal; im ASCII - Code X'1B' oder 27 dezimal). Information vor PLOTTER ON, zwischen PLOTTER OFF und PLOTTER ON, nach PLOTTER OFF wird ignoriert. Fehlt PLOTTER ON in der Information, so wird die gesamte Information als Plottinformation angesehen und vor der Ausgabe PLOTTER ON an den Plotter gesendet; entsprechend wird, falls die Information kein PLOTTER OFF enthält, nach Ausgabe PLOTTER OFF an den Plotter gesendet.

Information zwischen PLOTTER ON und LOTTER OFF wird als eine Zeichnung angesehen, so daß auch mehrere Zeichnungen ausgegeben werden können, z. B. 4 DIN A3 Zeichnungen auf der DIN A1 Zeichenfläche. Die Aufteilung der Zeichenfläche für die

einzelnen Zeichnungen wird von der Prozedur übernommen, so daß der Anwender keine Modifikation an seiner Information vornehmen muß.

Einige Kommandos können nicht zugelassen werden (z. B. die interaktiven Kommandos); diese werden in der Information gelöscht; einige Kommandos werden eingefügt oder geändert (z.B. Initialisieren und Beenden einer Plotausgabe). Der Anwender kann sich ein Protokoll über die Veränderungen erstellen lassen.

Die Information kann in EBCDIC oder in ASCII vorliegen. Die Codeumwandlung von ASCII --> EBCDIC wird von der Prozedur vorgenommen. Damit hat der Anwender die Möglichkeit, Dateien, die mittels Dateitransfer und Modus Binär auf die BS2000 Anlage übertragen sind, zu plotten.

Die Prozedur $DO.HPDRAFT besitzt eine Reihe von Parametern, die im Info ***$INFO.DO.HPDRAFT*** beschrieben sind. Eine Reihe von Parametern bestimmt Art und Umfang der allgemeinen Ausgabe, so

- ob geplottet werden soll,
- ob ein Protokoll erstellt werden soll,
- ob anfallende Information auf temporären Dateien abgelegt werden soll;

Eine weitere Reihe von Parametern beeinflußt die Plotter-Ausgabe,

- Festlegung der Größe der Zeichenfläche,
- Einteilung der Zeichenfläche in Teilflächen,
- Festlegung der Größe der Zeichnung,
- Festlegung des Nullpunktes der Zeichnung,
- Vergrößerungs-/Verkleinerungsfaktor für die Zeichnung,
- Umdefinition der Farbzuordnung.

Alle Parameter (außer Name der Eingabedatei) sind voreingestellt; wird als Eingabedateiname '*' angegeben, so zeigt die Prozedur alle Parameterwerte an und fragt, ob eine Änderung gewünscht wird. Wird die Prozedur mit 'HALT' verlassen, so bricht sie sofort ohne weitere Aktivitäten ab; wird die Prozedur mit 'END' verlassen, so werden die Parametereinstellungen ausgewertet.

Zur Anwendung der Prozedur : Eine Zeichnung wird auf einer (Teil-) Zeichenfläche dargestellt; dabei kann sie durch Festlegung des Nullpunktes verschoben werden und/oder durch Angabe der Größen von Zeichnung und (Teil-) Zeichenfläche 'gezoomt' werden (Anpassung in DINA-Format Einheiten) ; statt gezoomt kann die Zeichnung auch vergrößert oder verkleinert werden duch Angabe eines Faktors.

Die Beschreibung von HPGL entnimmt man den Programming Manuals for Graphics Plotter von HEWLETT-PACKARD.

Das Rechenzentrum bittet alle Anwender, die ihre Graphik über HPGL - Dateien erstellen, den neuen Plotter zu testen.

HINWEIS:

Das RZ weist in diesem Zusammenhang darauf hin, daß der nunmehr fast 20 Jahre alte, bisher genutzte CALCOMP-Plotter zum 31.12.89 stillgelegt wird.

Leitfaden zu ethischen und moralischen Fragen der Software-Nutzung

Analog zu einer ähnlichen Initiative in den USA soll jetzt auch hierzulande durch einige energische Schritte der unerlaubten Software-Nutzung begegnet werden. Jeder weiß oder vermutet zumindest, daß das Anfertigen von Software-Kopien eine unerlaubte Handlung darstellt; und wer möchte von sich behaupten, er habe noch nie bei einem Freund ein interessantes Programm entdeckt, das man selber 'immer schon haben wollte' oder 'gut gebrauchen kann' und sich durch eine schnelle Kopie im Handumdrehen in den Besitz dieser Software gebracht? Die Vielfalt der auf dem Markt angebotenen Software ist hoch, die Preise mitunter prohibitiv; es ist naheliegend und allzumenschlich, daß man sich auf leichte Art vor unliebsamen Kosten drückt.

Ungeachtet der Häufigkeit, mit der die 'unautorisierte' Software-Nutzung (weniger fein auch bekannt als 'Software-Klau' oder, in größerem Umfang, auch als 'Software-Piraterie') praktiziert wird, ist sie dennoch eine unerlaubte Handlung, der die *Arbeitsgemeinschaft der Leiter wissenschaftlicher Rechenzentren (ALWR)* nun mit einem **'Leitfaden zu ethischen und rechtlichen Fragen der Software-Nutzung** zu Leibe rücken will.

Vorbild für diesen Leitfaden war ein amerikanisches Papier, das von zwei amerikanischen Vereinigungen aus dem Hochschulbereich bzw. der Industrie, EDUCOM und ADAPSO, erstellt wurde. Der ALWR hat von diesem Papier als deutsche Fassung den oben benannten Leitfaden herausgebracht, der in Kürze verabschiedet und danach in großem Umfang verteilt werden soll. Er wird dann auch über das RZ zu erhalten sein. Die wichtigsten inhaltlichen Punkte aus diesem Leitfaden seien hier vorab kurz skizziert; eine ausführlichere Behandlung des Themas Urheberschutz von Software hat uns freundlicherweise im anschließenden Artikel Prof. Herberger vom Lehrstuhl für Rechtsinformatik gegeben.

Einige wichtige Grundsätze der Software-Nutzung:

Unautorisiertes Kopieren von Software ist unzulässig; Software ist durch das Urheberrecht genauso geschützt wie ein Erfinder durch das Patentrecht.

Das unautorisierte Kopieren von Software durch einzelne Mitglieder einer Universität kann die Institution als ganze beeinträchtigen, da sie für die Handlungen einzelner zur Verantwortung gezogen wird. Es liegt auf der Hand, daß durch unautorisiertes Kopieren einzelner ihrer Mitglieder eine Universität auch in ihrem Bemühen, Software legal weiterzuverbreiten und dabei günstigere Konditionen zu erhalten, geschwächt wird.

Wenig bedacht wird der Punkt, daß unerlaubtes Kopieren von Software nicht nur ihre Entwickler um den Lohn für ihre Arbeit bringt, sondern auch den Preis für Software in die Höhe treibt (weil dieses Raubkopieren bei der Preisfestsetzung einkalkuliert wird). Außerdem mindert sich dadurch die Qualität der weiteren Unterstützung, z.B. die Lieferung von Nachbesserungen.

Einige Aspekte zum Thema 'Software' und 'Recht'

- Software ist grundsätzlich durch das Urhebergesetz geschützt. Nur der Urheber hat das Recht zu Reproduktion und Vertrieb von Software. Public-Domain-Software ist von dieser Regelung ausgenommen. Erlaubt ist auch das Anfertigen von Sicherungskopien von rechtmäßig erworbenen Originaldisketten.

- Wurde gekaufte Software mit einer klar erkennbaren Lizenz-Vereinbarung ausgeliefert, so ist man bei einer evtl.

Weitergabe durch diese Lizenzbedingungen gebunden. Sofern diese Bedingungen es nicht ausdrücklich gestatten, ist die Nutzung auf mehreren Rechnern gleichzeitig nach dem Urheberrecht nicht erlaubt. Es kann aber erlaubt sein, einem Freund die Software auf Zeit auszuleihen, sofern eine Kopie beim Eigentümer verbleibt und dieser die Software in dieser Zeit auch nicht nutzt.

- Auch bei nicht ausdrücklich durch Copyright-Vermerke kopiergeschützter Software dürfen zur Weitergabe oder zum Verkauf keine Kopien angefertigt werden. Der fehlende Kopierschutz ist dabei als besondere Vertrauensbeweis gegenüber dem Käufer anzusehen.

- Bei Software, die in Campus-Einrichtungen zur Verfügung gestellt wird, und die gewöhnlich lizensiert ist, regeln die Lizenzen, wie und wo die Software von Mitgliedern der Institution genutzt werden darf. Es gibt Campus-Lizenzen, die für bestimmte Zwecke Kopien erlauben. Im Zweifelsfall ist bei einem hierfür kompetenten Mitarbeiter der Institution nachzufragen (in unserem Fall im RZ).

- Ausdrücklich nicht erlaubt ist die Vervielfältigung von Software durch einen Studenten oder anderen Hochschulangehörigen, um sie an die Teilnehmer eines Kurses oder einer Vorlesung zu verteilen, es sei denn, der Autor oder Vertreiber der Software lassen dies explizit zu.

- Auch Software, die über Software-Überlassungsverträge beschafft wurde, darf nicht kopiert werden, wenn der Hersteller, Verkäufer oder Vertreiber das im Vertrag untersagt.

Software ist mitunter recht teuer. Nicht immer kann man sich den Kauf der benötigten oder gewünschten Software leisten. Für diese Fälle gibt es einige rechtlich zulässige Alternativen zum unautorisierten Kopieren.

- Campus-Lizenzen und Mengenlizenzen

Die Hersteller oder Vertreiber von Software gewähren vielen Institutionen die Software-Nutzung zu besonders günstigen Konditionen. Darunter fallen auch die Campus- oder Mengenlizenzen. Doch auch Software mit diesen Lizenzen unterliegt dem Rechtsschutz und darf nicht ohne weiteres kopiert werden.

Fragen Sie im Bedarfsfall im RZ nach.

- Shareware

Bei Shareware handelt es sich um kopiergeschützte Software, bei der der Entwickler selbst dazu ermuntert, die Software zu benutzen und weiterzugeben. Diese Erlaubnis ist explizit in der Dokumentation enthalten. Lediglich eine kleine finanzielle Anerkennung oder Meldegebühr ist zu entrichten, wenn man die Software weiternutzen möchte. Im Falle einer Meldung erhält man weitere Unterlagen, Verbesserungen u.ä.

- Public-Domain-Software

Einige Autoren bestimmen, daß ihre Software frei verfügbar, also "public-domain" sein soll. Diese Art von Software unterliegt keinen Copyright-Bestimmungen und kann frei kopiert und verteilt werden. Da Software ohne Copyright-Vermerke public-domain sein kann, aber nicht muß, sollte man bei Software, die nicht ausdrücklich als public-domain gekennzeichnet ist, vor der Weitergabe stets den Rat von Experten einholen.

Die Konditionen zur Nutzung von Sofware sind sehr unterschiedlich geregelt. Deshalb sollte man bei jedem einzelnen erworbenen Software-Produkt die Begleitunterlagen prüfen. Im allgemeinen besteht kein Recht

- unautorisierte Softwarekopien entgegenzunehmen und zu nutzen oder

- unautorisierte Softwarekopien für andere herzustellen.

Fragen Sie deshalb im Zweifelsfall im RZ nach.

Urheberrechtsschutz für Software

Einige Anmerkungen zur "Lage"

von Maximilian Herberger

Daß Computerprogramme "im Prinzip" Urheberrechtsschutz genießen, ist nach einer entsprechenden Ergänzung des Urheberrechtsgesetzes (UrhG) im Jahre 1985 außer Streit. Paragraph 2 ("Geschützte Werke") UrhG lautet in dem diesbezüglichen Passus:

"(1) Zu den geschützten Werken der Literatur, Wissenschaft und Kunst gehören insbesondere:

1. Sprachwerke, wie Schriftwerke und Reden, sowie Programme für die Datenverarbeitung; ..."

Allerdings entscheidet nicht die Zugehörigkeit zum Katalog der geschützten Werke allein bereits über den urheberrechtlichen Schutz. In Betracht gezogen werden muß vielmehr zusätzlich noch Paragraph 2 Abs. 2 UrhG:

"(2) Werke im Sinne dieses Gesetzes sind nur persönliche geistige Schöpfungen."

Erst wenn ein Computerprogramm im Sinne dieser Vorschrift als "persönliche geistige Schöpfung" angesprochen werden kann, was voraussetzt, daß es einen ausreichenden "schöpferischen Eigentümlichkeitsgrad" aufweist, ist urheberrechtlicher Schutz gegeben.

Es leuchtet ein, daß die Kategorie "persönliche geistige Schöpfung" in diesem Sinne nicht einfach zu handhaben ist. Bezogen auf Software hat der Bundesgerichtshof (BGH) den Maßstab in der "Inkassoprogramm"-Entscheidung vom 9. Mai 1985 (vgl. "Informatik und Recht" 1986, S. 18 - 23) festgelegt. Danach ist bei der nötigen Beurteilung auszugehen "von den vorbekannten Programmen und den Arbeitsergebnissen der einzelnen Entwicklungsstufen mit ihren jeweils bekannten und üblichen Anordnungen, Systemen, Aufbau- und Einteilungsprinzipien" (S. 22). Dieser erste Bezugspunkt kann bereits als Ausschlußkriterium dienen:

"Alle in deren Nähe bleibenden Gestaltungsformen besitzen keinen hinreichenden schöpferischen Eigentümlichkeitsgrad." (a.a.O.)

Das zweite Testkriterium bildet ein Vergleich mit dem "Können des Durchschnittsprogrammierers":

"Lassen sich nach Maßgabe des Gesamtvergleichs mit dem Vorbekannten schöpferische Eigenheiten feststellen, so sind diese dem Schaffen eines Durchschnittsprogrammierers gegenüberzustellen. Das Können eines Durchschnittsgestalters, das rein Handwerksmäßige, die mechanisch-technische Aneinanderreihung und Zusammenfügung des Materials liegt außerhalb jeder Schutzfähigkeit." (a.a.O.)

Damit wird der Bereich der Schutzfähigkeit sehr weit vom Normalbereich entfernt angesiedelt. Mit den Worten des BGH:

"Erst in einem erheblich weiteren Abstand beginnt die untere Grenze der Urheberrechtsschutzfähigkeit, die ein deutliches Überragen der Gestaltungstätigkeit in Auswahl, Sammlung, Anordnung und Einteilung der Informationen und Anweisungen gegenüber dem allgemeinen Durchschnittskönnen voraussetzt." (a.a.O.)

Man hat aus dem zitierten Urteil zu Recht den Schluß gezogen, daß nur ein kleiner Teil der Software-Produktion, gewissermaßen die "creme de la creme" (vgl. Röttinger, in: Informatik und Recht 1986, S. 15), den Schutz des Urheberrechts genießt. Quantifizierende Schätzungen der Schutzdichte gehen weit auseinander. In der extremsten Variante wird angenommen, daß nur etwa 10% der am Markt verfügbaren Software den Test des BGH passieren würde.

Wer nun allerdings den skizzierten Befund so interpretiert, daß man risikolos von der Annahme ausgehen könne, es weitgehend mit ungeschützter Software zu tun zu haben, muß gewarnt werden. Zum einen (aber das zu beurteilen fällt nicht in die Kompetenz des Juristen) könnte es selbst bei einer insgesamt niedrigen Quote geschützter Software in Teilbereichen (etwa bei wissenschaftlicher Software) doch so sein, daß in diesem Sektor ein wesentlich höherer Anteil von Software geschützt ist. Was aber praktisch für die Orien-

tierung wichtiger ist, ist die Tatsache, daß unterinstanzliche Gerichte oft wesentlich großzügiger als der BGH die Schutzfähigkeit von Software bejahen. Dies gilt vor allem (und deswegen ist Sorglosigkeit in keinster Weise angezeigt) für die Strafverfolgungspraxis. In einer ganzen Anzahl von Fällen ist beim Kopieren selbst "normaler" Spiel-Programme eine Strafbarkeit angenommen worden. Von diesem praktisch wichtigen Aspekt soll deswegen abschließend die Rede sein, wobei auch die zivilrechtlichen Konsequenzen einer Urheberrechtsverletzung mit einzubeziehen sind.

Das Urheberrechtsgesetz enthält mit Paragraph 106 eine Strafbestimmung folgenden Inhalts:

"Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."

Im Falle des gewerbsmäßigen Handelns erhöht sich die Strafe nach Paragraph 108a UrhG auf "Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe". In dieser Variante des gewerbsmäßigen Handelns ist auch bereits der Versuch strafbar (Paragraph 108a Abs. 2 UrhG).

Zusätzliche Kosten können auf den Täter dadurch zukommen, daß der Verletzte bei Vorliegen eines berechtigten Interesses im Falle einer Verurteilung verlangen kann, daß die Verurteilung öffentlich bekanntgemacht wird. Die Art der Bekanntmachung ist im Urteil zu bestimmen (Paragraph 111 UrhG).

Unter Umständen sind die zivilrechtlichen Konsequenzen finanziell spürbarer als eine strafrechtliche Verurteilung zu einer Geldstrafe. Paragraph 97 Abs. 1 UrhG bestimmt nämlich, daß der Verletzte den Urheberrechtsverletzer im Falle von Vorsatz oder Fahrlässigkeit auf Schadensersatz in Anspruch nehmen kann. Dieser Ersatzanspruch umfaßt den gesamten Schaden, der ursächlich auf die Verletzungshandlung zurückgeht.

Zusammenfassend kann man sagen: Soweit sich die Praxis der Strafverfolgung überblicken läßt, muß man auch bei Software, die nicht den strengen Test des BGH passieren würde, mit einer Bestrafung nach den dargestellten Vorschriften rechnen, falls man eine unerlaubte Verwertungshandlung (Vervielfältigen etc.) begeht. Das ist eine unerfreuliche Situation. Unerfreulich deswegen, weil im Einzelfall eine nicht unerhebliche Rechtsunsicherheit besteht und sich außerdem je nach örtlicher Strafverfolgungspraxis eine heterogene Strafbarkeits-"Geographie" entwickeln kann. Diese Kritik ändert aber nichts daran, daß man sich auf die Situation so einrichten muß, wie sie sich gegenwärtig darstellt.

Wer sich übrigens genauer für diese (und andere) mit der EDV verbundene Rechtsfragen interessiert, kann dazu regelmäßig etwas in der ***Zeitschrift "jur-PC"*** *und dem dazugehörigen Newsletter lesen. Für die aktuelle Debatte gibt es dann noch die zugehörige* ***Mailbox "jur-PC"****, die über Datex-P (NUA: 45612133061) erreichbar ist. Außer einer persönlichen Anmeldung "kostet" die elektronische Lektüre dort nichts.*

(Nähere Auskünfte beim Lehrstuhl für Rechtsinformatik, Bau 15, Tel.: 302-3105)

Sabotage: Viren, Minen, Würmer und andere Arten von Vandalismus-Software

Ähnlich wie andere Hochschulen vor ihr muß sich nun auch die Universität des Saarlandes mit einem Problem befassen, das auch schon andere Hochschulen heimgesucht hat und das die Fachpresse seit etwa einem Jahr nicht mehr zu Ruhe kommen läßt.

Die Rede ist hier von Destruktiv-Programmen, 'Viren', 'Würmer', 'Minen', 'Pilze' und 'Trojanische Pferde', die auf äußerst unheilvolle Weise in den Rechner oder die Datenbestände eines Benutzers eingreifen.

Vor einigen Monaten wurde auf den beiden Atari-Rechnern des RZ ein bekannter harmloser Bootvirus entdeckt (siehe Benutzermitteilungen, S. 2). Außerdem stellte man vor wenigen Wochen auch auf den in der Benutzerberatung aufgestellten MS-DOS-Rechnern einen Virus fest, dessen unmittelbar sichtbare Wirkung darin besteht, befallene Programme kontinuierlich zu vergrößern und auf diese Weise unnötig Speicherplatz zu belegen.

Ausgerechnet CANTUS.DIA, das CANTUS-Kommunikationsprogramm für IBM- und kompatible Rechner erwies sich als befallen; da dieses Programm vom RZ routinemäßig verteilt wird, war der Virus unwissentlich auch an Benutzer weitergegeben worden. Wann und auf welche Weise es infiziert wurde, ist bei einem quasi-allgemein verfügbaren Rechner, zu dem der Zugang kaum kontrolliert werden kann, nicht zu rekonstruieren.

Was getan werden konnte, war die Reinigung des Rechners und eine Neuinstallation nachweislich unbefallener Programme sowie gewisse Schutzmaßnahmen, die einen erneuten Befall - der nicht auszuschließen ist -zumindest sofort anzeigen. Absoluten Schutz können weder organistorische Maßnahmen bieten, die den Zugang zum Rechner und das Einspielen neuer Software kontrollieren, noch programmtechnische Maßnahmen. Die einzige Methode, die einen Rechner garantiert vor Virusbefall schützen kann, - man belasse hierzu einfach den Netzstecker permanent im Zustand 'aus' - , ist eine rein theoretische, die in der Praxis leider nicht eingesetzt werden kann.

Erfahrung in der Entdeckung und Beseitigung von Sabotage-Software wird mittlerweile auch in der Bundesrepublik an verschiedenen Stellen gesammelt. Seit Mai 1988 arbeitet an der Universität Hamburg das Virus-Test-Center, das aus infizierten Programmen durch Rückverfolgen den Virus ermitteln, analysieren und beschreiben will ('Reverse Engineering').

Auch an der Universität Karlsruhe werden seit einiger Zeit im PC-Beratungszentrum Micro-BIT intensive Erfahrungen mit diesem Problem gesammelt. Neben der Analyse von Computer-Viren ist man dort auch mit der Entwicklung von Software beschäftigt, die einen Virenbefall frühzeitig erkennt. Aufgrund der großen Zahl von IBM- und kompatiblen Geräten ist das Know-How über die gerade auf diesen Rechnern aufgetretenen Viren besonders groß.

Die entsprechenden Mitarbeiter veröffentlichten außerdem in ihrem Benutzer-Informationsjournal einen ausführlichen Artikel über Computer-Viren, den sie uns für einen Nachdruck freundlicherweise zur Verfügung gestellt haben.

Computerviren auf der Spur

von Christoph Fischer und Torsten Börstler

Die Autoren dieses Beitrags sind im Microcomputer Beratungs- und Informationsteam (Micro-BIT) am Rechenzentrum der Universität Karlsruhe beschäftigt und befassen sich schon seit längerer Zeit mit dem Thema Viren.

Dieser Artikel wurde bereits im Micro-BIT Journal der Universität Karlsruhe veröffentlicht und wird hier mit freundlicher Genehmigung der Autoren wiedergegeben.

Durch internationale Vernetzung und zunehmenden Softwareaustausch ergibt sich eine ständig wachsende Bedrohung durch Computer-Viren.

Zu dieser Problematik wurden schon zahlreiche Artikel in den unterschiedlichsten Zeitschriften veröffentlicht. Das Thema ist jedoch so brisant, daß auch wir hierzu Stellung nehmen und Ihnen bei einer Infektion im Rahmen unserer Möglichkeiten mit Rat und Tat zur Seite stehen möchten. Wir erwarten in allernächster Zukunft einen massiven Einbruch von Viren in den Campusbereich der Universität Karlsruhe, wie bereits in Konstanz und Mannheim, sowie an der Fachhochschule Karlsruhe schon geschehen. Die dortigen Einrichtungen haben bereits mit einer gründlichen Durchseuchung zu kämpfen. Die Unkenntnis der Benutzer - oft sind es auch Unvernunft und Spieltrieb - werden dafür sorgen, daß mit großer Sicherheit auch die Rechner in unserem Bereich befallen werden.

Um in einer Großaktion die PCs (zur Zeit ca. 1800 im Bereich des Uni-Campus) zu überprüfen und befallene Programme aufzuspüren, Schutzmechanismen einzubauen und durch Aufklärungsaktionen für entsprechende Datenhygiene zu sorgen, werden nach unseren Berechnungen, die sich auf Erfahrungen an anderen Universitäten stützen, Kosten von ca. zweihunderttausend bis eine halbe Million Mark entstehen. Dabei sind Belastungen, die durch die Vernichtung nicht wiederbeschaffbarer Datenbestände entstanden sind, nicht eingerechnet.

Um die katastrophalen Auswirkungen eines solchen "Daten-GAUs" einzudämmen und einige Schutzvorkehrungen zu treffen, haben wir uns entschlossen, einige grundlegende Kenntnisse über Viren und verwandte Vandalismus-Software zu vermitteln. Micro-BIT entwickelt zur Zeit ein Softwarepaket, das den Befall durch Viren frühzeitig erkennt. Diese Software wird in Kürze kostenlos bei uns erhältlich sein. Spezialsoftware, mit der man bestimmte Viren aufspüren bzw. entfernen kann (Bitte keine allzu großen Hoffnungen; dies gelingt nur bei ganz primitiven Viren), wird Micro-BIT dann nur durch einen eigenen Mitarbeiter zum Einsatz bringen, um das Know-How keinesfalls in die Hände der Leute gelangen zu lassen, deren einziges Ziel es ist, Ihnen zu schaden.

Grundsätzlich sind drei Arten von Vandalismus-Software zu unterscheiden:

Die erste betrifft Rechnersysteme, die durch Kommunikationseinrichtungen miteinander verbunden sind. Solche Programme werden allgemein als *Netzwerk-Würmer* (Networkworms) bezeichnet. Sie haben meist keine zerstörerischen Auswirkungen, sondern verschicken sich selbst an weitere "Opfer", also eine Art automatisierter Kettenbrief.

Die zweite Art sind sogenannte *Trojanische Pferde* , die durch interessante Namen, Beschreibungen und Täuschungen den unkritischen Benutzer dazu veranlassen, sich ein solches Paket zu beschaffen (z.B. von Mailboxen) und auf seinem Rechner auszuführen. Dies endet meistens mit einer zerstörten Harddisk.

Die dritte Sorte sind die eigentlichen *Viren,* die ausführbaren Code infizieren und somit beliebige Programme als Verbreitungsmittel für sich selbst benutzen. Dabei bleibt ihr Werk nicht allein auf die Verbreitung beschränkt, da das Virusprogramm bei jedem Aufruf beliebige Operationen ausführen und damit unvorhersagbare Resultate erzielen kann.

Netzwerk-Würmer sind im PC-Bereich momentan nicht als akute Gefahr zu betrachten. Dennoch möchten wir die beiden bekanntesten kurz erläutern. Der Weihnachtsbaum-Wurm, der allen VM-Benutzern (Großrechner) unter dem Namen CHRISTMAS EXEC bekannt ist, benötigte gleich zweimal das manuelle Eingreifen des Benutzers! Das EXEC-Programm (Kommandosprache auf Be-

triebssystemebene) mußte durch einen Receive-Befehl aus dem elektronischen Briefkasten (Readerlist) genommen werden und in einem zweiten Schritt explizit aufgerufen werden. Für den Benutzer wurde danach am Bildschirm eine aus Buchstaben "gebastelte" Tanne angezeigt. Somit verstand jeder das Programm als einen Weihnachtsgruß.

Das unheilvolle Wirken jedoch begann im Hintergrund. Das elektronische Adreßbuch und das elektronische Posteingangs-/ausgangsbuch des Benutzers diente dem Programm als Verzeichnis von weiteren Mailbox-Teilnehmern, an die es sich jeweils selbst weiter versandte. Dieser deutsche Netzwerk-Wurm führte bis in die USA zu einer katastrophalen Verstopfung im Bereich von EARN / BITNET, sogar bis in das firmeneigene Netz von IBM, das seither total abgeschirmt wird.

Der zweite Wurm ist erst kürzlich aufgetreten und durch die Presse als Virus bezeichnet worden, was abermals nicht zutrifft. Dieses Programm hat eine haarsträubende Fähigkeit einiger UNIX-Mailer verwendet, um ohne Interaktion durch einen Benutzer zur Ausführung zu gelangen. Diese Mailerfunktion wurde daraufhin in einer Großaktion in den USA aus allen im ARPA-NET befindlichen Rechnern entfernt. Das Programm bestand aus einer SHELL (Pendant zu EXEC aus dem VM-Bereich), mit der unglaublichen Fähigkeit, beim Eintreffen sofort und ohne Benutzereingriff zur Ausführung zu gelangen. Dieser Wurm hat dann ständig neue Shells eröffnet, die wertvolle Rechnerkapazitäten belegten und somit zu einem Zusammenbruch des Rechners aufgrund der Überlastung führten.

Zusammenfassend sollte man sich merken:

Niemals unaufgefordert bzw. von unbekanntem Sender erhaltene Mail ausführen! Sourcecode anfordern und durch Experten überprüfen lassen. Es besteht Gefahr, daß Ihre Daten zerstört bzw. ausgekundschaftet werden!

Die sogenannten **trojanischen Pferde** sind für PC-Besitzer, die Mailboxen bzw. Public-Domain-Server benutzen, eine besondere Gefahr. Durch vielversprechende Namen und Beschreibungen verleiten sie den Benutzer, diese Software auf den PC zu übertragen und dort auszuführen. Zur Überraschung des Anwenders verbirgt sich jedoch darunter kein sinnvolles Programm sondern ein zerstörerisches Machwerk. Das kann zum Beispiel so aussehen, daß nach einem hämischen Kommentar Ihre Festplatte formatiert wird oder die darauf befindlichen Directories oder Dateien gelöscht bzw. nachteilig verändert werden. Die Untersuchung von Programmpaketen, die man in reinem Binärformat erhält, ist langwierig und nur durch einen Assemblerfachmann zu bewerkstelligen und meist sehr unwirtschaftlich. Deshalb sollte man keine Programme zur Ausführung bringen, deren Wirken nicht bekannt und deren Resultate nicht vorhersehbar sind. Beim Micro-BIT kann eine Liste solcher Programme eingesehen werden, die bekannte trojanische Pferde und deren Wirkungsweise enthält.

Programmierer solcher trojanischen Pferde verfallen dabei auf ganz üble Tricks. Um Speicherplatz zu sparen, werden Daten auf einem Server meist in einem gepackten Format abgelegt. Mittels eines Dekomprimierungsprogrammes namens *ARC* können die Daten wieder in lesbare Form konvertiert werden. Auf einigen Servern fand sich plötzlich ein Programm **ARC513.EXE**, das nicht nur, wie erwartet, Dateien im ARC-Format komprimiert bzw. dekomprimiert, sondern zusätzlich noch die Spur 0 der Hard-Disk überschreibt. An dieser Stelle befindet sich der Boot-Sektor der Festplatte. So mancher Benutzer wurde nach dem Einschalten seines Rechners plötzlich mit der Meldung "No system disk" empfangen.

Verheerendere Wirkung haben trojanische Pferde, die die File Allocation Table (FAT) bzw. das Directory einer Festplatte verändern oder sogar durch Aufruf des Low-Level-Formatters - dieser ist in der Regel in jedes BIOS eines DOS-Rechners integriert - den gesamten Inhalt der Platte vernichten.

Zusammenfassend sollte man sich merken:

Je vielversprechender der Name eines Programmes, desto vorsichtiger sollte man im Umgang mit diesem sein. Führen Sie solche Pakete zunächst auf einem reinen Floppy-System aus oder unterbrechen Sie die physikalische Verbindung zur Festplatte, um einen etwaigen Schaden durch das Unwesen eines trojanischen Pferdes zu begrenzen.

Die dritte Sorte sind die eigentlichen **Viren**, die durch ihre Fähigkeit, sich heimlich an Programme anzuhängen und beliebig oft fortzupflanzen, wohl die weiteste Verbreitung gefunden haben und damit die höchste Gefahr für Ihre Daten darstellen!

Die Palette der Arbeitsweise von Viren ist ebenso weit gestreut wie bei den Netzwerk-Würmern und den trojanischen Pferden. Es sei an dieser Stelle auch erwähnt, daß nicht nur Spieltrieb und Langeweile zum Entstehen eines Virus beitragen, sondern zum Teil auch böswillige oder sogar kriminelle Absichten dahinterstecken. Deshalb zunächst einige Beispiele, mit welcher Unverfrorenheit Viren-Programmierer zu Werke gehen.

Der **1704- oder Black Jack Virus** infiziert COM-Dateien. Seinen Namen hat er zum einen durch die Eigenschaft erhalten, COM-Dateien um 1704 Bytes zu vergrößern, zum anderen durch das Kartenspiel 17 und 4, das im Englischen Black Jack genannt wird. Der Virus ist auch unter der Bezeichnung "Second Austrian Virus" oder "T-Virus" bekannt sowie eine Abart davon, die COM-Dateien um 1701 Bytes verlängert.

Es gibt unterschiedliche Berichte über die Auswirkungen dieser Virusfamilie. Sicher ist, daß der Virus zunächst die Copyright Meldung im ROM-BIOS überprüft, ob der String "CORP. IBM" vorhanden ist. Er infiziert dann weiter die COM-Dateien, aber aktiviert nicht seine Störaktionen.

Wird das Programm nicht auf einem orginalen IBM PC gestartet, so aktiviert der Virus nach dem 1. Oktober 1988 sein nervenaufreibendes Spiel mit dem Bildschirminhalt: unter einem prasselnden Geräusch im Lautsprecher rieseln alle Buchstaben nach unten.

Beim Disassemblieren wurden in den bis jetzt bekannten Versionen des Virus keine Anhaltspunkte auf Programmteile gefunden, die Datenbestände löschen bzw. verändern. Dieser Virus scheint damit eher ungefährlich zu sein, was aber nicht bedeutet, daß man bei den oben genannten Veränderungen von COM-Dateien nicht sofort Sicherheitsmaßnahmen ergreifen sollte. Es ist jederzeit möglich, daß eine gleichartig aussehende Abart auftaucht, die dann Datenbestände auf Disketten und Festplatten bedroht.

Der Weiterverbreitungsmechanismus ist relativ hoch entwickelt, er installiert sich in chiffrierter Form als residente DOS-Extension im RAM und befällt von dort aus uninfizierte Programme. Er prüft die Schreibschutzeinrichtung von Diskettenlaufwerken, um nicht durch einen unerwarteten Schreibvorgang auf eine Diskette auf sich aufmerksam zu machen, was durch die entsprechende DOS-Fehlermeldung geschehen würde. Dateien, deren DOS-Flag auf Read-Only gesetzt ist, werden dennoch befallen. Filedatum und Filezeit werden bei der Infektion nicht verändert, nur die Länge der Datei wird um die oben genannten Werte vergrößert.

Ein Suchprogramm, das speziell diesen Virus lokalisiert und befallene Programme befreien kann, ist vorhanden.

Brain-Viren haben ihren Namen durch die Meldung "(C) Brain" erhalten, die bei der Ausführung ausgegeben wird. Die erste Generation wurde 1986 von den Brüdern Basit Farooq Alvi und Amjad Alvi in Lahore, Pakistan als Jux kreiert. Wie dieser Virus in die Vereinigten Staaten gelangte und dort an der George Washington University, der University of Delaware sowie der University of Pittsburgh auftauchte, ist unbekannt.

Dieser Virus befällt Teile des Betriebssystems und installiert sich zur Weiterverbreitung als residente DOS-Extension im Speicher. Als Transportmittel dienen hier also nur bootfähige Disketten. Dieser Virus verursachte keine bekannten Schäden an irgendwelchen Daten, sondern begnügte sich mit der Aufforderung, 100.000.-- Dollar an ein angegebenes Konto zu überweisen. Dadurch war es einfach, die Urheber des Virus' zu ermitteln, die in der Überzeugung handelten, der Virus könne nie den eigenen Campus verlassen.

Sind die Auswirkungen auch kein Anlaß, von einer direkten Bedrohung zu sprechen, so kann man doch an diesem Beispiel deutlich die schnelle und weite Verbreitung solcher Programme erkennen.

Das **Entfernen des Virus** ist recht einfach: Man schaltet den Rechner aus, um die im Speicher eingenistete Weiterverbreitungsroutine zu löschen und bootet dann von einer garantiert sauberen DOS-Diskette (das Orginal sollte jeder haben und mit einem SCHREIBSCHUTZKLEBER versehen!).

Im nächsten Schritt formatiert man eine Diskette in Laufwerk B: mit der Option "/S", um das uninfizierte System, das sich auf A: befindet, auf die Diskette in B: zu kopieren.

Danach löscht man auf der befallenen Diskette das vermutlich infizierte Systemfile COMMAND.COM.

Als letzter Schritt kopiert man alle Dateien der infizierten Diskette auf die neue, z.B. mit Hilfe des Befehles COPY A:*.* B:. Bei neueren DOS-Versionen können mittels XCOPY A:*.* B: /S auch Subdirectories mitkopiert werden. Die alte Diskette kann man danach mit FORMAT B: /S endgültig reinigen. In entsprechender Weise verfährt man mit der Harddisk, mit dem Unterschied, daß hier der Inhalt nicht auf eine Diskette paßt. An dieser Stelle kommt dann das Programm BACKUP oder ähnliche Software zusätzlich zum Einsatz.

Ein in letzter Zeit wieder aufgetauchter Virus ist der **Israel- oder Jerusalem-Virus**. Er wurde zum ersten Mal in Israel entdeckt. Es halten sich Gerüchte, daß dieser Virus von arabischen Extremisten als "High-Tech-Waffe" erdacht wurde, da er erstmals am 40. Jahrestag der Gründung des Staates Israel in Aktion treten sollte.

Dieser Virus befällt COM- und EXE-Dateien, ein Fehler im Weiterverbreitungsalgorithmus führte jedoch glücklicherweise zur vorzeitigen Entdeckung und Beseitigung. Da eine Mehrfachinfektion von EXE-Dateien nicht unterbunden wurde, löste dieser "Fehler" ein ständiges Wachstum vielbenutzter Programme aus und alarmierte dadurch die israelischen Spezialisten.

Das zerstörerische Werk des Israel-Virus beginnt immer an Freitagen, die auf den 13. fallen. Programmdateien werden dann direkt nach ihrer Aktivierung gelöscht.

Da ein Anwender zunächst an einen Bedienfehler denkt, wird er es zunächst mit anderen Programmen versuchen, die dann ebenfalls von der Festplatte verschwunden sind. Unbestätigte Meldungen sprechen sogar von Abarten, die eine Low-Level-Formatierung der Festplatte auslösen. Dies kann allerdings aus technischen Gründen nur auf XTs bzw. bei ATs mit speziellen Controllern passieren.

Um diesen Virus aufzuspüren, existieren inzwischen Anti-Virus-Programme, die recht zuverlässig arbeiten. Es sei aber noch einmal darauf hingewiesen, daß die Viren schneller mutieren, als irgendwelche Gegenmaßnahmen getroffen werden können. Deswegen wird es auch nie eine 100%-ige Bekämpfung geben können.

Obige Beispiele machen deutlich, mit welcher Geschwindigkeit sich Viren verbreiten und wie vielfältig sich die Auswirkungen solcher Programme präsentieren. Es bleibt zu befürchten, daß weiterhin Hacker und Computer-Frusties sich einen Spaß daraus machen, Ihnen zu schaden. Die Virusprogramme werden dabei immer raffinierter und sind nur noch sehr schwer aufzuspüren. Wohl dem, der dann nur einen rasenden Ping-Pong-Ball über den Bildschirm huschen sieht, dessen Datenbestände aber unangetastet bleiben.

Wichtige Verhaltensmaßnahmen vor dem Virusbefall:

Sicherungskopien

Glücklicherweise erlauben inzwischen die meisten Software-Hersteller eine Sicherungskopie ihrer Programme, so daß Sie sich auf rechtlich einwandfreiem Boden bewegen, wenn Sie ein Backup Ihrer Disketten anfertigen. Und genau das sollten Sie mit jeder neuen Software tun.

Versehen Sie zunächst das Original mit einem Schreibschutz-Kleber, erstellen Sie eine Sicherungskopie (z.B mit Hilfe des DOS-Befehles DISKCOPY) und verwahren Sie dann die Originaldisketten an einem sicheren Ort; gearbeitet wird ausschließlich mit der Kopie.

Zugriffsschutz

Können Sie nicht sicherstellen, daß nur befugte Anwender Zugang zu Ihrem Rechner bekommen, so versehen Sie diesen mit einem Hardwareschutz. Bei Neuanschaffungen kann dies bereits in der Gerätekonfiguration berücksichtigt werden, aber auch vorhandene Geräte (einschließlich PCs und XTs) lassen sich in solcher Weise modifizieren.

Eine weitere Möglichkeit besteht in einem Software-Password, das die Festplatte gegen unbefugte Zugriffe schützt, unabhängig davon, mit welchem System gebootet wurde. Solche Programme sind im Fachhandel erhältlich.

Präventiver Virusschutz

Je mehr Leute an Ihrem Rechner arbeiten, umso größer ist die Gefahr, daß mit unbekannten Programmen auch Viren in das System eingeschleppt werden (z.B. durch Spiele). Scheuen Sie nicht die Mühe, in regelmäßigen Abständen alle ausführbaren Programme zu überspielen (von Ihren virusfreien und hoffentlich schreibgeschützten Originaldisketten). Es kann auch hilfreich sein, von Zeit zu Zeit ein Backup von der Platte zu erstellen, und diese vor einem erneuten Überspielen zu formatieren.

Diese drei einfachen Maßnahmen können helfen, einen Virusbefall einzudämmen oder sogar zu verhindern.

In jedem Fall gilt:

Vorsorgen ist besser als Löschen!

Computerviren - Teil II

21. September 1993: Ein Mitarbeiter der Metallwarenfabrik Meyer & Co KG *) bringt eine Diskette mit einem neuen Spiel in sein Büro und präsentiert es stolz seinen Kollegen auf seinem Arbeits-PC.

Was dieser Mitarbeiter nicht weiß, ist die Tatsache, daß das Programm mit einem Virus verseucht wurde und nun drauf und dran ist, über das lokale Netzwerk alle weiteren Firmenrechner zu befallen.

Fünf Tage später geschieht das Ungeheuerliche: Alle Festplatten löschen sich wie von selbst. Zunächst fallen alle computergesteuerten Produktionsmaschinen aus, denen die nötigen Steuerinformationen fehlen. Kurz darauf bricht die Buchhaltung zusammen, da keine verwertbaren Daten mehr vorhanden sind. Ab diesem Zeitpunkt ruht das Unternehmen. Ob der Konkurs verhindert werden kann, hängt allein von den Rücklagen der Firma und dem Können der EDV-Spezialisten ab.

Dieser fiktive Alptraum scheint Ihnen wohl etwas zu weit hergeholt. Wie eine Studie jedoch belegt, ist die "Überlebenszeit" für ein Unternehmen bei Totalausfall aller DV-Anlagen höchst knapp bemessen. Sie beträgt für ca. 20% der Unternehmen nur einige Tage, für immerhin 5% sogar nur einige Stunden. Man denke z.B. an Großeinrichtungen der chemischen Industrie, die ohne Computer nicht mehr gesteuert werden können und dann unkontrollierte Prozesse erzeugen. Aus diesen Gründen ist es unbedingt erforderlich, selbst das geringste Infektionsrisiko durch Viren auszuschließen.

Wie erkennt man jedoch, ob sich ein Virus auf einem Rechner eingeschlichen hat ? Was kann man tun, wenn es tatsächlich zu einer Infektion gekommen ist ?

Zunächst müssen wir darauf hinweisen, daß es keinen 100%-igen Erkennungsmechanismus für Viren gibt. Anti-Virus-Programme können zwar bekannte Typen detektieren, aber im ewigen Kampf zwischen Virusprogrammierer und -bekämpfer werden wohl immer neuere und raffiniertere Arten entwickelt werden.

Also ist an dieser Stelle in höchstem Maße Ihre Beobachtungsgabe gefordert: seien Sie wachsam gegenüber jeglichen Veränderungen in Ihrem System. Ein sonderbares Verhalten eines Rechners kann das erste Symptom für einen Befall sein.

Um solche Vorgänge erkennen und beurteilen zu können, ist ein Wissen über grundlegende Arbeitsweisen und Verbreitungsmechanismen von Viren erforderlich. Deswegen nun eine

*) Name, Handlung und Zeit dieser Fiktion sind frei erfunden. Jede Ähnlichkeit mit existierenden Unternehmen wäre rein zufällig.

kleine Exkursion in die EDV-technische Welt.

Als Übertragungsmedium von Viren dienen entweder ausführbare Programme jedweder Art oder Teile des Betriebssystems. Dabei unterscheidet man zwischen **File-Viren** - diese werden nur über Programme weitergegeben - und **Boot-Viren** - deren Code wird bereits beim Start des Betriebssystems geladen und nistet sich im Speicher ein.

File-Viren

Beim Start eines infizierten Programmes wird zunächst der Viruscode aktiviert. Dieser prüft nach, ob sich der Viruscode schon im Hauptspeicher eingenistet hat. Ist dies nicht der Fall, so installiert der Virus eine Kopie seines ausführbaren Codes als residente Erweiterung des Betriebssystems (TSR). Ab diesem Zeitpunkt ist der Reproduktionsmechanismus in Ihrem System aktiviert. Je nach Art des Virus versucht er zu den unterschiedlichsten Zeitpunkten, eine Kopie von sich selbst an ausführbare Programme anzuhängen.

Damit ist der Teufelskreis geschlossen. Bei Weitergabe eines dieser infizierten Programme per Datenträger oder Kommunikationseinrichtung wird ein weiteres System befallen. Das Heimtückische an diesen Vorgängen ist die Tatsache, daß sich die Aktivitäten der Viren nicht nur auf die Weiterverbreitung beschränken, sondern auch anderen groben Unfug mit Ihrem Rechner oder Ihren Daten treiben.

Bei Veränderung einer Datei, z.B. bei Textverarbeitung oder beim Einfügen eines Datensatzes in eine Datenbank, ändern sich in der Regel auch Dateigröße und -datum (Last Access Time, LAT). Dies gilt ebenso für ausführbare Programme (.COM und .EXE Dateien). Hängt sich ein Virus an ein Programm an, so kann man anhand dieser beiden Kenndaten zumindest erkennen, daß an dem Programmcode vermutlich manipuliert wurde. Ein regelmäßiger Vergleich mit dem Original der Datei ist also auf jeden Fall lohnenswert.

Diese sehr einfache Methode kann jedoch nur als Bestätigung eines Virenverdachtes dienen und sollte zu einer eingehenderen Prüfung der Daten veranlassen.

Achtung! *Es existieren einige Programme, die sich selbst modifizieren. Ein geändertes Dateidatum ist deshalb noch kein Grund zur Panik.*

Das gleiche gilt für Programme, an denen noch entwickelt wird. Andererseits existieren Virus-Versionen, die sich an Programme anhängen, ohne Größe und Datum zu ändern.

Über deren Mechanismen möchten wir hier nicht detaillierter berichten, da für solche Viren einiges Know-How erforderlich ist; und dieses möchten wir im Micro-BIT Journal nicht vermitteln.

Boot-Viren

Der Start eines Systems geht in mehreren Schritten vor sich. Einer davon ist das Laden des Bootstrap-Sektors auf der Diskette oder auf der Festplatte. Dies ist eine fest definierte Stelle auf dem Datenträger, die Information über den weiteren Startvorgang enthält, z.B. Dateinamen der Betriebssystemprogramme.

Ein Virus, der sich hier einnistet, wird schon beim Booten als TSR in den Hauptspeicher geladen und beginnt dann sein unheilvolles Wirken. Die Verbreitung erfolgt über das Betriebssystem, d.h. beim Übertragen des Systems auf einen neuen Datenträger wird der Virus automatisch mitkopiert.

Auch hier ist die Beobachtungsgabe des Anwenders ein wichtiges Erkennungsmittel, jedes außergewöhnliche Verhalten des Rechners sollte ein erstes Alarmzeichen sein.

Unabhängig von Typ und Arbeitsweise eines Virus weisen alle eine Gemeinsamkeit auf: sie verändern Teile von Programmen oder des Betriebssystems. Der Viruscode muß irgendwo auf einem Datenträger permanent gespeichert sein, um auch nach dem Ausschalten des Rechners überleben zu können.

An dieser Stelle greifen nun die Detektionsmechanismen, die auch in dem Anti-Virus-Programm von Micro-BIT zum Einsatz kommen. Dabei kann man primär zwei Klassen der Erkennung unterscheiden.

Bekannte Viren erlauben die Suche nach charakteristischen Fragmenten, z.B. Zeichenketten oder Bruchstücke des Virencodes in Dateien, im Betriebssystem oder im Hauptspeicher. Dies ist jedoch nur möglich, wenn der Virus zuvor analysiert wurde.

Die zweite Klasse beinhaltet solche Verfahren, die global nach Änderungen im System

suchen und durch einen Vergleich mit einem früheren Zustand auf einen möglichen Virenbefall hinweisen.

Einige dieser Verfahren möchten wir nun vorstellen, anhand derer Maßnahmen zur Virenerkennung möglich sind. Die Realisierung kann z.B. mit Hilfe eines Turbo-Pascal Programmes oder z.T. auch schon mit Befehlen des Betriebssystems erfolgen.

Maßnahmen zur Erkennung eines Virenbefalls

- Regelmäßige Kontrolle von Dateigröße und Datum.
- Byteweiser Vergleich von Programmdateien.
- Generierung und Test von CRC-Prüfsummen.
- Vergleich von FAT und Inhaltsverzeichnis.
- Suche nach spezifischen Symptomen bekannter Viren.
- Untersuchung speicherresidenter Programme.
- Kontrolle von Schreibaktivitäten auf Datenträger.
- Bad-Sektor-Logging.

Dateigröße und -datum im Inhaltsverzeichnis

Durch Vergleich dieser beiden Parameter lassen sich sehr einfach und schnell Veränderungen erkennen. Wie zuvor aber schon erläutert, ist diese Methode sehr unzulänglich und sollte nie als einziges Kriterium herangezogen werden. Zum Erstellen einer Referenzwertliste darf nur die Originalsoftware herangezogen werden, die an einem separaten Ort gesichert aufbewahrt werden sollte.

Das Resultat dieser Überprüfung ist kein sicheres Indiz für oder gegen einen Virus.

Dateivergleich

Eine Erkennung von Unterschieden in Programmdateien erlaubt der DOS-Befehl *"COMP"*. Hierbei werden Dateien byteweise verglichen und bei Abweichungen eine Meldung ausgegeben. Dazu sind Referenzdateien erforderlich. Werden diese auf der Platte aufbewahrt, erfordert das viel Speicherplatz und es besteht die Gefahr, daß auch die Referenzdateien infiziert werden. Letzteres Problem kann man umgehen, indem man die Referenzdatei zuvor umbenennt (nicht mehr die Extension .COM, .EXE oder .SYS). Noch sicherer ist die Verwendung einer virusfreien Originaldiskette für den Vergleich.

Eine weitere Möglichkeit besteht in der Verwendung von gepackten (komprimierten) Referenzdateien. Zum einen reduziert sich erheblich der Platzbedarf, zum anderen steigt der Aufwand, der zur Implantierung eines Virus in eine gepackte Datei erforderlich wäre, übermäßig an.

Das Resultat dieser Überprüfung kann ein Indiz für einen Virus sein.

CRC-Check

Nachteilig wirkt sich beim Dateivergleich der hohe Speicherplatzbedarf für die Referenzdateien aus. Deshalb wurden Verfahren entwickelt, die wesentlich sparsamer mit diesen Ressourcen umgehen. So wird z.B. beim CRC-Verfahren über eine Programmdatei mit Hilfe eines binären, höhergradigen Polynoms eine Prüfsumme gebildet, die als Vergleichswert dient. Zum Erstellen einer Referenzwertliste darf nur die Originalsoftware herangezogen werden. Dieses Verfahren ist nur bei solchen Programmen sinnvoll, die sich nicht (mehr) selbst modifizieren (also erst nach einer Konfiguration).

Das Resultat dieser Überprüfung ist in der Regel ein hochgradiges Indiz für einen Virus.

Vergleich von Inhaltsverzeichnis und File Allocation Table

Neben dem Inhaltsverzeichnis existiert auf Speichermedien von MS-DOS-Systemen eine weitere Parametertabelle, die File Allocation Table (FAT). Mit Hilfe des DOS-Befehles "CHKDSK" (check disk) wird ein Vergleich zwischen dieser FAT und den Inhaltsverzeichnissen eines Datenträgers durchgeführt. Auftretende Abweichungen können auf einen Virus hinweisen, oft entstehen solche Unterschiede aber auch bei der Entwicklung

eigener Programme, die das Dateisystem verwenden und unzuverlässige Operationen ausführen.

Das Resultat dieser Prüfung ist kein sicheres Indiz für oder gegen einen Virus.

Suche nach spezifischen Symptomen bekannter Viren

Die Suche nach bekannten Viren gestaltet sich etwas einfacher, da man hier spezielle Muster aufspüren kann. Dafür kommen z.B. Zeichenketten (Identifikationsstrings) oder Viruscode-Fragmente in Frage. Jedoch lassen sich solche Merkmale leicht ändern, so daß man mit diesem Verfahren dem aktuellen Stand wohl immer etwas hinterherhinkt.

Zum Test werden einzelne Programmdateien, Betriebssystemdateien, Volumelabel und Bootsektoren herangezogen. Sinnvoll ist auch eine physikalische Überprüfung des Datenträgers, unabhängig von den logischen Strukturen.

Das Resultat dieser Überprüfung dient in den meisten Fällen als Indiz für einen Befall des Systems mit einem bekannten Virus.

Untersuchung von speicherresidenten Programmen

Die meisten Viren hängen sich als speicherresidente Ergänzungen in den Systemspeicher. Von da aus überwachen sie Vorgänge im Betriebssystem und greifen unter gewissen Umständen - je nach Programmierung - ein und führen ihre unheilvollen Manipulationen durch.

Aus solchen Gründen ist es sinnvoll, in regelmäßigen Abständen zu prüfen, welche speicherresidente Routinen aktiv sind. Erscheinen dabei plötzlich unbekannte Programme, so ist das ein untrügliches Alarmzeichen.

Beispiele für sinnvolle speicherresidente Erweiterungen sind etwa VDISK (RAM-Disk), DOSEDIT (komfortable Befehlseingabe im Betriebssystem), SIDEKICK (allg. Utilities) oder Hardcopy-Programme für die Graphikausgabe.

Das Resultat dieser Überprüfung dient in vielen Fällen als Indiz für einen Virusbefall.

Überwachen der Schreibaktivitäten auf Datenträger

Ein Virus kann sich nur weiterverbreiten, indem er auf Datenträger zugreift und eine Kopie seines Codes darauf schreibt. Deshalb empfehlen einige Fachleute, sämtliche Schreibvorgänge durch eine speicherresidente Routine zu überwachen und jeweils zuvor die Genehmigung des Benutzers zum Schreiben einzuholen.

Die meisten Anwender dürften aber überfordert sein, zwischen dem Schreibzugriff eines Virus und dem eines normalen Programmes zu unterscheiden. Deshalb können wir nicht zu dieser Methode raten, sie wurde jedoch zur Vervollständigung aufgeführt.

Das Resultat dieser Überprüfung dient nicht als Indiz für oder gegen einen Virus.

Bad-Sektor-Logging

Manche Viren nisten sich auf Datenträgern nicht als Programmerweiterungen im logischen Dateisystem ein, sondern setzen sich an einer ausgewählten physikalischen Stelle des Speichermediums fest. Solche Positionen werden dann als sogenannte "Bad-Blocks" (fehlerhafte Sektoren) gekennzeichnet und stehen danach dem Betriebssystem nicht mehr zur Verfügung. Deshalb empfiehlt sich eine regelmäßige Überwachung der Bad-Blocks, z.B. mit Hilfe des Programmes DISKTEST (Norton-Utilities).

Das Resultat dieser Überprüfung dient nicht als Indiz für einen Virusbefall, sollte jedoch zu weiteren Untersuchungen Anlaß geben.

Durch Anwendung mehrerer der zuvor genannten Verfahren sollte es möglich sein, einen Virus relativ zuverlässig zu erkennen. In einigen Fällen ergibt sich nur die Tatsache eines Virenbefalls, in anderen Fällen erhält

man den genauen Virustyp.

Als nächster Schritt erfolgt nun die Beseitigung des Virus aus dem System. Auch hier bieten sich unterschiedliche Verfahren an, die je nach aktuellen Gegebenheiten angewendet werden können.

Maßnahmen zur Beseitigung von Viren

- Restauration des ursprünglichen Zustandes mittels Backups.
- Entfernen des Virencodes aus dem infizierten Programm.
- Überschreiben des schädlichen Viruscodes.

Beseitigung von Viren mittels Backup

Wurde die Infektionsquelle zuvor genau lokalisiert, so kann mit einer nicht infizierten Sicherungskopie der originale Zustand wieder hergestellt werden. Dies setzt voraus, daß sorgfältig mit den Originalen verfahren wird und daß diese ständig virenfrei gehalten werden.

Um Boot-Viren sicher beseitigen zu können, ist das Formatieren des Datenträgers erforderlich. Auch hier ist ein virenfreies Original unabdingbar.

Die Archivierung der Originalsoftware ist jedoch nicht ganz unproblematisch. Aktuelle Änderungen der Konfiguration und andere Daten müssen in der Regel ebenfalls gesichert werden. An dieser Stelle besteht die große Gefahr, daß sich ein Virus in die archivierten Programme einschleicht. Aus diesen Gründen sollte auch die Software des Backups unbedingt auf Viren hin getestet werden.

Das Risiko kann man noch geringer halten, indem man sogenannte "Generationen-Backups" anlegt, d.h. in regelmäßigen Abständen eine Sicherungskopie erstellt und für eine gewisse Anzahl von Generationen archiviert.

Entfernen von Virencode aus infizierten Programmen

Die Beseitigung des Viruscodes aus einer Programmdatei gestaltet sich als äußerst schwierig, da je nach dessen Arbeitsweise unterschiedliche Ansatzpunkte gefunden werden müssen. Oft wird es erforderlich, den Programmcode zu disassemblieren und zu untersuchen, an welcher Stelle sich der Virus in das Programm eingebunden hat. Dies ist eine Aufgabe für Spezialisten, an die sich nur Anwender mit sehr viel Erfahrung heranwagen sollten. Ist der Virustyp jedoch bereits bekannt und analysiert, dann kann diese Methode automatisiert werden.

Überschreiben des destruktiven Viruscodes bzw. des Reproduktionsmechanismus

Alternativ zum Entfernen des Viruscodes kann man auch versuchen, den Weiterverbreitungsmechanismus und die destruktiven Codeteile zu überschreiben und damit unschädlich zu machen. Das erspart die Suche nach der Einsprungstelle, an der sich der Virus in das Programm eingehängt hat. Aber auch hier gilt: dies ist eine Arbeit, die nur von Spezialisten ausgeführt werden sollte. Die Gefahr, gesunde Programmteile zu überschreiben, darf nicht übersehen werden.

Die oben angeführten Verfahren machen deutlich, daß es wesentlich mehr Ansatzpunkte zum Erkennen eines Virus gibt als zu dessen Beseitigung. Deswegen sollte man bereits der Prävention und der Detektion höchste Aufmerksamkeit schenken.

Nicht minder wichtig ist aber der Schutz vor einer Reinfektion. Wurde ein Virus aus einem System entfernt, so besteht immer noch die Gefahr, daß Benutzer mit ihrer ebenfalls verseuchten Diskette den Virus erneut in das System einschleusen. Deshalb sind nach Abschluß der Reinigungsaktivitäten noch einige Punkte zu beachten, die sich z.T. wieder mit den präventiven Schutzmaßnahmen überdecken. Sie wenden sich sowohl an den Benutzer als auch an Systemprogrammierer bzw. Betriebssystemarchitekten.

Maßnahmen zum Schutz vor erneutem Virenbefall

- Sämtliche Verfahren zur Detektion eines Virus.
- Dummy-Viren in Programmen.
- Modifizierte Betriebssysteme.
- Killer-Virus. Wird von Micro-BIT strikt abgelehnt!
- Disk-Washing für Benutzerdisketten.

Einsatz von Dummy-Viren

Viele Viren überprüfen vor der Infektion eines Programmes ob dieses bereits verseucht ist. Durch die "Vorspiegelung falscher Tatsachen" wird der Reproduktionsmechanismus des Virus dann quasi überlistet.

Modifikation des Lademoduls des Betriebssystems

Durch Integration von Anti-Virus-Routinen in das Betriebssystem erfolgt eine Überprüfung von Programmen vor deren Ausführung.

Killer-Virus

Einige clevere Virusbekämpfer sind darauf verfallen, den Virus mit einem Gegenvirus zu bekämpfen. Dies bedeutet jedoch, den Teufel mit dem Beelzebub auszutreiben. Das Micro-BIT lehnt solche Methoden strikt ab!

Disk-Washing

Enthält ein System einen Virus, so kann man davon ausgehen, daß dieser sich auch auf Disketten von Mitarbeitern festgesetzt hat. Deshalb sind nach einer Reinigungsaktion unbedingt alle verwendeten Disketten zu überprüfen bzw. neu zu formatieren. Einige Rechenzentren gehen sogar soweit, daß generell sämtliche Benutzerdisketten geprüft werden und nur solche ohne ausführbare Programme und ohne Betriebssystem zugelassen sind.

Das durch diesen Artikel vermittelte grundlegende Wissen bezüglich Viren, deren Arbeitsweise und Bekämpfung sollte es ermöglichen, einfache Schutz- und Gegenmaßnahmen selbst zu ergreifen.

Darüber hinaus steht das Micro-BIT jederzeit für Nachfragen und Hilfe zur Verfügung. Wir werden auch in Zukunft die aktuellen Entwicklungen beobachten und an dieser Stelle gegebenenfalls berichten. Die bisher gesammelte Erfahrung wird auch in unsere Anti-Virus-Software einfließen, die wir nach Abschluß der Implementierungsarbeiten uniweit zur Verfügung stellen.

Nachtrag:

Eine Liste mit bisher auf IBM- und kompatiblen Rechnern bekannten trojanischen Pferden ist auch bei der hiesigen Anwenderberatung im RZ, Gebäude 36.1, einsehbar.

Dort liegt auch eine Liste mit Anti-Virus-Software für verschiedene PC-Typen bereit (Amiga, Atari, Apple II, Macintosh, IBM-Geräte). Mittlerweile gibt es auf allen gängigen PC-Typen unterschiedliche Viren, die z.T. die auf einem bestimmten Rechnertyp anfälligen Teile gezielt infizieren.

Weitere Informationen zum Thema sind neben dem Micro-BIT in Karlsruhe bzw. dem VTC in Hamburg auch auf elektronischem Weg aus der INFO-BOX der Gesellschaft für Informatik erhältlich. Aus dieser INFO-Box kann ein Katalog der im VTC Hamburg untersuchten Viren, ergänzt durch einen entsprechenden Anti-Virus-Katalog, bezogen werden. Ziel dieses Dienstes ist es, ein qualitativ gehaltvolles international verfügbares Brett für Virus-Information und Virus-Warnungen einzurichten.

Um über die Vorgänge zum Thema Viren auf unserem Campus auf dem Laufenden zu bleiben, bittet das RZ die Anwender, uns akute Virenvorkommnisse mitzuteilen. Bitte

bringen Sie bei einem konkreten Virusbefall eine Diskette mit dem vermutlich befallenen Programm/Betriebssystem im RZ vorbei oder wenden Sie sich direkt ans Micro-BIT unter nebenstehender Adresse.

Micro-BIT ***Tel. 0721-***
Universität Karlsruhe ***608-2997***
Zirkel 2, Postfach 6980
7500 Karlsruhe

Technisch-wissenschaftliche Anwendersoftware für BS2000

Das RZ erwägt im Rahmen der verfügbaren-Mittel die Anschaffung neuer BS2000-Anwendungssoftware für den technisch-wissenschaftlichen Bereich. Beispielsweise könnten bei entsprechendem Interesse die folgenden Programmbibliotheken bzw. Programmsysteme beschafft werden:

NAG:

Numerical Algorithms Group Library - eine sehr umfangreiche Unterprogrammsammlung für Mathematik und Statistik.

FIDAP:

Fluid Dynamics Analysis Package - ein Programmpaket zur Anwendung der Finite-Element-Methode auf die Analyse strömungsdynamischer Vorgänge.

FFTPACK:

Fast Fourier Transformation Package - ein System zur Lösung von Fourier-Transformationen.

LINPACK:

Umfangreiche Programmsammlung zur Analyse und Lösung linearer Gleichungssysteme und linearer Least-Squares-Probleme.

IMLS:

MATH/LIBRARY

STAT/LIBRARY

SFUN/LIBRARY

Programmsammlungen für Mathematik, Statistik und spezielle Funktionen.

Bei diesen aufgeführten Bibliotheken handelt es sich um Beispielangaben. Bei entsprechendem Interesse kann auch andere Software beschafft werden.

Voraussichtlich ab Mitte nächsten Jahres werden zwei neue zentrale UNIX-Rechner zur Verfügung stehen. Auch für diese soll entsprechende Anwendersoftware beschafft werden.

Um die Wünsche der Anwender besser einschätzen zu können, bittet das RZ alle interessierten Anwender, die von ihnen gewünschte Software zu spezifizieren und dem RZ mitzuteilen. Bitte benutzen Sie für Ihre Rückmeldung das Formblatt auf der Rückseite.

Name: .....

Institut/Fachrichtung: .....

Tel: .....

Ich bin an der Anschaffung folgender Software interessiert:

.....
.....
.....
.....
.....
.....
.....
.....
.....

Ich benötige die Software, um folgende Aufgaben/Projekte zu realisieren:

.....
.....
.....
.....
.....
.....
.....

Die von mir benötigte Software soll ablauffähig sein a) unter BS2000: .....

b) unter UNIX: .....