MICROSOFT: KEIN GRUND ZUR KLAGE

DAS UNABHÄNGIGE MACINTOSH~MAGAZIN

MAC up

MIDI: Mac macht Musik

HyperCard 1.2: ROYAL FLUSH!

Infektionsgefahr: AUF ALLEN VIREN!

4. JAHRGANG
AUSGABE 7
JULI 1988
5 MARK
5 FRANKEN
45 SCHILLINGE

IN 80 TAGEN UM DIE WELT

VON BENJAMIN HEIDERSBERGER

Mit dem Auftauchen von Virusprogrammen hat ein neues Kapitel der Computerei begonnen. Und wieder stellt sich die alte Frage, ob der Mensch tun darf, was er tun kann. Was Viren so gefährlich macht, ist ihre Selbständigkeit, die Fähigkeit, sich der menschlichen Kontrolle zu entziehen. Und schon werden die digitalen Erreger öffentlichen Ärgernisses mit der Gentechnik und deren Gefahren in Verbindung gebracht. ***Computerviren sind eine vollkommen neue Gattung von Programmen.*** Sie haben Eigenschaften, die man vorher nicht kannte, und bergen gänzlich neue Möglichkeiten und Chancen. Ein Virus hat die Fähigkeit, sich zu reproduzieren. Das Programm hängt Kopien seiner selbst an Wirtsprogramme, und zwar derart, daß bei deren Aufruf weitere Programme infiziert werden.

Virusprogramme bestehen aus drei Teilen:

- Eine Kennung sorgt dafür, daß infizierte Programme und das Virus selbst nicht noch einmal infiziert werden. Das erhöht erheblich die Effektivität.
- Ein Reproduktionsmechanismus findet nicht infizierte Programme und bindet sich an sie.
- Ein Funktionsteil löst beliebige Aktionen auf Computern aus. Der gestalterischen Freiheit sind keine Grenzen gesetzt.

Viren können sehr klein sein. Die theoretische Minimalgrenze liegt bei einigen 10 Byte. Dabei sind in Assembler geschriebene Programme am effektivsten, da sie in direkt ausführbarem Maschinencode vorliegen. Neben Viren, die nur auf dem Speichermedium herumlungern, gibt es auch solche, die sich nach dem Aufruf speicherresident installieren, um von hier aus Programme zu infizieren. Das Übergreifen eines Virus auf

einen anderen Computertyp ist zwar nicht ausgeschlossen, aber relativ unwahrscheinlich, da es dort auf einen anderen Prozessor, ein anderes Betriebssystem und eine andere Systemarchitektur stößt.

Viren wären halb so schlimm, wenn sie sich lediglich fortpflanzen würden. Sie wären nur lästig, weil sie Rechenzeit und Speicherplatz brauchen und somit die Performance eines Systems verschlechtern.

Was sie gefährlich macht, ist ihr Funktionsteil, der beliebige Befehle tragen kann. Alles ist möglich: von der Verbreitung von Botschaften und Witzeleien bis hin zur Zerstörung und Veränderung von Daten und Programmen. Dabei ist das unbemerkte Verändern von Daten ein besonderes Problem. Dem könnten Softwarehersteller durch Einführen von Prüfsummen Einhalt gebieten.

Doch nicht allein die Software ist gefährdet. Viren können ebenso Hardware zerstören. Beliebtes Opfer sind große Monitore, deren Bild- und Zeilenfrequenzen durch Registerinhalte programmiert sind. Bei entsprechender Veränderung wird der Zeilentrafo zerstört. Der alte Mac zumindest bietet hier keine Eingriffsmöglichkeit, weil die Zeilenfrequenz direkt durch die Hardware erzeugt wird.

Bei Disketten- und Festplattenlaufwerken sind klassische Angriffsvarianten das Anfahren nicht existenter Spuren oder unzulässige Veränderungen der Drehzahl, was im allgemeinen jedoch keinen Schaden hinterläßt.

Unangenehm hingegen ist die Zerstörung von Kontrollspuren auf Festplatten. Die kann nur der Hersteller reparieren. Besonders anfällig sind SCSI-Platten, da hier auf einer besonderen Spur Teile des plattenin-

WOLFGANG NOWACKI

ternen Betriebssystems und andere Informationen lagern, die dem Benutzer nicht zugänglich sind.

Viren können größere Schäden verursachen, wenn der befallene Computer der Produktions- und Ablaufsteuerung dient. Hier ist alles denkbar: vom Fließbandstillstand über abstürzende Raketen bis zu explodierenden Kernkraftwerken.

Hardware- und Softwarehersteller, Programmierer und Anwender: sie alle haben ihr ganz spezielles Verhältnis zu der neuen Mac-Seuche.

Apple als Hardwarehersteller bringen die Viren nur Scherereien. Sie stellen die Zuverlässigkeit des Systems in Frage. Deshalb hat Apple Cupertino einerseits rechtliche Schritte gegen die Verantwortlichen angekündigt, andererseits eine Einsatzgruppe gegründet, die eilends ein Antivirusprogramm namens „Virus RX" fertigstellte.

Gerade in Zeiten, in denen sich der Mac, nach anfänglichen Schwierigkeiten, im Busineßbereich immer größerer Akzeptanz erfreut und niemand mehr den Spielzeugcharakter des Rechenwürfels bemängelt, ist man für Rückschläge besonders empfindlich. Es sei nur daran erinnert, daß vor noch gar nicht so langer Zeit die Kugel mit der Zündschnur ein gewohntes Icon auf dem Desktop war und sich der Mac-User durch eine gewisse Gelassenheit auszeichnete, die bisweilen auch in eine Bomben-Stimmung umschlagen konnte.

Die Ansichten der Softwarehersteller sind schwieriger zu durchschauen. Solange es um die Zuverlässigkeit ihrer Programme geht, ist ihre ablehnende Haltung klar. Der Softwarehersteller hat genug damit zu tun, seine eigenen Programme stabil zu machen und den sich ständig ändernden Umgebungen anzupassen; sei es nun, daß sich die Änderungen durch das Betriebssystem, die Hardware oder durch andere Programme ergeben.

Durch Viren entsteht aber auch ein neuer Softwaremarkt. Da die Benutzer vom tadellosen Funktionieren ihrer Maschinen abhängig sind, ist Virenbekämpfung ein sehr profitables Marktsegment – solange dieses gewisse Gefühl der Ohnmacht da ist. So sind sicher einige Entwickler versucht, mit der Angst der Leute Geld zu machen. Und da neue Viren immer mit neuen Programmen bekämpft werden müssen, hat dieser Markt Aussicht, lange Zeit bestehen zu bleiben. Witzig, daß Viren wahrscheinlich am besten durch Viren zu bekämpfen sind.

Ein anderes Kapitel der Softwareindustrie ist die Geschichte des Kopierschutzes. Mit allerlei Tricks wurde verhindert, Software mit Mitteln des Betriebssystems zu kopieren. Da das praktische Arbeiten so nicht möglich war, hat man den Kopierschutz fallengelassen, zugleich aber eine veränderte Kopiermoral zu schaffen versucht. Das gelang indes nur teilweise. So kommt es der Softwareindustrie sehr gelegen, daß allgemein in Umlauf befindliche und vor allem geknackte Software virenverseucht sein kann. Das wird auch entsprechend laut propagiert.

Problematisch wird's nur, wenn auch Originalsoftware verseucht ist – so geschehen mit Aldus' FreeHand. Was die Sache in diesem Fall noch delikater macht, ist der Umstand, daß offensichtlich eine dritte Firma mit Hilfe dieses Virus versehentlich in Umlauf geratene Software mit bestimmter Kennung zu vernichten suchte, das Virus aber aus der Kontrolle geriet.

Der Einsatz von Viren als Kopierschutz wurde in Erwägung gezogen. Hier ist aber die Grenze zur Illegalität deutlich überschritten.

Für den fortgeschrittenen Programmierer ist ein Virus das Größte, was er schaffen kann. Es ist die Ausgeburt seines Bestrebens, Schöpfer zu sein. Das Virus ist nämlich ein Programm mit Eigenschaften des Lebendigen. Der Faszination des simulierten Lebens und der Omnipotenz bei dem Gefühl, etwas geschaffen zu haben, das vielleicht den Weg um die Welt schafft, kann man sich nur schwer entziehen. Der gute Programmierer muß dem Wesen nach ein Hacker sein. Welche Botschaft er in das Virus legt, entspricht schlicht seinen Erfahrungen und seinem Charakter, sei es nun die Botschaft des Friedens oder die Vernichtung aller Daten.

Arm dran ist der Benutzer. Er wußte noch nie so recht, was er von den Vorgängen im Computer halten sollte. Seine Unsicherheit erlangte aber erst mit dem Auftauchen der Viren ihren traurigen Höhepunkt. Für jede Unregelmäßigkeit am Computer machen leidgeplagte Anwender jetzt ein Virus verantwortlich. Da somit eine Art Universalerklärung für alle Schwierigkeiten gefunden ist, erlangt das Phänomen des Virus eine unverhältnismäßige Publizität.

Wie groß die momentane Hilflosigkeit ist, kann man dem ernstgemeinten Vorschlag entnehmen, Programme im Source-Code Zeile für Zeile zu prüfen und dann zu kompilieren.

Die erste und wichtigste Maßnahme ist die Änderung der Kopiergewohnheiten. Überlegen Sie, welche Software Sie wirklich zum Arbeiten brauchen. Der Gewohnheit, allerlei verschiedene Programme auf die Platte zu kopieren, um sie gelegentlich einmal auszuprobieren, sollte man nicht länger frönen. Neue Software aus dunklen Quellen probiert man am besten nur auf Diskette aus, und die Platte klemmt man, wenn möglich, ab.

Die Softwarehersteller waren bisher bemüht, Programme ohne Viren zu verbreiten. Jedoch wird auch im Softwaremarkt inzwischen mit härteren Bandagen gekämpft. So stellt sich für manchen Anbieter die Frage, ob er weiterhin sauber bleiben soll, denn mit Viren lassen sich allerlei für die Konkurrenz unangenehme Dinge anstellen.

Infizierte Programme sind oft jene kleinen praktischen Utilities, die man von einem freundlichen Bekannten bekommt oder von Mailboxen herunterlädt. Vielleicht auch die Betaversion einer ganz neuen Software. Oder das geknackte oder wie auch immer kopierte Programm. Nützlich kann ein Vergleich der Größe der

Files sein, ebenso ein Test unter kontrollierten Bedingungen.

Beobachten Sie Ihren Rechner genau. Dauert es beim Starten immer länger? Greift der Rechner plötzlich mal auf die Platte zu? Verändert sich die Größe der Files? Mutiert ein Icon? Verändert sich das Datum der letzten Veränderung?

Beim Macintosh gibt es die Möglichkeit, Files als Read-Only zu markieren, indem man unter „Information" „geschützt" anklickt. Tun Sie das mit möglichst vielen Programmen. Da der Mac bei einigen Programmen bestimmte Informationen zurückschreiben muß, läßt sich auf diese Weise nicht alles schützen. Raffiniertere Viren werden natürlich die Betriebssystemroutinen umgehen.

Auf eine Virusinfektion sollte man vorbereitet sein. Wann haben Sie das letzte Backup gemacht? Nützlich ist ein getrenntes Backup der Dokumente, da diese nicht befallen werden, und ein Backup der Programme zu einem Zeitpunkt, an dem sie garantiert noch sauber sind. Bei einem generellen Backup läuft man Gefahr, schon infizierte Programme mit zurückzukopieren. Sinnvoll ist auch ein Backup in mehreren Generationen, da gegebenenfalls die Möglichkeit eines Rückgriffs auf eine nicht infizierte Generation besteht.

Taucht ein Virus auf, sollte man sofort die Platte und die Arbeitsdisketten formatieren, den Rechner ausschalten, um speicherresidente Viren zu löschen, und die Platte neu aufbauen. Der Anstand gebietet es, Leute zu informieren, denen man eventuell infizierte Programme gegeben hat. Und beten Sie, daß das Formatierungsprogramm nicht schon infiziert ist.

Größte Vorsicht erfordern Netzwerke, da jeder Rechner mit eigener Platte angreifbar ist und die Reinigung besonders unangenehm ist. Dazu sollte man jeden Rechner vom Netz trennen und jede Platte einzeln, wie oben beschrieben, formatieren. In Umgebungen mit Publikumsverkehr, etwa auf Messen, sollte man den Rechner in Arbeitspausen vor unbefugtem Zugriff durch Paßwortschutz schützen, und zwar nicht nur bestimmte Programme, sondern den ganzen Rechner.

Die meisten Antivirusprogramme wirken nur auf ein bestimmtes Virus. Der Kampf zwischen Virusprogrammierern und -bekämpfern wird sich entwickeln wie der zwischen Kopierschützern und Softwareknackern. Man sollte sich also nicht auf die Wirksamkeit solcher Programme verlassen. Abgesehen davon ist ein Antivirusprogramm die beste Gelegenheit, ein Virus zu verbreiten.

Inzwischen gibt es eine größere Anzahl von Programmen, die Viren bekämpfen sollen. Dabei ist eine Entwicklung zu beobachten von einfachen Programmen, die nur bestimmte Viren erkennen und beseitigen, hin zu Programmen, die eine allgemeine Kontrolle und Beobachtung aller Files gestatten, um im Ernstfall auf eine Infektion aufmerksam zu machen.

„AntiVirus" von Softhansa ist eines der ersten Programme. Es findet und beseitigt N-VIRUS, eines der ersten Viren, die in Deutschland auftauchten. Zugleich installiert AntiVirus einen Schutz gegen weiteren Befall.

„Vaccine" wird als Init-File in den Systemfolder kopiert und ist über das Kontrollfeld zu erreichen. Es zeigt während des Arbeitens an, wenn sich bestimmte Resourcen verändern, und fragt, ob das denn seine Richtigkeit hat.

„Virus RX" ist Apples erste Antwort auf die Viren. Beim Aufruf zeigt es alle beschädigten, unsichtbaren und veränderten Programme sowie die Init-, cdev- und RDEV-Files an. Das Ergebnis dieser Untersuchung schreibt Virus RX zum späteren Vergleich in ein File.

„Safer Mac", ein kommerziell vertriebenes Programm von Heyden & Son, registriert beim ersten Start alle Programme und Systemdateien. Bei Veränderungen erfolgt eine Warnung. In der Praxis kann das natürlich nervend sein, da ständig Veränderungen erfolgen.

„Virus Buster", das Michael Fuchs für den MACup Public Domain Club schrieb, registriert ebenfalls Veränderungen. Es ist etwas langsam, dafür aber sehr gründlich (siehe auch Seite 58).

„Ferret" bekämpft das Scores-Virus, das zu Systemabstürzen und Datenverlusten führt. Benannt wurde es nach dem File „Scores", das es im Systemordner hinterläßt. Ferret beseitigt es aus allen Files und spürt beschädigte Programme auf.

Seit es Viren gibt, denken Computermenschen auch über mögliche positive Anwendungen nach. Einer der ersten Gedanken war die Verbreitung von File-Kompressionsalgorithmen innerhalb des Rechners. Jedoch gibt es andere Methoden, die die Performance des Systems nicht so sehr beeinträchtigen. Andere Ideen gehen in Richtung selbständiger Softwareentwicklung durch selbstmodifizierende und -reproduzierende Strukturen. Hier ergeben sich aber auch besonders gefährliche Viren, die ihre Kennung und Arbeitsweise ändern.

Mit Computerviren werden Macianer leben müssen. Es geht vornehmlich darum, deren Verbreitung zu erschweren und die Auswirkungen zu begrenzen. Die Vireninvasion kommt besonders schnell voran, wenn die Anwender nicht darauf vorbereitet sind.

Gerade die Hersteller von Betriebssystemen sind aufgerufen, schon auf dieser Ebene entsprechende Software einzubauen. Die Möglichkeiten sind vielfältig, weil das Betriebssystem die Verwaltung des Systems übernimmt. Vorstellbar sind Programme, die genau die Aktivitäten des Rechners beobachten. Oder Prüfsummen, die beim Starten eines Programmes gecheckt werden. Das Zurückschreiben auf Programmfiles sollte nur unter bestimmten Bedingungen möglich sein. Der Mac ist durch die Offenheit seines Betriebssytems besonders gefährdet.

Es gibt – wie im richtigen Leben – keinen 100prozentigen Schutz vor Viren.