Andreas Reisinger
Homepage: www.user.xpoint.at/aki
E-Mail: aki@xpoint.at
Spezialgebiet Informatik

Computerviren

Inhalt:

1) Computerviren allgemein:

a) Definition eines Computervirus:

Ein Computervirus ist ein Programm, daß in der Lage ist, Kopien von sich selbst herzustellen und in andere Programme einzupflanzen (infizieren). Der Virus kann eine genau definierte Aufgabe ausfüllen. Programme die infiziert wurden sind ihrerseits wiederum Viren.

c) Ziel und Zweck eines Computervirus:

Viren richten im allgemeinen nur Schaden an. Zu Forschungszwecken werden auch Viren eingesetzt die sich nur reproduzieren und keine Veränderungen an Programmen vornehmen.

Mögliche Schäden:

-) *Harmlose aber störende Bildschirmanimationen*
-) *Daten- bzw. Dateizerstörung* durch Löschen oder Überschreiben
-) *Zerstörung von gesamten Disketten- bzw. Festplatteninhalten* durch Formatieren
-) *Manipulation von Daten* durch z.B.: *)Ersetzen bestimmter Zeichenketten
*)Verfälschung der Tastatureingaben
-) *Beschädigung von Hardware* durch z.B.: *) Die Erhöhung der Bildschirmfrequenz mittels der Grafikkarte hat manchmal ein Verschmoren der Leuchtschicht an der Bildschirminnenseite zur Folge.
*) Bei manchen Diskettenlaufwerken verklemmt sich der Lese/Schreibkopf wenn versucht wird über die innerste Spur hinauszulesen.
*) Die Überbeanspruchung eines elektronischen Bauteils wie z.B. des Co-Prozessors kann zu dessen Beschädigung führen.
-) *Blockierung von Speicherplatz* durch z.B.: *) das Schreiben riesiger Dateien mit sinnlosem Inhalt auf die Festplatte oder Diskette.
*) das Laden sinnloser Programme in den Arbeitsspeicher.
-) *Reduzierung der Systemleistung* durch z.B.: *) Verkleinerung des Arbeitsspeichers (siehe oben)
*) Beanspruchung der Prozessorleistung für sinnlose Berechnungen.
-) *Blockierung von Programmen* durch Aufforderung zur Eingabe eines Paßwortes ohne dessen ein Programm nicht gestartet werden kann.
-) *Nichts*

c) Woher kommen Viren:

Viren werden meistens von Privatpersonen mit destruktiver Veranlagung, still und heimlich im einsamen Kämmerlein programmiert. Der “klassische” Computervirus hatte meistens das Ziel bestimmte Unternehmen und Firmen durch Datenmanipulation- oder Zerstörung zu schaden. Vorteile eines Virus:

-) Die Herkunft eines Virus nur selten feststellbar ist
-) Viren an Daten herankommen, die vor direkten Zugriffen geschützt sind

-) Viren sehr schnell verbreitet werden können, da die Vermehrung exponentiell verläuft.

Die häufigsten Herkunftsländer (nach Bedeutung geordnet):
1) USA
2) Rußland
3) Deutschland
4) Bulgarien
5) Polen

In Österreich, beispielsweise, verursachen Computervirenschäden jährlich einen Schaden von ca. 100 Mio. S
Derzeit sind ca. 8000 Viren bekannt. Täglich kommen 2-3 neue dazu. Durch flächendeckenden Einsatz von Virenbekämpfungsmaßnahmen wurden aber schon viele Viren praktisch total unschädlich gemacht.

c) Rechtslage:
In Österreich und Deutschland ist die Rechtslage bezüglich Computerviren sehr ungenau definiert. Das Programmieren von Computerviren ist demnach nicht ausdrücklich verboten, sehr wohl aber deren - auch nur versuchte - Anwendung und vor allem die daraus resultierende Veränderung von Daten. Strafbar ist die Anwendung jedes Virus, auch wenn er keinen Schaden anrichtet, da in jedem Fall durch das Kopieren des Virusprogramms eine Veränderung von Datenbeständen erfolgt. Es gibt aber keine wirklich genauen Verbote für die indirekte Verbreitung von Viren, etwa für das Einschleusen in Netzwerke anstatt durch direkte Infektion des zu manipulierenden Computers. In der Schweiz hingegen sind alle Schritte, vom Programmieren bis zur Verbreitung, sowie der Anstiftung dazu, mit einer Freiheitsstrafe von bis zu 5 Jahren belegt. Sowohl in der Schweiz als auch in Österreich und Deutschland ist allerdings mit weitreichenden Schadenersatzforderungen sowie einer Bestrafung für andere, durch den Vireneinsatz begangene Delikte, etwa Betrug durch einen Virus, der Bankguthaben verschiebt, zu rechnen.
Immer wieder wird der Einsatz von Viren als Schutz vor Raubkopien diskutiert, d.h. ein illegal benütztes Programm setzt einen Virus frei. Dies ist allerdings rechtlich nur so weit gedeckt, als nur das betroffene Programm - und kein Byte mehr - in Mitleidenschaft gezogen wird.

2) Computervirenarten:

a) Programmvirus
Programmviren befallen Dateien die in ausführbarem Programmcode vorliegen. Zumeist sind diese .EXE, .COM und oft auch .SYS Dateien. Diese Programme bestehen aus 3 Teilen: *Start – Eigentliches Programm – Ende*

Programmviren gliedern sich wiederum in 2 Bereiche:

α) Nichtüberschreibende Viren:
Der Virus kopiert sich entweder

*) *an das Programmende*. Dabei verschiebt er auch den Startteil des Wirtprogrammes an das Ende und fügt einen Verweis auf den Viruscode am Anfang der Datei ein. (siehe Grafik) Beim Aufruf der Datei springt der DOS Loader (=Leseroutine) zum Virus und führt ihn aus. Die ursprüngliche Startanweisung zeigt auf den normalen Programmcode, der dann gestartet wird. Danach wird das Programm beendet.
Der Anwender merkt davon nichts, da Viren meist nur winzig klein sind und in einem Bruchteil einer Sekunde ihre Arbeit erledigt haben. Die Länge des Ursprungsprogrammes wird erweitert obwohl es nach außenhin normal abläuft. So bleiben Infektionen oft lange unbemerkt

*) a*n den Programmanfang*. Zunächst wird der 1. Teil des Wirtprogrammes in der Größe des Viruscodes herausgeschnitten, mit Hilfe einer Verschieberoutine (VR) markiert und am Ende der Datei eingefügt. Der Virus wird an den Dateianfang kopiert.
Beim Start des infizierten Programmes wird der Virus ausgeführt und dann die VR gestartet, die den verschobenen ersten Programmteil in seine Ursprungsposition, über den Viruscode, rückt. Das Programm ist wiederhergestellt und kann normal gestartet und beendet werden. Da das Ausführen eines Programmes im Arbeitsspeicher erfolgt, bleibt die Datei auf der Festplatte unverändert und somit noch immer infiziert.

β) Überschreibende Viren
Bei der Fortpflanzung eines Virus dieses Typs, überschreibt dieser einfach den Anfang des Wirtprogrammes. Dieses wird aber dadurch fehlerhaft und funktionsunfähig.

Vorteile:
*) Einfach zu programmierender Virus
*) Da die Dateigröße nicht verändert wird, können manche Antivirenprogramme den Virus nicht aufspüren.

Nachteil:
*) Durch das fehlerhafte Programm bemerkt der Benützer den Virus sehr schnell, vielleicht bevor dieser sich ausreichend vermehren konnte.

b) Speicherresidente Viren:
haben eine etwas effektivere Fortpflanzungsmethode als die Vorhergenannten. Wird nämlich ein infiziertes Programm aufgerufen, laden sich der speicherresidente Virus in den Arbeitsspeicher. So kann er auch wenn das eigentliche Programm beendet wird aktiv bleiben und seinen "Auftrag" ausführen.

Und das geht so:
Die Computerviren überwachen bestimmte DOS- oder BIOS- Interrupts in der Interrupt-Vektor-Tabelle. Benötigt ein Programm nun eine Systemfunktion (z.B. eine Tastatureingabe) so fordert sie diese über einen Interrupt an. Was bei dem Ausführen eines Interrupts geschieht, steht in der Interrupt-Vektor-Tabelle. Da diese Tabelle im Arbeitsspeicher liegt, kann der Virus hier verändernd eingreifen und der angeforderte Interrupt führt anstatt der ursprünglichen Interruptfunktion, die Virusfortpflanzungsroutine aus. Das aktive Programm wird infiziert.

c) Source-Code Viren:
Hier liegt der Computervirus nicht als ausführbarer Programmcode vor, sondern als Quellcode einer Programmiersprache wie z.B.: Pascal, C, usw.
Da ein plötzlich auftauchender fremder Code in einem Programm sehr verdächtig sein würde, infiziert der Virus bevorzugt Programmbibliotheken, die meist nicht kontrolliert werden.
Compiliert und startet man nun das Programm, wird irgendwann auch die Programmbibliothek benötigt und der Virus kann somit aktiv werden. Er sucht dann wiederum nach anderen Bibliotheken und infiziert diese. Das funktioniert aber nur wenn noch der Quellcode des Virus in der uncompilierten Datei vorliegt.

d) Call Viren:
Call Viren versuchen Auffälligkeiten wie die Veränderung der Dateigröße oder Zerstörung des Wirtprogrammes zu vermeiden. Deshalb liegt der Virus als versteckte Datei irgendwo auf dem Datenträger vor. Nur ein Link, der ggf. so angebracht werden kann, daß das infizierte Programm nicht verlängert wird, ruft den Virus vom Wirtsprogramm aus auf.

e) Bootsektorviren:
Der Bootsektor ist der Sektor einer Festplatte der beim Systemstart als erster gelesen wird und der dem Rechner mitteilt, was er nach dem Einschalten machen soll. Ein Bootsektorvirus überschreibt diesen Sektor mit dem eigenen Programmcode und verweist, nach der Erfüllung seiner Aufgabe, auf eine zuvor angelegte Kopie des originalen Bootsektors auf der Festplatte.

f) Partition Table Virus:
Der Virus nistet sich im Partition Table (Sektor 0) der Festplatte ein und infiziert von dort aus den Bootsektor. Selbst beim Formatieren der Festplatte oder löschen des Bootsektors bleibt der Virus erhalten. Weitere Strategie des Virus siehe e).

g) Companion Viren:
Der Virus liegt in Form einer .COM Datei vor, die den selben Namen hat wie die infizierte .EXE Datei. Da DOS immer die .COM Dateien zuerst startet, kann hier der Virus aufgerufen werden, der nach dem Ausführen seines Programmes die ursprüngliche .EXE Datei startet.

h) Macro Viren:
Ein Macro ist eine Zusammenfassung einer Abfolge von Befehlen. Sie werden zur Arbeitserleichterung in Programmen wie MS-Word eingesetzt. Macroviren sind die neueste Generation von Computerviren und sehr effektiv, da Makros an normale Dokumentdateien gebunden sind und somit leicht verbreitet werden. So ist es z.B.: möglich von Word aus unbemerkt die Festplatte zu formatieren.

Folgende Virenarten sind Spezialformen der oben von a)-h) genannten:

i) Cavity Viren:
Cavity Viren versuchen die Größe der infizierten Datei nicht zu verändern um sog. Check- Summen Programmen zu entgehen. Sie suchen in der Zieldatei eine Stelle mit einer Reihe an identischen Zeichen die mindestens so groß wie der Virus selbst sein muß. Dieser komprimiert dann diese Zeichenkette und fügt sich in die entstandene Lücke ein.
Greift das Programm auf die vermeintliche Zeichenkette zu, wird der Virus ausgeführt, der nach Erfüllung seiner Aufgabe die Zeichenkette dekomprimiert und das Programm kann normal weiterlaufen.

Bsp. einer Infektion:
Programm vorher: AJF3JS2000000000000000000000000000DNFJAKSF289a
Programm nach Infektion: AJF3JS2=>*VIRUSCODE+12*0*<=00000000DNFJAKSF289a

j) Stealth Viren:
Stealth Viren versuchen dem Benutzer vorzugaukeln, sie wären gar nicht im System. Sie tarnen sich dadurch, daß sie die Zugriffe auf die infizierten Dateien überwachen. Will z.B. der DOS-Befehl DIR die Größe einer infizierten Datei anzeigen, subtrahiert der Virus von diesem Wert seine Codegröße und täuscht somit eine “gesunde” Datei vor.

Durchsucht ein Antivirusprogramm beispielsweise die Festplatte desinfizieren manche Stealthviren die infizierten Dateien und kopieren sich in den Arbeitsspeicher. Nach der Beendigung des Antivirenprogrammes werden die Dateien wieder infiziert.

k) Polymorphe Viren:
Da ein Großteil der Antivirusprogramme nach fixen Viruszeichenketten sucht, bietet es sich als Virus an, eben solche nicht anzubieten. Polymorphe Viren beinhalten Zeichenketten, die sich ständig, mit Hilfe einer Mutations-Engine, verändern und eine gezielte Suche sehr erschweren.

l) Bounty Hunter Viren:
suchen nach Antivirussoftware und verändern diese oder machen sie unschädlich. Diese Viren sind äußerst selten, aber sehr effektiv, da sie nach dem Ausschalten der AV praktisch freie Bahn haben.

m) Hybrid Viren:
stellen eine Virusart dar, die möglichst viele Mechanismen vereint. Sie vereinen beispielsweise einen Programmvirus, einen speicherresidenten Virus und einen Bootsektorvirus zu einem äußerst gefährlichem Programm.

3) Genereller Aufbau:

Ein Computervirus besteht mit Ausnahmen aus 2 Hauptteilen:

a) Der Fortpflanzungsmechanismus:

Genau wie bei einem biologischen Virus ist eine der Aufgaben eines Computervirus die möglichst weite Verbreitung in alle Winkel eines Computersystems. Dazu wird ein oft ausgeklügelter Fortpflanzungsmechanismus geschrieben. Je nach Virenart (siehe 2)) werden Dateien, Bootsektoren, Arbeitsspeicher, BIOS-Speicher, Macros, MBRs infiziert.

Bei der Infektion einer Datei kopiert der Virus neben dem eigentlichen Programm einen speziellen Code in das File. Falls der Virus jetzt versucht eine schon infizierte Datei nochmals zu infizieren und dabei auf seinen eigenen Code stößt, weiß er, daß die Datei schon von ihm infiltriert ist und eine doppelte Infektion wird somit vermieden.

b) Der Auftrag:

Nach dem Ziel, das der Programmierer verfolgt, gestaltet sich der Auftrag. Vom einfachen Nichtstun bis zur Zerstörung von Bildschirm, Laufwerke und Löschung von Festplatten usw. ist alles möglich.

Um möglichst lange unentdeckt zu bleiben und um sich weit verbreiten zu können, tritt die Schadensfunktion meistens erst nach einiger Zeit in Kraft. Viren verwenden dazu sog. Trigger, d.h. der Virus wird erst nach dem Eintreten eines bestimmten Ereignisses aktiv.

Beispiele für Trigger:
Aktivierung
-) an einem bestimmten Datum (Fr 13.13.1333)
-) nach dem 100. Start des infizierten Programmes
-) nach dem 200. Start des Computers
-) nach Drücken einer bestimmten Tastenkombination
-) an einer bestimmten Uhrzeit

4) Allgemeine Funktionsweise:

Der folgende Beispiel-Pseudo-Pascal-Programmcode beschreibt die prinzipielle Funktionsweise von Computerviren:

```
1  program BÖSER_VIRUS
2  HIHÄHU
3
4  procedure Infiziere_neues_Programm;
```

```
5   begin
6   gefunden:=false;
7   repeat
8    zieldatei:=irgendeine_EXE_oder_COM_Datei;
9      if not (2. Zeile von zieldatei)=HIHÄHU then begin
10            gefunden=true;
11            infiziere_Datei(zieldatei);
12            end;
13  until gefunden=true;
14  end;
15
16  procedure Aufgabe;
17  begin
18   if Datum=13.13.1333 then format C:
19  end;
20
21  begin
22   Infiziere_neues_Program;
23   Aufgabe;
24   Starte_Wirtprogramm;
25  end.
```

In dieser Form wäre der Virus natürlich nicht funktionstüchtig.

Erklärung der einzelnen Abschnitte:

Zeile 2: Dies ist der spezielle Viruscode der schon in 3)a) erklärt wurde. Bei jeder Neuinfektion einer Datei überprüft der Virus ob diese Zeichenkette in der Datei schon enthalten ist. Ist das der Fall, ist die Datei schon infiziert.

Zeile 4-14: Hier wird eine zu infizierende Datei gesucht (Zeile 8) und überprüft ob sie noch "gesund" ist (Zeile 9). Ist das der Fall, wird sie "gekränkt".

Zeile 16-19: Hier sind die Aufgabe des Virus und der Zeitpunkt der Ausführung definiert. In diesem Fall formatiert der Virus am 13.13.1333 die Festplatte C:.

Zeile 21-25: Das ist das Hauptprogramm in dem die einzelnen Abschnitte (Infektion, Aufgabe, Start des Wirtprogramms) aufgerufen werden. In Zeile 24 wird das Wirtprogramm gestartet um dem Benutzer ein fehlerfreies Programm vorzugaukeln.

5) Virenschutz:

a) Virenverbreitung:

Viren können sich so ziemlich über jeden Zugriff auf einen infizierten Speicher fortpflanzen.
Bei einem Bootsektorvirus reicht das Vergessen einer infizierten Diskette im Laufwerk beim Bootvorgang. Wird auf die Diskette zugegriffen, offenbart sich dem Virus quasi eine neue Mahlzeit und er beginnt das System zu infizieren.
Das Internet stellt die beste Verbreitungsmöglichkeit für Viren dar. Tausende Programme werden täglich downgeloaded von denen jedes einen Virus beinhalten kann. Der Weg über die Telephonleitung ist der schnellste Weg für einen Virus sich auf der ganzen Welt

zu zerstreuen. Entgegen vieler Befürchtungen können Viren nicht über E-Mails übertragen werden, außer natürlich, wenn die, über E-Mail übertragenen Programme, infiziert sind.

b) Antivirenprogramme:

Antivirenprogramme sind die beliebteste und bequemste Methode sich vor Viren zu schützen. 100%igen Schutz können sie aber nicht bieten. Die einzige Möglichkeit allen Infektionen vorzubeugen ist, den Computer von fremden Daten total abzuriegeln. Keine Diskette, CD-ROM oder Internetverbindung wäre in diesem Fall erlaubt. Sogar Originaldisketten können Viren transportieren.
Weiters können AVs auch falschen Alarm geben (sog. False Positives), falls sich ein legitimes Programm dem Verhalten eines Virus zu sehr annähert.

Es gibt mehrere verschiedene Arten von AVs:

α) Monitor-Programme:

sind speicherresidente Programme. Sie warten im Hintergrund auf virentypische Aktivitäten wie z.B.:

*) Veränderung von ausführbaren Dateien
*) Verbiegen von Interrupt Vektoren
*) Formatieren von Sektoren
*) usw.

Sie fragen dann den Benutzer ob diese Zugriffe legitim und erlaubt sind oder nicht. Wenn nicht, ist vermutlich ein Virus im Spiel.
Leider können die meisten Monitore von manchen Viren problemlos übergangen werden.

Man sollte nie mehr als ein Monitor-Programm auf seinem Rechner installiert haben, da sie sich garantiert nicht vertragen.

β) Scanner:

sind die meistverwendeten AVs. Die älteren Programme dieser Art durchsuchen die Dateien nur nach virenspezifischen Zeichenketten oder nach sog. Jokerzeichen, die auf mehrere Virenvarianten passen und somit den Scanner flexibler machen.
Leider muß, um mit diesen Programmen einen Virus finden zu können, dieser schon bekannt und analysiert worden sein. Außerdem sind sie gegen polymorphe Viren (siehe 2)i)) so gut wie hilflos da in diesem Fall jede Virengeneration- oder Variation ihren eigenen Scan-String bräuchte.
Deswegen verwenden moderne Scanner Ansätze von künstlicher Intelligenz und heuristische Methoden (siehe 5)b)δ)) um gegen unbekannte Viren besser gewappnet zu sein. In diesem Fall erhält der Benutzer aber keine Information über den Virus sondern muß auf Grund der erkannten Symptome und einer Wahrscheinlichkeitsaussage seitens des Scanners selbst entscheiden ob eine Infektion vorliegt oder nicht.

Um ein System wirkungsvoll zu schützen sollte man mindestens 2 verschiedene Scanner alle 2 Wochen benützen.

**) Speicherresidente Scanner:*

sind eine spezielle Form der herkömmlichen Scanprogramme. Sie werden bei einem Programmstart oder Dateizugriff seitens des Benutzers aktiv und scannen die betroffenen Files. Wird ein Virus gefunden, gibt der TSR-Scanner Alarm.

χ) Integrity-Checker oder Checksummenprogramme:
sind Programme, die von Datenabschnitten Checksummen erstellen. Datenabschnitte können Bootsektoren, Dateigrößen, Programme, Sourcecodes, usw. sein. Diese Checksummen werden mit einer, von Zeit zu Zeit neu erstellten, verglichen. Suspekte Änderungen der Datenabschnitte können auf einen Virus hinweisen.
Gute Integrity-Checker erkennen zudem auch Sicherheitslücken und spüren Companion-Viren (siehe 2)e)) auf.
Weiters weisen sie auf nicht durch Viren manipulierte Dateien hin und bemerken Datenverluste durch, beispielsweise, einer alten Festplatte.

δ) Heuristische Scanner:
arbeiten nach dem Prinzip der Fuzzy-Logic (Berechnungen erfolgen Daumen mal Pi). Sie analysieren Programme auf deren Funktion und Aufbau. Werden hier verdächtige Funktionen erkannt, schlägt der Scanner Alarm wenn die untersuchte Datei mehrere beinhaltet.

Verdächtige Funktionen sind z.B.:
*) Schreiben in ausführbare Dateien
*) Modifizieren von Dateiattributen
*) Undokumentierte Interruptzugriffe
*) Suchen nach beliebigen ausführbaren Dateien

c) Viren Cleaner:
Die meisten Antivirenprogramme enthalten auch Viren-Entfernungsfunktionen, die versuchen, Dateien wieder in ihre ursprüngliche Form – nicht infiziert – zu versetzen. Diese können aber nur vernünftig funktionieren, wenn eine exakte Beschreibung des Virus vorliegt und dieser außerdem richtig erkannt wurde. Da aber oft sehr viele Variationen eines Virus im Umlauf sind, wird die wiederherzustellende Datei meistens, durch einen nicht genau genug passenden Entfernungsvorgang, beschädigt und somit unbrauchbar. Somit ist es immer günstig ein Backup aller wichtigen Daten auf der Festplatte bei der Hand zu haben.

6) Virenbeispiele:

a) "Form" – Virus:

Charakteristik:
Der Form-Virus ist eine Mischung aus Bootsektorvirus und speicherresidenten Virus. Er infiziert einen Teil des High DOS Memory, den Bootsektor und die letzten zwei Sektoren der Festplatte. Dateien bleiben von ihm gänzlich unberührt.

Bei der Infektion kopiert er sich selbst in den Bootsektor und verschiebt die Originaldaten und einen Verweis in die letzten 2 Sektoren. Sollten diese später vom Benutzer überschrieben werden, ist die Bootinformation futsch und der Computer läßt sich nicht mehr ordnungsgemäß starten.
Weiters infiziert der Virus Disketten.

Indikatoren einer Infektion:
*) Bei jedem Tastendruck an dem 18. Tag eines jeden Monats ertönt ein Klickgeräusch.
*) Das System kann durch einen nichtgeglückten Festplattenzugriff abstürzen.

*) Der Form-Virus benötigt 2k an Arbeitsspeicher. Dies läßt sich durch den DOS-Befehl MEM feststellen.
*) Der DOS-Befehl CHKDSK stellt außerdem 1,024 Bytes an zerstörten Sektoren fest, in denen der Originalbootsektor gespeichert ist.
*) Im Viruscode steht folgender Text :"The FORM-Virus sends greetings to everyone who's reading this text. FORM doesn't destroy data! Don't panic! (Expletive) go to Corrine."

Methode der Infektion:
Ein System kann nur durch das Booten von einer infizierten Diskette befallen werden. Auch wenn die Diskette nicht bootable ist und er DOS-Text:"Non-system disk or disk error" erscheint ist der Bootsektor der Festplatte bereits infiziert.
Bei jedem folgenden Systemstart wird der Virus in den Arbeitsspeicher geladen und kann bei jedem Floppy-Disk-Zugriff deren Bootsektor infizieren und sich so verbreiten.

Virus Daten:

Datum der Entdeckung:	Juni 1990
Herkunftsland:	Schweiz
Länge:	512 Bytes
Typ:	Bootsektorvirus, speicherresidenter Virus
Häufigkeit:	oft, weitverbreitet

b) "Friday 13th" – Virus:

Charakteristik:
Der Friday 13th Virus ist ein Programmvirus. Er infiziert .COM-Dateien außer der COMMAND.COM. Bei jedem Start des Virus werden 2 neue .COM Dateien auf der Festplatte und eine neue auf dem A: Laufwerk gesucht und – falls vorhanden – infiziert.

Indikatoren der Infektion:
*) Das Leuchten des Diskettenzugrifflämpchens im Floppy-Disklaufwerk, hervorgerufen durch die Suche des Virus nach neuen Wirtdateien auf dem A: Laufwerk, ist der einzige Indikator der Infektion.
*) Bei einem Computerstart an einem Freitag 13. wird die COMMAND.COM gelöscht.

Methode der Infektion:
Durch das Ausführen einer infizierten Datei wird der Virus gestartet und verbreitet.

Virus Daten:

Datum der Entdeckung:	November 1987
Herkunftsland:	Rep. Südafrika
Länge:	512 Bytes
Typ:	Programmvirus
Häufigkeit:	selten

c) "Cascade" – Virus:

Charakteristik:
Der Cascade Virus ist ein überschreibender Programmvirus und speicherresident. Er infiziert im speziellen .COM-Dateien.

Indikatoren der Infektion:

*) Zwischen dem 1. und 31. Oktober 1988 führte der Cascade Virus seine Aufgabe aus. Diese gestaltete sich so, daß, kurz nach dem Start des infizierten Programmes, alle Buchstaben auf dem Bildschirm auf den unteren Bildschirmrand fallen und dort einen Haufen bilden.

Methode der Infektion:

Durch das Ausführen einer infizierten Datei wird der Virus gestartet und verbreitet.

Virus Daten:

Datum der Entdeckung:	Oktober 1987
Herkunftsland:	Deutschland
Länge:	1701 oder 1704 Bytes
Typ:	Programmvirus, speicherresident
Häufigkeit:	oft, weitverbreitet

Es wurden Grafiken aufgrund des hohen Platzbedarfs (4 Mb) entfernt!
Wir bitten Sie daher, falls Sie die Grafiken benoetigen, sich an den Autor zu wenden