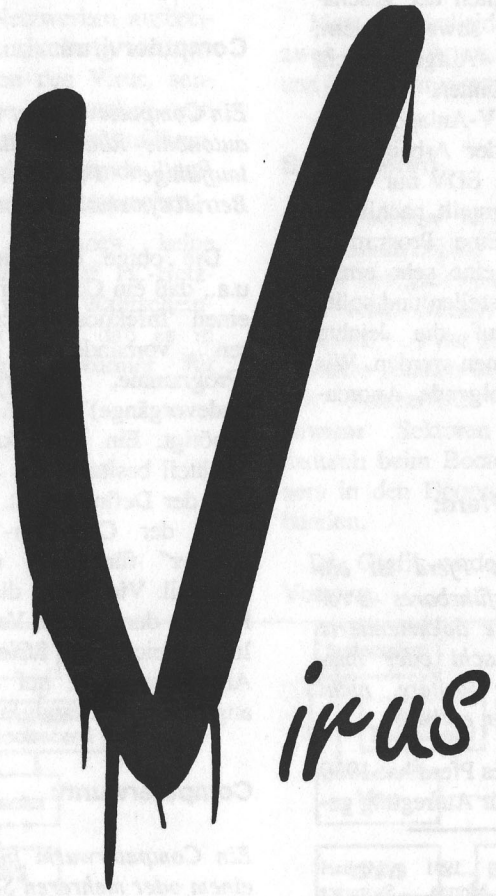
PC-Viren, Würmer und trojanische Pferde

Michael Reinschmiedt und Morton Swimmer



In jedem großen Programm
steckt ein kleines,
das sich nach oben kämpft.

[1]Programmanomalien stellen eine Gefahr für die elektronische Datenverarbeitung (EDV) dar. Programmanomalien können Datenbestände verändern oder löschen, sie können auch, meist aufgrund von Inkompatibilitäten mit den verwendeten Programmen, das Verhalten der geschädigten Rechner soweit ändern, daß diese Ihre Aufgabe nicht mehr erfüllen können. Fehlfunktionen in der EDV-Anlage bedeuten auch, daß der Arbeitskreislauf, in dem die EDV nur einen Arbeitsschritt darstellt, nachhaltig gestört wird. Eine Programmanomalie kann eine sehr ernsthafte Gefahr darstellen und sollte deshalb nie auf die leichte Schulter genommen werden. Wir unterscheiden folgende Anomalien:

Trojanisches Pferd:

Ein trojanisches Pferd ist ein autonomes, ausführbares Programm, daß eine dokumentierte Funktion vortäuscht oder ausführt aber eine weitere, nicht bekannte Funktion enthält.

Ein trojanisches Pferd hat 1989 in Deutschland für Aufregung gesorgt. Hier war eine zusätzliche Funktion, nämlich die Kodierung der Festplatte nach einer bestimmten Anzahl von Bootvorgängen, in einem Programm integriert worden, das Informationen über den HIV-Virus "AIDS" zu liefern.

Computervirus:

Ein Computervirus ist eine nichtautonome Routine, die sich an lauffähige Programme oder Betriebsysteme ankoppeln kann.

Die obige Definition besagt u.a., daß ein Computervirus zum einen "Infektiös" ist, zum anderen vorhandene Strukturen (Programme, Betriebsystem-Ladevorgänge) für seine Existenz benötigt. Ein Virus kann einen Wirkteil besitzen, der aber nicht Teil der Definition ist. Vielmehr dient der Computer-Virus als "Träger" für einen möglichen Wirkteil. Viren sind die Anomalien mit der größten Verbreitung. Im Bereich der PC's ist ihre Anzahl weltweit auf etwa 420 angewachsen (Stand: Jan 1991).

Computerwurm:

Ein Computerwurm besteht aus einem oder mehreren Segmenten, die entweder eigenständige Programme oder nicht-autonome Routinen sind und sich über Computernetze selbständig ausbreiten können.

Der bekannteste Fall einen Computerwurm ist der 1988 in USA aufgetretene "Internet-Wurm", wo binnen kurzer Zeit einige tausend Rechner (SunOS und ULTRIX-Maschinen) durch einen Wurm zum Stillstand gebracht wurden.

Computerviren können sich auch in PC-Netzwerken ausbreiten. Diese Ausbreitung ist aber keine Funktion des Virus, sondern auf eine Eigenschaft von PC-Netzwerken zurückzuführen, die es ermöglicht fremde Laufwerke wie eigene anzusprechen.

Obgleich es noch keine "echten" Würmer auf PC-Netzwerken gibt, ist die Wahrscheinlichkeit recht hoch, daß es in Zukunft Computerwürmer für PC-Netze geben wird.

Computerviren

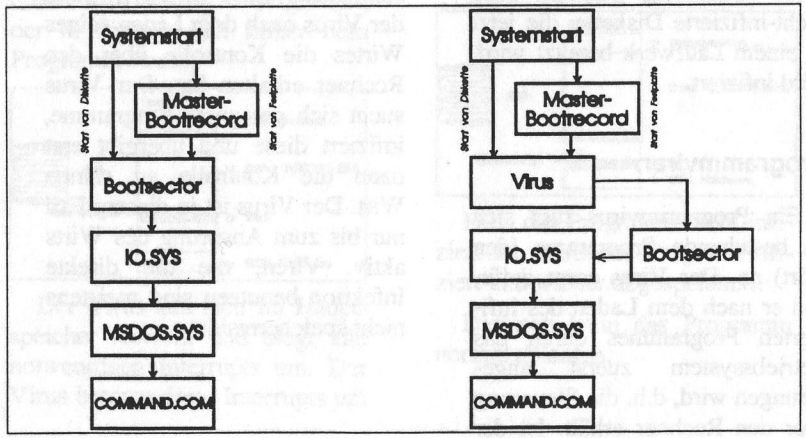
Computerviren sind die häufigsten Anomalien, und bedürfen deshalb einer genaueren Betrachtung. Abgesehen davon ist die "Viren-Eigenschaft" ein recht interresantes Phänomen.

Man unterscheidet bei Viren zwei grobe Arten, Systemviren und Programmviren.

Systemviren

Systemviren hängen sich in den Bootvorgang ein. Beim Laden des Betriebssystems werden vom Rechner bestimmte Sektoren von der Festplatte oder Diskette geladen und ausgeführt. Ein Systemvirus ersetzt nun gewisse Sektoren und wird dadurch beim Booten des Rechners in den Bootvorgang eingebunden.

Die Grafik verdeutlicht diesen Vorgang.



Bei einem normalen Systemstart (Bild links) von der Festplatte, lädt die POST-Routine (Power-On Self-Test) im BIOS (Basic Input/Output System) den Master-Bootrecord, oder bei einer Diskette den Bootsektor. Diese lädt wiederum das Betriebssystem. Je nach MS-DOS-Variante sind das die z.B. die Dateien IBMBIO.COM und IBMDOS.COM oder IO.SYS und MSDOS.SYS. Diese Bootvorgang gilt für alle PC-Betreibssysteme, z.B. auch UNIX. Dannach wird die Kommando-Interpreter geladen, meist COMMAND.COM.

Ein System-Virus kann sich überall in dieser Kette reinhängen, aber in der Regel ersetzen Viren den Bootsektor (Bild rechts), oder den Master-Bootrecord. Nachdem der Virus sich im Hauptspeicher resident gemacht hat, lädt er den Original-Bootsektor/Master-Bootrecord nach. Das Betriebssystem wird dann vollständig geladen. Jede nicht-infizierte Diskette, die jetzt in einem Laufwerk benutzt wird, wird infiziert.

Programmviren

Ein Programmvirus fügt sich an bestehende Programme (den Wirt) an. Der Virus sorgt dafür, daß er nach dem Laden des infizierten Programmes durch das Betriebssystem zuerst angesprungen wird, d.h. die Steuerung über den Rechner erhält. Ist der Virus abgearbeitet, so gibt er die Kontrolle an das Wirtsprogramm ab.

Die Grafik verdeutlicht diesen Vorgang. Während normalerweise das Programm sofort nach dem Laden durch das Betriebsystem die Kontrolle über den Rechner erhält, zeigt der Programmzeiger des infizierten Programmes zuerst auf den Virus. Sobald dieser abgearbeitet ist, gibt er die Kontrolle an das Wirtsprogramm weiter.

Infektionsvarianten:

Ein weiterer wichtiger Punkt bei Viren ist die Technik, die zur Infektion eines möglichen Wirtsprogrammes benutzt wird. Wir unterscheiden auch hier zwei grobe Arten:

Direkte Infektion

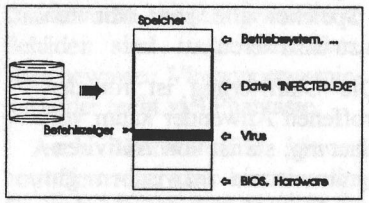
Bei der direkten Infektion werden weitere Programme ausschließlich dann infiziert, wenn der Virus nach dem Laden seines Wirtes die Kontrolle über den Rechner erhalten hat. Der Virus sucht sich geeignete Programme, infiziert diese und übergibt erst dann die Kontrolle an seinen Wirt. Der Virus ist in diesem Fall nur bis zum Ansprung des Wirts aktiv. Viren, die die direkte Infektion benutzen sind meistens nicht speicherresident.

Indirekten Infektion

Diese Viren sind hauptspeicherresident und überwachen bestimmte Systemaktivitäten, die dann Auslöser einer Infektion sind. Ein häufiges Vorgehen von diesen Viren ist die Überwachung der Betriebsystemfunktion "EXEC". Diese Funktion wird benutzt um ein Programm zu starten. Stellt der Virus diesen Vorgang fest, so wird das durch den Anwender beschriebene Programm durch den Virus infiziert und erst dann durch das Betriebbsystem geladen und angesprungen. Anders ausgedruckt: jedes geeignete Programm, das auf diesem Rechner gestartet wird, wird mit dem Virus infiziert.

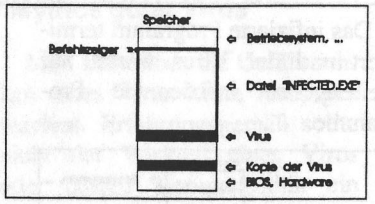
Ablauf einer indirekten Infektion

Eine infizierte Datei ("INFECTED.COM") wird von dem Datenträger geladen. Als erstes wird der Virus ausgeführt, der in diesem Fall hinter dem Programm steckt.

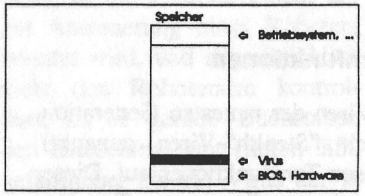


Der Virus lädt sich im Hauptspeicher resident und biegt alle notwendigen Interrupts um. Der Virus benutzt diese Interrupts um später aktiviert zu werden, z.B. beim Laden eines Programms.

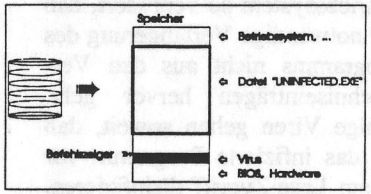
Dannach übergibt der Virus die Kontrolle an das Wirts-Programm, welches dann normal abläuft.



Nachdem das Wirts-Programm beendet ist, bleibt der Virus im Speicher aktiv und infiziert weitere Programme.

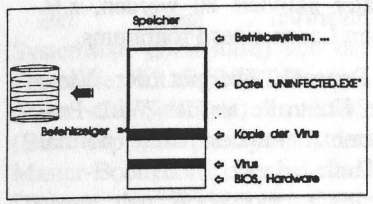


Ein nicht-infiziertes Programm wird geladen. Der Virus beobachtet dies, und wird aktiv. Als erstes prüft der Virus ob das Programm infiziert ist.

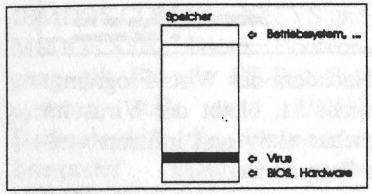


Falls das Programm nicht infiziert ist, wird das Program infiziert und wieder abgespeichert.

Dannach kann das Programm normal ablaufen.



Das infizierte Programm terminiert und der Virus wartet auf weitere, zu infizierende Programme.



Tarnfunktionen

Viren der neuesten Generation (auch "Stealth"-Viren genannt) weisen Tarnfunktionen auf. Diese Funktionen dienen zur Tarnung vor dem Entdecken durch Standardverfahren und Viren-Such-Programmen.

Am häufigsten wird das Betriebssystem so verändert, daß die notwendige Verlängerung des Programms nicht aus den Verzeichniseinträgen hervor geht. Einige Viren gehen soweit, daß sie das infizierte Programm vor einem Lese-Zugriff disinfizieren. So "sehen" Antiviren und Checksummen-Programme nur das saubere Programm.

Andere Möglichkeiten der Tarnung ist die Vermeidung von Interruptaufrufen um so von Interrupt-Monitor-Programmen (z.B. Flu-Shot) nicht erkannt zu werden. Hierbei werden die Interrupts durch "CALL FAR" Anwiesungen ersetzt, oder durch eine direkte Veränderung des Betriebssystems.

Obwohl solche Funktionen jetzt häufiger auftreten, sind sie jedoch nicht neu. Sehr alte Viren, wie z.B. der Shoe-B-Virus, besitzen schon Tarn-Funktionen.

Chiffrierung

Schon die ältesten Viren kannten die Möglichkeit der Chiffrierung. Letztendlich dient die Chiffrierung nur dazu, die Suche nach brauchbaren Such-Strings für Scanner zu erschweren. Ebenso wird damit erreicht, daß ein und derselbe Virus in verschiedenen Wirtsprogrammen nicht identisch vorliegt, weswegen er durch einen einfachen Codevergleich nicht mehr nachgewiesen werden kann. Chiffierung dient aber auch dazu, offentsichtliche Texte im Virus zu verbergen. Ein aktueller Virus ist sogar so weit gegangen, sich im Speicher alle paar Minuten neu zu chriffieren!

Die Chiffrierung ist für den betroffenen Anwender kaum von Bedeutung; sie ist von Antiviren-Programmierern inzwischen gut in den Griff bekommen worden, und stellt keine zusätzliche Gefahr dar.

Der Wirkteil

Ein letzter Punkt, der bei iren zu beachten ist, ist der Wirkteil. Man unterscheidet bei Viren zwischen zwei Arten von Wirkteilen. Solche Wirkteile, die keinen bleibenden Schaden hinterlassen - **transienter Schaden** - und jene die einen permanenten Schaden produzieren **-permanenter Schaden.**

Transienter Schaden

Transiente Schäden können Zeitschleifen, Bildschirmmanipulationen, Musik usw. sein. Z.B. der Herbst-Virus lässt in den Herbst Monaten die Buchstaben auf den Bildschirm (wie Blätter) herrunterfallen. Die Datei die augenscheinlich beschädigt wird wurde nicht angerührt. Der Oropax-Virus spielt alle fünf Minuten Melodien.

Permanente Schäden

Ein permanenter Schaden kann etwa das Kodieren oder Formatieren von Datenträgern oder Dateien sein. Andere permanente Schäden sind auch vorstellbar. Hier beweisen Virenprogrammierer leider recht viel Phantasie.

Auch Hardwareteile können betroffen sein, aber hierzu sollte frau zwei Punkte beachten: 1) Es gibt noch keine solchen Viren, 2) Es ist relativ unwahrscheinlich, daß solche Viren sich einer hohen Verbreitung erfreuen würden. *Ein Virenprogrammierer müsste eine solche Schadensroutine prüfen können, was nur ein recht vermögender Virenprogrammierer tun könnte.*

"Mythos guter Virus"

Man kann über die Gefährlichkeit eines Virus keine Aussagen machen. Erfahrungsgemäß sollte nicht der Wirkteil eines Virus oder desses Kompatibilität ein Kriterium für die Einschätzung sein, viel entscheidender ist die Bedeutung und Aufgabe des befallenen Rechners. Beispielsweise ist ein Prozessrechner, der zur Ansteuerung eines Roboters benutzt wird, und augenblicklich nicht den Roboterarm kontrolliert, da er gerade Buchstaben den Bildschirm runterfallen läßt, gefährlicher als ein Virus der in einem Kinderzimmer die Festplatte formatiert.

Schutz gegen Anomalien

Es gibt verschiedene Möglichkeiten sich vor Anomalien zu schützen. Jedoch gibt es auch bei Anwendung aller möglichen Schutzmaßnahmen keine absolute Gewißheit, daß eine EDV-Anlage frei von Anomalien ist. Dennoch läßt sich die Gefahr des Auftretens von Anomalien durch diese Methoden sehr stark herrabsetzen. Als einen ersten Schritt (und auch dem wichtigsten) zur Virusabwehr sollte das Verständnis der Anwender geschult werden. Es muß jedem Anwender klar sein, daß die Rechner an denen sie arbeiten, nicht sicher sind. Jede Sicherheitskonzeption steht und fällt mit dieser Einsicht.

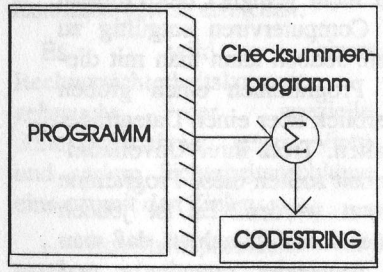
Die Methoden zur Vermeidung von Anomalien kann man grob in zwei Gruppen unterteilen. Zum einen gibt es die sogenannten Standardverfahren, zum anderen softwaregestützte Verfahren.

Standardverfahren

Es gibt eine Reihe von Betriebssystembefehlen oder externen Betriebsystemkommandos mit deren Hilfe man eine vielzahl von Viren nachweisen kann. Beispielsweise verlängern Programmviren die infizierten Programme. Das Kommando "DIR" kann nun diese Verlängerung anzeigen. Ebenso kann die Zeit/Datum-Angabe der Programme mit denen der Programme auf dem Originaldatenträger verglichen werden. Sind hier Abweichungen feststellbar, so sollten schon einmal leise die Alarmglocken klingeln. Leider können nicht alle Computerviren so einfach nachgewiesen werden. Die oben erwähnten Stealthviren sind so nicht zu entdecken. Hier empfiehlt es sich auf Programme zurückzugreifen, die einem bei der Suche und eventuell auch bei der Beseitigung von Viren behilflich ist.

Checksummenprogramme

Checksummenprogramme sind geeignet eine vielzahl von Viren nachzuweisen. Diese Programme bilden eine Checksumme über die zu prüfenden Dateien. Wird ein Programm von einem Virus infiziert, so wird sich auch dessen Checksumme verändern. Nun kann leider nicht immer der Schluß gezogen werden: "Wenn sich die Checksumme ändert, so ist dieses Programm infiziert", meist wird man aber dennoch gute Aussagen erhalten können. Der Vorteil von Checksummenprogrammen liegt zum einen darin, daß diese einen Datenträger selbständig prüfen können, ohne das ein Anwender spezielle Eingaben machen muß (es gibt auch implementierungen wo Betriebssystems durch eine Checksummenroutine erweitert wird und nur diejenigen Programme lädt, deren Checksumme nicht verändert sind), zum anderen können mit Checksummenprogrammen eine Vielzahl (auch unbekannte Viren) festgestellt werden. Der Nachteil dieser Checksummenprogramme ist offensichtlich. Da diese Programme lediglich die Veränderung von Dateien aufzeigen, ist eine Aussage, ob diese Veränderung durch einen Virus bedingt wurde, nicht möglich. Der Anwender ist dann auf weitere Informationen angewiesen. Ein weiterer Nachteil besteht darin, daß ein Anwender natürlich nicht sicher sein kann, ob ein neu installiertes Programm zum Zeitpunkt des ersten Checks virenfrei ist. Hier helfen aber schon einige Softwarehersteller, die ihre Programme mit der Angabe der Checksumme vertreiben, sodaß der Anwender zum Zeitpunkt der Installation das Programm noch einmal überprüfen kann.

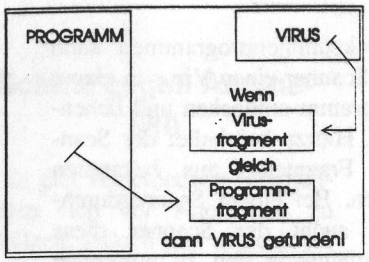


Scanner

Scanner gehören auch zu den Programmen, die man zum Nachweis von Viren einsetzen kann. Aber anders als bei Checksummenprogrammen kann ein Scanner einen Virus in einem Programm entdecken und benennen. Hierzu beinhaltet der Scanner Fragmente aus bekannten Viren. Bei einem Scannerdurchlauf sucht der Scanner diese Fragmente in den zu prüfenden Programmen- ist ein solches Fragment gefunden, so wird das Programm als mit dem Virus infiziert ausgewiesen.

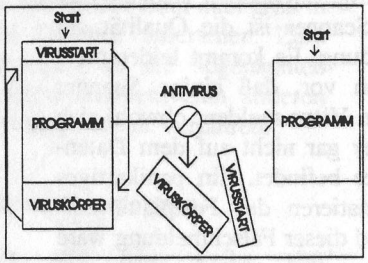
Scanner sind eine schnelle und relativ sichere Möglichkeit Viren nachzuweisen. Außerdem sind Scanner meist Shareware-Programme und somit preisgünstig. Dennoch besitzen Scanner auch einige Nachteile. Scanner können nur bekannte Viren suchen. Hierdurch sind diese Scanner relativ schnell veraltet. Ferner kann ein Scanner nicht alle Viren beinhalten, d.h. der Scanner ist nie vollständig. Ein anderer Nachteil dieser Scanner ist die Qualität der Meldung. Es kommt leider nicht selten vor, daß einige Scanner einen Virus melden, obwohl sich dieser gar nicht auf dem Datenträger befindet. Ein panikartiges Formatieren der Festplatte aufgrund dieser Falschmeldung wäre fatal.

Erweitert man ein Scanprogramm durch eine Routine, die in der Lage ist, einen gefundenen Virus aus dem Wirtsprogramm zu entfernen, so erhält man einen Antivirus.



Antivirus

Ein Antivirus ist die bequemste Methode einen Virus zu beseitigen. Speziell bei einer großen Anzahl von Rechnern ist der Einsatz eines Antivirus meist die einzige Möglichkeit einen Virus in einer angemessenen Zeit und mit einem angemessenem Aufwand zu entfernen. Die bislang vorgestellten Programme können einen Virus erst dann nachweisen, wenn er bereits aufgetreten ist, also ein oder mehrere Programme bereits infiziert sind.



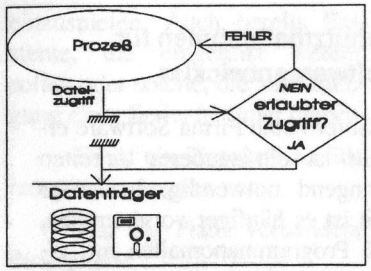
Zugriffsüberwachungsprogramme

Zugriffsüberwachungsprogramme haben diesen Nachteil nicht. Diese Schutzprogramme versuchen "online" Schreibzugriffe auf Datenträger aufzuzeigen und gegebenenfalls zu unterdrücken. Grundlage dafür ist die Tatsache, daß ein Virus bei der Infektion auf ein Wirtsprogramm natürlich Schreiboperationen ausführen muß. So vielversprechend sich diese Ansätze auch anhören mögen ist uns bislang jedoch kein Zugriffsüberwachungsprogramm bekannt, dessen Vorteile seine Nachteile überwiegen. Es treten bei Einsatz dieser Programme vielfach Inkompatibilitäten auf, die ein Arbeiten mit dem Rechner erschweren oder teilweise auch unmöglich machen. Desweiteren sind einige Bildschirmmeldungen nur schwer verständlich:

```
WRITE TO SEC 12, HEAD 4
(Continue/Cancel)
```

Es wird sich wohl kaum ein Anwender finden lassen, der auf solcherlei Meldungen richtig reagiert.

Alle vorgestellten Verfahren sind nicht geeignet das Problem der Computerviren entgültig zu lösen. Jedoch kann man mit diesen Programmen einen groben Überblick über einen Datenträger erhalten. Trotz ihrer Unvollkommenheit sollten diese Programme benutzt werden. Es ist jedoch immer darauf zu achten, daß man als Anwender quantitativ und qualitativ gute Aussagen über ein Problem erhält, da eine schwerwiegende Entscheidung wie das Formatieren von Datenträgern (und somit der Verlust der Daten) wohl begründet sein sollte.



Organisatorische Maßnahmen

Die Viren-Problematik ist nur ein Teil der Rechnersicherheit. Andere Gefahren sind z.B. Datenverlust durch Software/Hardware Fehler, Sabotage, oder Wirtschafts-Spionage. Um diese Gefahren entgegenzutreten bedarf es einen Rechnersicherheits-Konzept. Leider gibt es auch hier keine Patentrezepte; jeder Firma muss seine eigene Schwerpunkte setzen da es gilt eine akzeptable Gleichgewicht zwischen Sicherheit und Benutzbarkeit zu erreichen.

Es wird einen Rechnersichterheitskonzept gebraucht, der spezielle Schutzmaßnahmen gegen Viren und andere Sicherheitsprobleme einsetzt mit den Zielen:

- Sicherheitsprobleme vermeiden,
- Sicherheitsverstösse entdecken,
- die Ausmaße einer Unfall zu beschränken,
- nach einen Unfall den normalen Betrieb innerhalb kurzer Zeit und mit geringen Kosten wiederherzustellen.

Um diese Ziele zu verwirklichen, richten wir Aufmerksamkeit auf folgende Punkte:

Benutzer Schulung:

Benutzer sollten über die Rechnersicherheit unterrichtet werden und insbesonders auf gefahrenquellen hingewiesen werden. So werden die Benutzer für die Problematik sensibilisiert, und werden eher bereit sein, einschränkungen hinzunehmen. Ausserem spielen die Benutzer bei der Bekämpfung von Viren eine wichtige Rolle, und sollten sich deshalb gut mit ihren Rechner auskennen.

Software Verwaltung:

Zu der Einführung und Pflege von Software sollte ein Konzept erstellt und eingehalten werden. Man sollte darauf achten, daß angeschaffte Software die erforderliche Sicherheitsanforderungen entspricht. Die Endbenutzer sollten auf diese Software geschult werden, da nur gute Kenntnis über die Software die richtige Bedienung und so wenige Probleme gewähleisten kann.

Technische Zusätze:

Der Einsatz von Software- und Hardware--Zusätze sollten überlegt werden. Es gibt eine Reihe

von nutzliche Software- und Hardware- Erweiterungen. Die Sicherheitsansprüche entsprechend, sollten soche Zusätze eingesätzt werden.

Überwachung:

Benutzer und programmaktivitäten sollten überwacht werden um Sicherheitsverstösse oder Sicherheits-Probleme zu erkennen, sowie auch die Effektivität der Sicherheitsmaßnahmen zu prüfen.

Notfall-Planung:

Eine funktionierende Notfall-Plan sollte zu jeder Konzept gehören. Datensicherungen sollten regelmässig durchgeführt werden. Einige Backups sollten auch länger behalten werden. Programme sollten allerdings nicht mitgesichert werden, sondern bei Bedarf von den Originalen wieder installiert werden. Sämtlich Parameter sowie andere Installations-Informationen sollten protokolliert werden, damit dieses Wissen nicht im Zeitaufwendigen Verfahren wiedererlangt werden muss. Bei totaler Ausfall der Rechner kann bei Bedarf eine Ausweichsrechner zur Verfügung gestellt werden. Ausserdem sollte eine Trockenübung ausgefüht werden um die Wirksamkeit der Notfall-Planung zu prüfen.

Schutzmaßnahmen für Softwareentwickler

Sofern eine Firma Software erstellt ist ein sauberes Arbeiten zwingend notwendig. In letzter Zeit ist es häufiger vorgkommen, daß Programmanomalien mit einer Originalsoftware ausgeliefert wurde. Dies führte bei den beteiligten Firmen nicht nur zu Schadensersatzforderungen, sondern auch zu einem hohen finanziellen Aufwand um eine anomaliefreie Version als ´quasi Update´ auszuliefern. Ebenso ist der rufschädigende Effekt, den eine Firma erleidet, nicht zu unterschätzen.

Bei der Erstellung des Endproduktes sollte ein Rechner verwendet werden, dessen Datenträger neu formatiert sind, bzw ein Rechner der ausschließlich der Endcompilation dient. Folgendes sollte beachtet werden

- Der Rechner ist von einer Originaldiskette zu booten und das Betriebssystem ist von der Originaldiskette einzuspielen

- Es dürfen nur Programme eingespielt werden, die zur Herstellung des Endproduktes zwingend notwendig sind (Compiler, Linker, Libraries)

- Alle Programme müssen Originalsoftware der Originaldatenträger sein.

- Alle weiteren Programme sind in Form von Sourcetexten

einzuspielen. Auch bereits Existente, die eingelinkt werden sollen oder solche, die zur Erzeugung einer Seriennummer dienen.

- Es ist ein Protokoll zu führen mit der Angabe von

+ Auf der Platte vorhandene Programme

+ Zeit, Datum, Benutzer

+ Reihenfolge der Programmaufrufe, sowie deren Zwischenerzeugnisse

+ eventuell Beschreibung der Zwischenprodukte mit Länge, CRC

- formatieren der benötigten Disketten auf diesem Rechner

- duplizieren der erzeugten Programme auf Diskette(n)

- schreibschutz der Diskette anbringen.

- Prüfung der Diskette(n) mit weiteren Hilfsmitteln auf einem anderen Rechner.

- Beschreibung der Disketten

+ Zeit, Datum der Erstellung, Benutzer

+ Verweis auf obiges Compilationprotokoll

+ Beschreibung der Daten auf der Diskette(n) mit Länge, Modifikationdatum, lokalität auf dem Datenträger, CRC der Dateien sowie der physikalischen Bereiche der Diskette.

Die oben genannten Prüfungen sind mit einer zufällig ausgewählten Anzahl und einer zufällig gewählten Reihenfolge der Disketten zu wiederholen, die von einer Kopierumgebung erstellt wurden. Das Verfahren bietet keinen absoluten Schutz vor Programmabnormalitäten, jedoch ist bei so einem Vorgehen die Möglichkeit einer Solchen stark reduziert und eine notwendige Lokalisierung dieser leichter möglich. Desweiteren ist der Forderung Rechnung getragen, daß im Rahmen der zu Verfügung stehenden Mittel eine Programmanomalie ´vermieden´ wurde (dies hat auch eine rechtliche Relevanz). In wieweit diese Protokolle oder die Aublaufschemata von einer aussenstehenden Quelle (Notar o.ä.) beobachtet, bzw geprüft werden ist von Fall zu Fall zu untersuchen.

Aussichten

Der Anzahl der Viren steigt sprunghaft an. Waren es 1988 erst 20 Viren, so waren es 1989 schon 120 Viren. Heute im Februar 1991 sind es bereits über 450 Viren allein im Bereich der PC´s. Diese Zahl klingt nicht nur gewaltig, sie beschreibt auch die große Gefahr des Anwenders seine Arbeiten mit Hilfe von PC´s nicht mehr ordnungsgemäß erledigen zu können. Selbst wenn diese Viren nicht das Ende von MS-DOS bedeuten sollten, so doch wohl von der allzu großen Überzeugung über den unfehlbaren Computer. Es gibt keinen absoluten Schutz vor Computerviren, aber gerade aus dieser Einsicht herraus sollte ein jeder Anwender lernfähig sein und die Gefahren und Hindernisse die mit der PC-Technik verbunden sind begreifen. Erst wenn diese Einsicht der Anwender genauso stark zunimmt wie die Anzahl der Viren ist ein Bankrott der PC-Welt abzuwenden.

Wir wünschen ihnen eine viren-freie Zunkunft!