Geschichte der Computer-Viren

1980 verfaßte Jürgen Kraus am Fachbereich Informatik der Universität Dortmund eine Diplomarbeit mit dem Titel "Selbstreproduktion bei Programmen". In dieser Arbeit wurde zum ersten Mal auf die Möglichkeit hingewiesen, daß sich bestimmte Programme ähnlich wie biologische Viren verhalten können. Der Verfasser schilderte die Konstruktion möglichst einfacher selbstreproduzierender Programme, ging aber nicht auf das Problem der IT-Sicherheit ein. Die Arbeit wurde nicht veröffentlicht und verschwand im Archiv der Universität.

1984 veröffentlichte der Amerikaner Fred Cohen seine Arbeit mit dem Titel "Computer Viruses - Theory and Experiments". Da er insbesondere auf die Gefahren einging, die Computer-Viren für Rechner darstellen können, erregte seine Untersuchung auch internationales Aufsehen. Cohen ist auch die Definition des Begriffs Computer-Virus zu verdanken:

A "computer virus" is a program that can "infect" other programs by modifying them to include a possibly evolved version of itself.

Es dauerte nicht lange, bis aus der theoretischen Bedrohung eine praktische Gefahr für die Betreiber von Computern werden sollte. Hauptsächlich betroffen waren Rechner, deren Betriebssysteme keinen oder nur sehr ungenügenden Schutz in Bezug auf IT-Sicherheit boten. Dazu gehörten in erster Linie die Personalcomputer.

1986 erschienen zum ersten Mal auf IBM-kompatiblen Personalcomputern Computer-Viren. Diese Viren waren recht einfach gebaut und konnten anhand fester Zeichenfolgen entdeckt werden, die im Programm-Code zu finden waren. Häufig handelte es sich dabei um Viren, die zu irgendeinem bestimmten Zeitpunkt eine Meldung ausgeben sollten. Man brauchte also nur nach solchen Meldungstexten zu suchen, um den Virus zu entdecken.

Da solche sogenannten "Scan"-Codes auch veröffentlicht wurden, dauerte es nicht lange, bis die ersten Viren auftauchten, die den Virus-Code verschlüsselten. Das hatte zur Folge, daß nach Textausgaben von Viren nicht mehr einfach gesucht werden konnte, da diese Texte jedesmal anders verschlüsselt abgelegt wurden. Zum Glück blieb der Code der Verschlüsselungsroutine bei jedem Virus gleich, so daß man wenigstens danach suchen konnte. Die Anzahl der Bytes, die für einen bestimmten Virus typisch waren, verringerte sich jedoch entscheidend.

Die nächste Stufe waren dann die " Stealth "- Viren. Diese Viren nutzten spezielle Eigenschaften des Betriebssystems aus, indem bestimmte Systemaufrufe abgefangen und verfälscht ausgegeben wurden. So konnten diese Viren in einem infizierten System zum Beispiel die alte Programmlänge vortäuschen oder dem Benutzer statt bestimmter geänderter Sektoren der Festplatte die Original-Sektoren vorspiegeln, die der Virus an eine andere Stelle verschoben hatte.

So richtig schwierig wurde es dann, als 1990 die ersten sogenannten polymorphen Computer-Viren auftauchten. Soll ein Programm eine bestimmte Funktion erfüllen, so kann man dafür die verschiedensten Befehle in der unterschiedlichsten Anordnung verwenden. Zur Verdeutlichung ein Vergleich: Nehmen wir an, daß durch Addition von Zahlen ein bestimmter Wert, z.B. 19, erreicht werden soll. Hierzu kann man auf verschiedene Weise vorgehen: 9+10 oder 9+9+1 oder 1+9+0+9 oder 7+8+9+1-8+9-7 und so weiter. Diese neuartigen Viren funktionieren ganz ähnlich; sie verwenden entweder verschiedene Befehle oder sie ordnen Befehle anders an, bisweilen tun sie sogar beides. Wird dies geschickt genug gemacht, ergeben die unterschiedlichsten Programm-Codes die gleichen Virus-Funktionen. Um einen derartigen Virus zu entdecken, genügt es nicht mehr, nur nach bestimmten Zeichenfolgen zu suchen. Nur ein algorithmisches Verfahren, das nach bestimmten Eigenschaften des Virus sucht, führt dann noch zum Erfolg.

Zusätzliche Probleme bei der Bekämpfung der Computer-Viren ergaben sich aus dem Umstand, daß in Zeitschriften und Büchern Programm-Codes für Viren abgedruckt wurden, so daß auch Personen mit sehr wenig Erfahrung im Programmieren in die Lage versetzt wurden, durch Abtippen der Befehle selbst neue Viren zusammenzubasteln und zu verbreiten. Schon bald darauf nahmen sogenannte "Viren-Baukästen" dem Virus-Programmierer sogar noch die Arbeit des Abtippens ab. Es handelt sich dabei um Programmsysteme, die durch einfaches Ankreuzen von vorgegebenen Menü-Punkten einen neuen Virus zusammensetzen konnten.

Die neueste Bedrohung ist die "Mutation Engine", kurz "MtE" genannt. Man benötigt dazu lediglich einen einzigen fertigen Virus, und nach dessen Behandlung mit diesem Programmsystem entstehen Millionen von verschiedenen Varianten.

Bisher waren die Programmierer von Anti-Virus-Software in der Lage, den Vorsprung der Viren-Programmierer im Wettlauf mit der Zeit immer relativ rasch einzuholen. Es ist aber zu befürchten, daß die Zeitspanne zwischen Auftreten eines neuen Virus und der Erstellung des passenden Gegenmittels immer länger wird.

Häufig wird die Frage gestellt, wer eigentlich Computer-Viren programmiert. Dieser Personenkreis reicht vom Schüler, der seinem Freund einen Streich spielen will und deshalb einen Virus in die Welt setzt, der Buchstaben durcheinanderpurzeln läßt oder nervierende Musik auf dem Lautsprecher des Personalcomputers spielt, über das verkannte Genie, das glaubt, auf diese Weise seine Programmierkunst beweisen zu müssen, bis hin zum "Techno"-Terroristen, der möglichst viel Schaden anrichten will.

Definition von Virus und den Grundtypen

- ***Virus***

Nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen (payload, damage) des Virus vorhanden sein.)

- **Boot-Virus**

Der Virus befindet sich im Boot-Sektor einer Diskette bzw. Festplatte. Der Virus wird durch einen Kalt- oder Warm-Start (bzw. bei Daten-Disketten auch erfolglosem Boot-Versuch) aktiviert.

- **File-Virus**

Der Virus ist in einem Programm (Wirtsprogramm) enthalten und wird nur durch Aufruf dieses Programms aktiviert.

- **Makro-Virus**

Während sich die vorgenannten Viren anstelle von Programmcode einnisten, benutzen Makro-Viren Steuersequenzen von Daten-Dateien als Wirt. Moderne Programme erlauben es, häufig benötigte Steuerinformationen, z.B. zum Layout von Texten, mittels einfach erlernbarer Programmiersprachen zu erstellen. Dies kann zur Programmierung von Computer-Viren missbraucht werden, die beim Arbeiten mit den Daten-Dateien automatisch ablaufen. Sofern die Hauptprogramme auch für andere Betriebssysteme als MS-DOS angeboten werden, können auch die damit programmierten Viren plattformübergreifend arbeiten. Makro-Viren haben in den letzten Jahren starke Verbreitung gefunden.

Unterarten und Zusatzfunktionen von Viren

- ***Companion-Virus***

Virus nutzt die Hierarchie des Betriebssystems beim Aufruf von Programmen aus und erzeugt namensgleiche Dateien mit seinem Code, die bei Aufruf des Programms dann zuerst ausgeführt werden (z.B. FORMAT.COM zusätzlich zu FORMAT.EXE).

- ***logische Bombe***

Manchmal Bezeichnung des Sonderfalls eines Trojanischen Pferdes: Programm, dessen Scahdensfunktion von einer logischen Bedigung gesteuert wird, z.B. dem Datum; der Spezialfall einer zeitlichen Bedingung wird auch als "Zeitbombe" *(time bomb)* bezeichnet.

- ***Multipartite-Virus***

Virus, der sich über verschiedene Ausprägungen seines Wirtes verbreiten kann (z.B. sowohl als Boot-Virus als auch als File-Virus

- ***Programm mit Schadensfunktionen (malicious software)***

Alle Arten von Programmen, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige Veränderungen unkontrollierbare Schäden an Programmen und Daten bewirken und somit zusätzliche Arbeit und Kosten verursachen oder Vertraulichkeit und Verfügbarkeit von Daten oder Programmen negativ beeinflussen.

- ***residenter Virus***

Virus, der nach Aktivierung bis zum Ausschalten des Rechners im Hauptspeicher aktiv bleibt.

- ***selbstverschlüsselnder Virus (selbstkryptierender Virus)***

Virus verschlüsselt (kryptiert) seinen Code mit festem oder wechselndem Schlüssel.

- ***Tarnkappen-Virus (Stealth-Virus)***

Residenter Virus, der seine Anwesenheit im infizierten System durch Manipulation des Betriebssystems zu verbergen versucht.

- ***Trojanisches Pferd***

Selbständiges Programm mit einer verdeckten Schadensfunktion, ohne Selbstreproduktion.

- ***Wurm***

Selbständiges, selbstreproduzierendes Programm, das sich in einem System (vor allem in Netzen) ausbreitet.

Falsche Virenmeldungen: Hoaxes

Mittels E-Mail werden seit ca. 5 Jahren häufig "Virus-Meldungen" verschickt, die vor einem "ganz neuen, gefährlichen" Virus warnen, der schon beim bloßen Lesen einer E-Mail aktiviert wird und sofort Daten löscht oder die Festplatte formatiert.

Die Meldungen stimmen jedoch nicht, sie sollen nur ungeschulte Computernutzer bei ihrer Hilfsbereitschaft und Gutmütigkeit ansprechen und zu schädlichen Aktionen veranlassen.

Eine solche Meldung wird deshalb als *Hoax* (englisch für Zeitungsente) bezeichnet. Man muß dazu wissen, daß jeden Monat ca. 300 neue Viren und ähnliche Schadsoftware bekannt werden, die nicht gefunden werden, solange sie "ganz neu" sind. Nach ca. 2 Tagen haben die Hersteller von Anti-Virus-Software die Erkennung in Ihre Programme eingebaut. Würde für jeden neuen Virus eine Warnung verbreitet...

Der Anwender kann Hoaxes an vier charakteristischen Merkmalen erkennen:

- Es wird dazu aufgefordert, die Meldung an möglichst viele andere Nutzer zu verteilen.
- Es handelt sich um einen Virus der so neu ist, daß kein Anti-Viren-Programm in momentan findet, und er löscht schon beim Lesen der E-Mail sofort Daten.
- Die Information stammt von einer Autorität. (Beispiele: Microsoft, AOL, Polizei, Rundfunk)
- Die originale E-Mail-Adresse des ursprünglichen Absender oder eine konkrete WWW-Adresse ist nicht vorhanden.

Der Name der gefährlichen Datei ist das Einzige, was ständig verändert wird.

Die Meldung darf ***nicht*** sofort weiter geleitet werden. Wenn jeder Anwender dies tun, wird das E-Mail-System überlastet und blockiert. Das ist die Schadensfunktion, die der anonyme Urheber der Meldung bezweckt.

Im Normalfall ist der behauptete Sachverhalt frei erfunden.

Maßnahmen:

Anwender
Alle Virus-Meldungen zur Kenntnis nehmen und anschließend sofort löschen. **Nicht** weiterleiten, **nicht** den Systemadministrator oder Benutzerdienst anrufen und nachfragen!

Systemadministrator
Die Meldung auf die obigen Merkmale prüfen. Treffen auch nur einige davon zu, so handelt es sich um einen Hoax. Andernfalls sollte auf den Internetseiten des Herstellers oder Lieferanten der benutzten Viren-Schutz-Software geprüft werden, ob dort schon Gegenmittel oder weitere Informationen bereit stehen. Die sogenannten News-Ticker der Computer-Zeitschriften im Internet veröffentlichen solche Informationen ebenfalls frühzeitig.

Beispiel für eine Hoax E-Mail

Name: **Sulfnbk.exe**
Alias: **Tha Rippa**
Art: **Hoax**
Betriebssystem: **Microsoft Windows**
Verbreitung: **Meldungen aus Europa und USA**
Risiko: **mittel (wenn genannte Datei gelöscht wird)**
Handlungsbedarf:
nein
Schadensfunktion:
Überlastung des E-Mail Sytems

**** Beginn ****

Hallo ihr Lieben!
bitte mal Systeme checken... das ist kein fake oder Scherz!
Nach einer Warnung vor einem "schlafenden Virus" habe i c h diesen Virus auf meinem Rechner gefunden und jetzt gelöscht - ohne ihn zu öffnen! Er wird wohl von vielen Virenprogrammen nicht erkannt und aktiviert sich zu einem späteren Zeitpunkt. Er verbreitet sich durch Emails, infiltriert

C:\Windows\command und löscht - wenn er sich aktiviert - alle Dateien/Ordner auf der Festplatte.

Ich bitte alle, die in den letzten Monaten von mir eine mail bekommen haben, ihn zu suchen und ggf. zu löschen. Dabei wie folgt verfahren:

Auf "Start" klicken
dann "Suchen"
"Dateien/Ordner"
Name: SULFNBK.EXE
Suchen in: "C"

Ist der Re chner infiziert erscheint die Datei im Ergebnisfeld.
AUF KEINEN FALL ÖFFNEN! (durch Doppelklick oder ausführen)
sondern wie folgt verfahren:

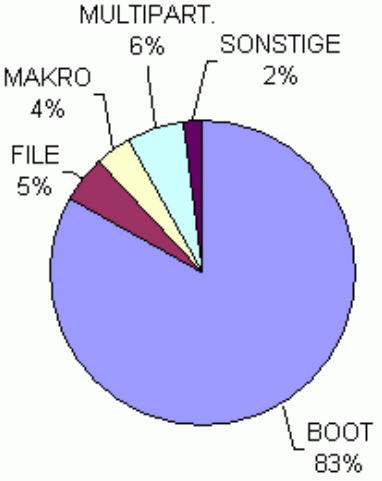
"Bearbeiten"
"Alles Markieren" (es steht nur diese Datei im Ergebnisfeld) und die Datei löschen.

Dann auf jeden Fall noch den Papierkorb leeren.
Wenn die Datei gefunden wurde, alle Empfänger/Innen von Emails der letzten Monaten informieren.

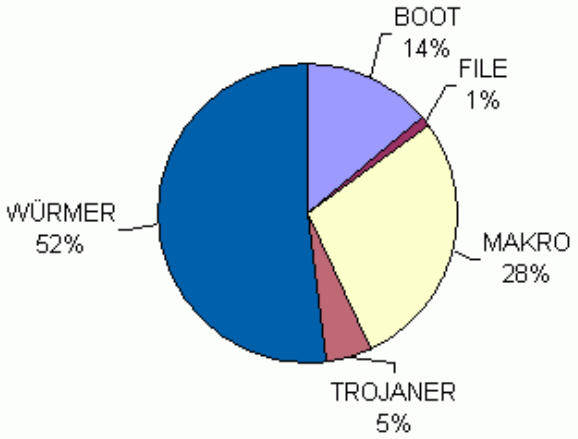
Diese Virenwarnung hab ich auch von anderen bekommen. Ich hatte den Virus auch. Also bitte Ernst nehmen und weiterleiten.

Habe den Virus eben gelöscht!!!! Unter Garantie habt ihr den auch!
Also seht nach. Geht ganz schnell!

Verteilung der Virentypen 1996 in prozent:



Verteilung der Virentypen 2001 in Prozent:



Aufbau eines Computer-Virus

- **Reproduktionsteil**
- Mit diesem Programmteil wird die Vermehrung des Virus durchgeführt.
- **Erkennungsteil**
- Im Erkennungsteil wird geprüft, ob bereits die Infektion eines Programms oder Systembereichs erfolgte. Die Verbreitung wird beschleunigt, wenn der Virus auf eine Infektion "verzichten" kann, weil sie bereits geschehen ist. Jedes Wirts-Programm wird daher nur einmal infiziert. Die Entdeckung wird damit auch verzögert, da durch mehrfache Anlagerung des Virus-Codes die Dateien sonst so groß werden, daß sie entweder nicht mehr ausführbar sind oder aber dem Benutzer die Größenveränderung schneller auffällt.
- **Schadensteil**
- In einigen Viren ist absichtlich eine Schadensfunktion programmiert, meist das Überschreiben oder Verändern von Programmen oder Daten, oder aber auch nur die Ausgabe von Meldungen und Geräuschen auf dem Rechner. Dieser Programmteil kann fehlen, aber auf jeden Fall entsteht Schaden durch Inanspruchnahme von Speicherplatz im Hauptspeicher und auf Datenträgern. Durch Programmierfehler, Veränderungen des Betriebssystems oder ähnliches können weitere Schäden als Nebeneffekte auch dann auftreten, wenn sie nicht absichtlich programmiert sind
- **Bedingungsteil**
- Sowohl die Verbreitung als auch die Schadensfunktion können von Bedingungen abhängig programmiert sein, z.B. tritt bei einigen Viren der Schaden an einem bestimmten Datum (z.B. Michelangelo-Virus) oder bei einer bestimmten Anzahl von Aufrufen ein. Auch dieser Teil kann fehlen.
- **Tarnungsteil**
- Hierunter fallen Programmroutinen, um die Entdeckung des Virus im infizierten System zu erschweren. Dieser Teil ist meist nur bei neueren Viren zu finden.

Obwohl Computer-Viren prinzipiell bei jedem Computertyp und Betriebssystem denkbar sind, erlangten sie PC's die größte Bedeutung. Bei den hier am meisten verbreiteten Betriebssystemen (MS-DOS, Windows) wurden Anfang 1994 weltweit rund 4000 Viren (einschließlich Varianten) gezählt. Entsprechend vielfältig sind weitere Merkmale und Eigenschaften.

Infektion des Systems

- **durch Boot-Viren**

  Boot-Viren werden durch einen Boot-Vorgang mit infizierten Disketten verbreitet. Nach dem Rechnerstart von einer infizierten Diskette wird der Virus sofort im Speicher resident und auf die Festplatte *C:* übertragen. Meist werden dann alle nicht schreibgeschützten Disketten, die man in diesem infizierten Computer anschließend benutzt, ebenfalls infiziert, da ein Boot-Sektor auf jeder Diskette vorhanden ist. Deshalb kann auch der Boot-Versuch von einer vergessenen Daten-Diskette eine Infektion bewirken.

  Wenn man nach der Fehlermeldung (z.B.):

- "Kein System oder Laufwerksfehler Wechseln und Taste drücken"

  die Diskette entfernt, kann die Festplatte schon infiziert sein. Man sollte deshalb grundsätzlich auch Daten-Disketten, die man von anderen erhält, auf Virus-Befall prüfen.

- **durch File-Viren**

  File-Viren werden durch Aufruf eines infizierten Programmes, z.B. von einer Diskette oder CD, aktiviert. Infizierte Programme können aber auch über andere Medien, wie z.B. Datenübertragung per Modem oder vom File-Server eines Netzwerkes, in den Computer eines Anwenders gelangen. Jedoch erst nach dem Aufruf eines infizierten Programms können andere Programme oder Systembereiche auf anderen Datenträgern infiziert werden. Durch Prüfung aller neu beschafften Programme vor dem ersten Aufruf mit einem aktuellen Viren-Suchprogramm kann man die Gefahr vermindern.

Geschichte des Michelangelo-Virus

Immer wieder tauchen in der Presse Meldungen über Computer-Viren auf. Den größten Wirbel dürfte Anfang 1992 der "Michelangelo"-Virus verursacht haben, der damit sicher der weltweit bekannteste Computer-Virus wurde.

Am 4. Februar 1991 entdeckte ein Computerhändler in Melbourne, Australien, daß bei der Installation eines Anti-Viren-Programms auf einem Rechner merkwürdige Meldungen erschienen. Die Untersuchung einer infizierten Diskette durch Roger Riordan von der Firma CYBEC ergab, daß es sich um einen neuen Boot-Virus handelte. Die Analyse zeigte weiterhin, daß dieser Virus am 6. März jeden Jahres die Festplatte mit willkürlichen Zeichen überschreiben sollte. Die Quelle des Virus war mit hoher Wahrscheinlichkeit Software aus Taiwan. Als Roger Riordan einen Freund wenige Tage später vor diesem Virus warnte und auf das Auslösedatum 6. März hinwies, meinte dieser: "Oh, das ist mein Geburtstag." Er wußte, daß auch der berühmte italienische Künstler Michelangelo an diesem Tag geboren war. So kam der Virus zu dem Namen "Michelangelo".

Der "Michelangelo"-Virus ist eine Abart des weit verbreiteten "Stoned"-Virus. Er gehört zur Klasse der einfachen Viren, d.h., er weist keine Besonderheiten, wie "Stealth"-Funktion, auf. Er enthält auch keinerlei Buchstabenfolge mit "Michelangelo", mit der man ihn sofort identifizieren könnte. Auf einer einwandfreien Diskette ist im Boot-Sektorder Name und die Version des Betriebssystems zu finden, sowie der Text von Fehlermeldungen, die ausgegeben werden, wenn irrtümlich eine Daten-Diskette im Rechner beim Start vergessen wurde. Bei einer infizierten Diskette fehlen die Angaben über das Betriebssystem, außerdem ist der Text der Fehlermeldungen verstümmelt. Der Original-Boot-Sektor wird in den letzten Sektor des Hauptverzeichnisses ausgelagert, was bei Disketten mit sehr vielen Dateien zur Überschreibung der Dateinamen und damit zu Datenverlust führt.

Eine Hauptquelle der Verbreitung waren Treiber-Disketten zu Bildschirmkarten und Maus-Eingabegeräten, vorwiegend aus dem ostasiatischen Raum (Taiwan, Hongkong, Singapur etc.).

Aufgrund des Namens "Michelangelo" griffen die Medien den Sachverhalt auf und riefen durch teilweise reißerische Berichterstattung nahezu eine Panik unter den PC-Anwendern hervor. Es bildeten sich Menschenschlangen vor Geschäften, die kostenlose Entdeckungsprogramme für den "Michelangelo"-Virus anboten.

Insgesamt gingen bis zum Aktivierungszeitpunkt, dem 6. März, rund 800 Meldungen, die 1300 einzelne Computer betrafen, über die Entdeckung des Michelangelo-Virus ein. Wenn man als Untergrenze von einer zehnfachen Dunkelziffer ausgeht, so wurde in der Bundesrepublik mindestens bei 13.000 PCs der Virus rechtzeitig erkannt und entfernt.

Nach dem Auslösetag gab es Meldungen von 150 einzelnen Computern, bei denen Michelangelo "erfolgreich" die Daten einer Festplatte vernichtet hatte. Auch hier ist wieder von einem Verhältnis von mindestens 1 zu 10 von gemeldeten zu tatsächlichen Fällen auszugehen, d.h. bei etwa 1500 PCs gab es totalen Datenverlust auf Festplatten. Lag keine aktuelle Datensicherung vor, gab es für einige Benutzer am 6. März 1992 ein böses Erwachen.

Als positives Ergebnis des Falles "Michelangelo" bleibt festzuhalten, daß erstens die Viren-Problematik einer breiten Öffentlichkeit bewußt wurde, zweitens die Notwendigkeit einer aktuellen Datensicherung erkannt wurde und drittens viele andere Computer-Viren anläßlich der Suche nach "Michelangelo" zufällig entdeckt wurden.

"Michelangelo" übt seine zerstörerische Tätigkeit als echter "Geburtstags-Virus" jedes Jahr am 6.März aus.

Der "Michelangelo"-Virus ist jedoch ein Boot-Virus und kann sich nur über Disketten verbreiten. Da der Zeitpunkt seiner Programmierung vermutlich Anfang 1991 war, war dem unbekannten Autor nur die Existenz der 5,25"-Disketten vertraut und nur dieser Disketten-Typ wird "einwandfrei" infiziert. Bei den 3,5"-Disketten werden die Disketten mit doppelter Dichte (DD, 720 KB) nicht infiziert. Die Disketten mit hoher Dichte (HD, 1,44 MB) werden zwar infiziert, können jedoch anschließend von den Betriebssystem MS-DOS nicht mehr gelesen werden.

Es erscheint dann die Fehlermeldung (z.B.):

"**Allgemeiner Fehler beim Lesen von Laufwerk A**"

Dadurch ist in vielen Fällen der Virus vor dem Schadensdatum entdeckt worden.

Wenn der Rechner mit solch einer infizierten Diskette (auch Daten-Diskette) gestartet wird, kann er dennoch infiziert werden. Dies hat dann zur Folge, daß jede 3,5"-HD-Diskette im Start-Laufwerk (A:), die nicht schreibgeschützt ist, bei ihrer Verwendung infiziert wird und damit nicht mehr vom Betriebssystem gelesen werden kann.

Aufgrund der großen Verbreitung der 3,5"-Disketten, die die 5,25"-Disketten nahezu abgelöst haben, ist dem "Michelangelo"-Virus damit der wichtigste "Wirt" für die Verbreitung entzogen worden, so daß ab 1995 nur noch in Einzelfällen bei alten Rechnern, die über ein 5,25"-Start-Laufwerk (Laufwerk A:) verfügen, tatsächlich noch Schäden auftraten.

"Michelangelo "-Virus

Namensgebung: Die Schadensfunktion des Virus wird am 6. März aktiv, dem Geburtstagvon Michelangelo.

Virus-Art: Boot-Virus

Beschreibung: Der Virus speichert sich in den Boot-Sektor von Disketten und in den Partition-Sektorvon Festplatten. Der originale Boot-Sektor bzw. Partition-Sektor wird gesichert. Bei Disketten wird dieser Sektor am Ende des Hauptverzeichnisses abgelegt. Sind dort Verzeichnis-Einträge vorhanden, werden diese überschrieben; dadurch kann es zu Datenverlusten während der Infektion kommen.

Wird der Rechner am 6. März gestartet, überschreibt der Michelangelo-Virus wichtige Systembereiche und Dateien. Die Festplatte des Rechners muß dann neu eingerichtet werden, die Daten sind in der Regel verloren - vor allem dann, wenn nur eine Partition (nur C:) eingerichtet ist.

Infektion

- **der Festplatte:** Die Infektion erfolgt über Booten (bzw. Boot-Versuch) von einer infizierten Diskette.
- **des Arbeitsspeichers:** Während des normalen Systemstarts über die infizierte Festplatte wird der Virus speicherresident. Im infizierten System werden 2048 Bytes Arbeitsspeicher weniger angezeigt.
- **der Diskette:** Im infizierten System versucht der Virus jede Diskette im Laufwerk A: zu infizieren, auf die zugegriffen wird. Ist der Disketten-Schreibschutz aktiv, so bricht der Virus den Versuch ab. Disketten im Laufwerk B: werden nicht infiziert.

Besonderheit bei 3,5" Disketten:

720 KB-Disketten werden nicht infiziert.
1,44 MByte-Disketten sind nach der Infektion nicht mehr lesbar.

Intakter Boot-Sektor einer Diskette(ausschnitt):

```
000000      ·<·MSDOS5.0·····
000010      ···@·····
000020      ·····)··H·VOLUM
000030      E-NAMEFAT12   ·3
000040      ·····|···x·6·7·V
        . . . . . . .
        . . . . . . .
        . . . . . . .
000190      ·····$|·6%|·····
0001A0      Kein System oder
0001B0       Laufwerksfehler
0001C0      ··Wechseln und T
0001D0      aste drücken···I
0001E0       O      SYSMSDOS
0001F0        SYS·····U·
```

Befallener Boot-Sektor einer Diskette(ausschnitt):

```
000000      ·····.···P
000010      ··u·3·····?··u·X
000020      ··.·····X
000030      ·.·.··PSQR··VW··
000040      ·····3·
        . . . . . . .
        . . . . . . .
        . . . . . . .
000190      ·····r·····!
0001A0      ·····3·····
0001B0      ·····er
0001C0      ··Wechseln und T
0001D0      aste drücken···I
0001E0       O      SYSMSDOS
0001F0        SYS·····U·
```

"Hare"-Virus

Namensgebung: "Hare" im Virus-Programm verschlüsselt enthalten.

Virus-Art: multipartite

Beschreibung: "Hare" ist ein residenter , mulitpartite Virus mit polymorpher Verschlüsselungs-Technik.

Der Virus infiziert COM- und EXE-Dateien, den Partition-Sektor von Festplatten und den Boot-Sektor von Disketten. Infizierte Objekte werden verschlüsselt. Hare infiziert keine Dateien, die mit "TB" oder "F-" beginnen oder den Buchstaben "V" im Datei-Namen haben. Dadurch werden die meisten Anti-Viren-Programme nicht infiziert, was ansonsten durch deren Selbstüberprüfungsmechanismus zu einer frühen Entdeckung des Virus führen würde.

Bei einigen Computern wird bei der Infektion der Inhalt der Partition-Tabelle zerstört. Der Virus kopiert sich hinter das Ende des von DOS erreichbaren Festplatten- bzw. Disketten-Bereichs. Aufgrund der zerstörten Partition-Tabelle darf der Befehl **" FDISK /MBR "** ***keinesfalls*** eingesetzt werden!

Wird ein infizierter Rechner am 22. August oder 22. September gestartet, so erscheint die Virus-Meldung:

"HDEuthanasia" by Demon Emperor: Hare Krsna, hare, hare...

Danach versucht "Hare" den Festplatten-Inhalt zu überschreiben.

Der "Hare"-Virus wurde über Newsgruppen des Internet verteilt und sorgte im Frühjahr 1996 für eine gewisse Hysterie in den Medien, obwohl - im Gegensatz zum " Michelangelo"-Virus - kaum Schadensfälle gemeldet wurden. Dies ist auch auf einige Programmierfehler des Virus-Autors zurückzuführen, die zu einer frühen Entdeckung der Infektion führten und damit glücklicherweise eine größere Verbreitung verhinderten.

Infektion

- **der Festplatte:** Die Infektion erfolgt entweder über Booten (bzw. Boot-Versuch) von einer infizierten Diskette, oder durch Ausführen eines infizierten Programms.
- **des Arbeitsspeichers:** Der Virus wird speicherresident, wenn der infizierte Rechner gestartet wird, oder ein infiziertes Programm ausgeführt wird.
- **von Disketten:** Nach dem Start eines infizierten Rechners versucht der Virus jede Diskette zu infizieren, auf die zugegriffen wird. Ist der Disketten-Schreibschutz aktiviert, so bricht der Virus den Versuch ab.
- **von Programmen:** Ist der Virus speicherresident, werden COM- und EXE-Dateien bei ihrer Ausführung infiziert

Viren bei Linux

Das Betriebssystem LINUX ist eine auf IBM-kompatiblen PC lauffähige UNIX-Variante, die Hardware ist mit der bei MS-DOS-Rechnern identisch. Zusätzlich zum Betrieb von DOS- und Windows-Programmen in Emulatoren werden häufig beide Betriebssysteme, LINUX und MS-DOS in getrennten Teilen der Festplatte auf dem jeweiligen Rechner installiert. Beim Booten kann man eines der beiden Betriebssysteme auswählen. Dadurch bestehen unter DOS/Windows die gleichen Gefahren durch DOS-Datei-Viren wie bei reinen DOS-Rechern. Unter LINUX laufen einige wenige dieser Viren im DOS-Emulator. LINUX verwendet ein anderes Dateisystem und eine andere Speicherverwaltung, dadurch funktionieren modernere Viren nicht, die mit aufwendigen Eingriffen in das Betriebssystem MS-DOS ihre Anwesenheit im System verbergen wollen. Unter LINUX ist es möglich, durch das sogenannte "Mounten" das DOS-Dateisystem mit seinen Dateien in die Arbeit einzubeziehen. Dadurch können DOS-Viren auch auf LINUX-Festplatten bzw. -Partitionen gespeichert sein, auf die übliche DOS-Viren-Suchprogramme nur unter den Emulatoren von LINUX Zugriff haben. Ein Suchlauf sollte daher nicht nur durchgeführt werden, wenn DOS gebootet wurde, weil dann die Suche auf die DOS-Platte begrenzt ist, sondern ggf. auch unter einem LINUX-DOS-Emulator.

Schäden durch Computer-Viren

Computer-Viren verursachen mittlerweile allein in der Bundesrepublik Deutschland jährlich Schäden in dreistelliger Millionenhöhe - mit steigender Tendenz. Die Schäden lassen sich verschiedenen Bereichen zuordnen:

Beabsichtigte, programmierte zerstörerische Schadensfunktionen

Ein geringer Teil - man schätzt rund 5 Prozent der bekannten Computer-Viren - sind echte Daten-Killer, die durch absichtsvoll programmierte Schadensfunktion darauf aus sind, möglichst umfassend Schäden auf Datenträgern, insbesondere Festplatten, anzurichten.

Unbeabsichtigte Seiteneffekte bei angeblich harmlosen "Scherz-Viren"

Eine Vielzahl von vermeintlich harmlosen "Scherz-Viren", die eigentlich den Anwender nur durch "witzige" Meldungen auf dem Bildschirm oder die Ausgabe von Geräuschen bzw. Melodien über den Lautsprecher des Rechners ärgern wollen, weisen unbeabsichtigte Seiteneffekte auf, die aufgrund von Programmierfehlern oder auch Änderungen im Betriebssystem dann zu Datenverlusten führen. Viele Boot-Viren lagern den originalen Boot-Sektor im letzten Sektor des Hauptverzeichnisses von Disketten aus, ohne zu überprüfen, ob hier eventuell Einträge von Dateien oder Unterverzeichnissen stehen.

Der Zugriff auf die zugeordneten Daten ist dann nur noch durch erfahrene Spezialisten möglich.

Inanspruchnahme von Speicherplatz im Hauptspeicher und auf Datenträgern

Die direkten Schäden durch einen Virus - ob beabsichtigt oder nicht - haben sicher den geringsten Anteil an der Schadenshöhe. Jeder Virus verursacht aber immer Schaden, da er Speicherplatz auf Datenträgern und auch im Hauptspeicher in Anspruch nimmt. Der Rechner wird langsamer, weil zusätzlich ein Computer-Virus alle Schreib- und Lese-Zugriffe kontrolliert, um sich weiter ausbreiten zu können. Bei Datei-Viren vergrößern sich die Programme um Hunderte oder auch Tausende von Bytes.

Materieller und personeller Aufwand beim Suchen und Entfernen

Den größten Anteil bei der Zurechnung der Schäden ergiben sich aus dem Aufwand, der materiell wie personell entsteht, um nach Computer-Viren zu suchen und sie gegebenenfalls auch zu entfernen. Rechner können solange nicht benutzt werden, bis der Virus beseitigt ist. Unverseuchte Programm-Versionen müssen eingespielt oder vielleicht muß sogar eine vollständige Neu-Installation von Betriebssystem, Anwendungs-Software und gesicherten Datenbeständen vorgenommen werden. Alle Datenträger, die in einem infizierten Rechner benutzt worden sind, sind zu überprüfen. Gegebenenfalls müssen Dritte informiert werden, daß unbeabsichtigt infizierte Disketten weitergegeben wurden. Alle diese zusätzlichen Arbeiten, die notwendig sind, um einen Virus aufzuspüren und zu vernichten, schlagen sich natürlich in Personal- und Material-Kosten nieder.

Zusätzlich zu ergreifende organisatorische Abwehr-Maßnahmen

Nicht zu vernachlässigen sind auch die Kosten, die durch zusätzlich zu ergreifende organisatorische Abwehr-Maßnahmen bei Firmen und Behörden entstehen. Mitarbeiter müssen geschult werden, Anti-Virus-Software muß gekauft und regelmäßig aktualisiert werden sowie zusätzliche Überprüfungsabläufe in den Organisationsablauf eingebunden werden.

Panik-Reaktionen von Anwendern

Anwender, die erstmalig die Meldung durch ein Anti-Viren-Produkt bekommen, daß ihr Rechner infiziert ist, haben durch unüberlegte panische Reaktionen mehr Schaden angerichtet, als dies der Computer-Virus auch unter ungünstigen Umständen hätte verursachen können. Obwohl es genügt hätte, die infizierten Programme durch die unverseuchten Originale zu ersetzen, wurden Festplatten formatiert (was niemals nötig ist!), ohne daß eine aktuelle Datensicherung vorhanden war.

Vorbeugende Maßnahmen

- Regelmäßig Datensicherung durchführen
- Sicherheitskopien von Datenträgern sicher aufbewahren
- Schreibschutz bei allen Disketten setzen, auf die nicht geschrieben werden muss (dies gilt insbesondere für die meisten Programm-Disketten).
- Aktuelle Viren-Schutzsoftware verwenden.
- Alle ein- und ausgehenden Datenträger auf Viren überprüfen.
  Ausgehende Datenträger mit Schreibschutz versehen.
- Vorinstallierte Neugeräte und gewartete Geräte auf Viren überprüfen.
  Ebenso Programme über andere Datenkanäle bei Ein- und Ausgang auf Viren überprüfen. (z.B. Mailbox oder E-Mail, Internet)
- Notfall-Diskette erstellen.
- Mehrere Partitionen (logische Laufwerke) im Rechner einrichten.
- Computer und Datenträger vor unbefugter Benutzung schützen.
- Mitarbeiter über Computer-Viren schulen.

Einfache Maßnahmen zur Reduzierung der Gefahr vor Viren

1. Einstellungen am Rechner

Bereits durch das Aktivieren verfügbarer Sicherheitsfunktionen wird das Eindringen von Computer-Viren erheblich erschwert.

- Alle vorhandenen Sicherheitsfunktionen des Rechners aktivieren (Passwort-Schutz, Bildschirmschoner mit Passwort, etc.), damit während der Abwesenheit des berechtigten Benutzers Unbefugte keine Möglichkeit haben, durch unbedachte oder gewollte Handlungen den Rechner zu gefährden.

- Aktuelles Viren-Schutzprogramm mit aktuellen Signatur-Dateien einsetzen, das im Hintergrund läuft (resident) und bei bekannten Computer-Viren Alarm schlägt.

- Makro-Virenschutz von Anwendungsprogrammen (WinWord, Excel, Powerpoint, etc.) aktivieren und Warnmeldungen beachten.

- Sicherheitseinstellungen von Internet-Browsern auf höchste Stufe einstellen (Deaktivieren von aktiven Inhalten (ActiveX, JavaScript) und Skript-Sprachen (z.B. Visual Basic Script)).

2. Eingehende E-Mail

Eingehende E-Mail ist das größte Einfalltor für Computer-Viren. Bei sicherheitsbewusstem Verhalten lassen sich hierbei schon die meisten Computer-Viren herausfiltern.

- Offensichtlich nicht sinnvolle E-Mails von unbekannten Absendern sofort ungeöffnet löschen.

- Bei E-Mail auch von vermeintlich bekannten bzw. vertrauenswürdigen Absendern prüfen, ob der Text der Nachricht auch zum Absender passt (englischer Text von deutschem Partner, zweifelhafter Text oder fehlender Bezug zu konkreten Vorgängen etc.) und ob das Attachment auch erwartet wurde.

- Vorsicht bei mehreren E-Mails mit gleichlautendem Betreff.

- Kein "Doppelklick" bei ausführbaren Programmen(*.exe) oder Script-Sprachen (*.bat), Vorsicht auch bei Office-Dateien (*.DOC)

- Auch eine E-Mail im HTML-Format kann aktive Inhalte mit Schadensfunktion enthalten

- Nur vertrauenswürdige E-Mail-Attachments öffnen (z. B. nach tel. Absprache). Es ist zu beachten, dass die Art des Datei-Anhangs (Attachment) bei Sabotageangriffen oft getarnt ist und über ein Icon nicht sicher erkannt werden kann .

3. Verhalten bei Downloads aus dem Internet

Daten und Programme, die aus dem Internet abgerufen werden, stellen einen Hauptverbreitungsweg für Computer-Viren dar, um Benutzerdaten auszuspähen, weiterzuleiten, zu verändern oder zu löschen. Es muß darauf hingewiesen werden, dass auch Office-Dokumente Makro-Viren enthalten können.

- Programme sollten nur von vertrauenswürdigen Seiten geladen werden, also insbesondere von den Originalseiten des Erstellers. Private Homepages, die bei anonymen Webspace-Providern eingerichtet werden, stellen hierbei eine besondere Gefahr dar.

- Die Angabe der Größe von Dateien, sowie einer evtl. auch angegebenen Prüfsumme, sollte nach einem Download immer überprüft werden. Bei Abweichungen von der vorgegebenen Größe oder Prüfsumme ist zu vermuten, dass unzulässige Veränderungen, meist durch Viren, vorgenommen worden sind. Daher sollten solche Dateien sofort gelöscht werden.

- Mit einem aktuellen Viren-Schutzprogramm sollten vor der Installation die Dateien immer überprüft werden.

- Gepackte (komprimierte) Dateien sollten erst entpackt und auf Viren überprüft werden. Installierte Entpackungsprogramme sollten so konfiguriert sein, dass zu entpackende Dateien nicht automatisch gestartet werden.

Verhalten bei Befall

- Bei Verdacht auf Virus-Befall Arbeit wie gewohnt aber unverzüglich beenden.
- Computer ausschalten.
- Unerfahrene Anwender sollten einen Fachmann zu Rate ziehen(z. B. Benutzerdienst)
- Von virenfreier, schreibgeschützter System-Diskette booten
- Mit aktuellem Viren-Suchprogramm die Festplatte untersuchen; dabei ein Protokoll erzeugen.
- Datensicherung durchführen (falls nicht vorhanden).
- Virus von Festplatte entfernen
- Mit Viren-Suchprogramm die Festplatte erneut überprüfen.
- Alle anderen Datenträger (Disketten, CD-ROM, Wechselplatten) auf Viren-Befall untersuchen und Viren entfernen.
- Andere Benutzer warnen (wenn Daten- und E-Mail-Austausch von infiziertem Rechner erfolgte).
- Versuchen, die Quelle der Viren-Infektion festzustellen
  - wenn erfolgreich, anschließend:
- bei Programm-Disketten und CD-ROM: Hersteller informieren.
  bei Daten-Disketten: Ersteller des Datenträgers informieren.