Viren

EINFÜHRUNG

Was ist als erstes zu tun?

Brechen Sie nicht in Panik aus. Machen Sie am besten überhaupt nichts, wirklich. Trinken Sie eine Tasse Tee oder Kaffee, und tippen Sie um Gotteswillen nicht auf der Tastatur drauflos, bevor Sie nicht genau wissen, was jetzt zu tun ist. Nach meiner Erfahrung wird der meiste "durch Viren verursachte Schaden" tatsächlich durch Leute verursacht, die unbedingt etwas tun müssen, bevor sie überhaupt wissen, welche Massnahmen zu ergreifen sind, was nichts anderes als eine Umschreibung der üblichen Panik ist. Also keine Panik.

WAS IST EIN VIRUS?

Ein Virus ist ein Programm, das sich selbst kopiert und eine Hostdatei hat.

Das ist die Definition von Viren. Es gibt drei Arten von eigentlichen Viren.

- Datei-Virus
- Boot-Virus
- Makro-Virus

Ein Virus braucht sich also lediglich zu vermehren, um ein echter Virus zu sein, und tatsächlich machen 95 % aller Viren nichts anderes als das, von ein paar lächerlichen Zugaben, wie etwa einer piepsenden Tastatur oder einer merkwürdigen Bildschirmmeldung einmal abgesehen.

Die Begriffe "Computervirus" und "Virus" werden in der Umgangssprache sehr weit gefasst und sind gleichbedeutend mit "Ärger" und "Schwierigkeiten".

Sowohl Viren als auch Würmer, trojanische Pferde und logische Bomben sind unerwünschte Eindringlinge. Es bestehen jedoch wichtige Unterschiede zwischen ihnen.

In der folgenden Tabelle sind die einzelnen Kategorien definiert:

Begriff	**Host erforderlich?**	**Erstellt Kopien?**
Virus	Ja. Viren benötigen einen Host. Ihr Ziel ist es, andere Dateien zu infizieren, um länger zu "überleben". Einige, aber nicht alle Viren führen zerstörerische Aktionen aus. Viele Viren verstecken sich, um nicht erkannt zu werden. Hinweis: Viren sind einfach Softwareprogramme.	Ja. Alle Viren erstellen Kopien von sich selbst und infizieren, wenn möglich, System-Boot-Sektoren, Master-Boot-Sektoren, Programme oder Datendateien.
Wurm	Nein. Ein Host ist nicht notwendig, da Würmer typischerweise auf Grossrechnern auftreten und sich vor den meisten Benutzern nicht verstecken müssen.	Ja. Ein Wurm erstellt selbsttätig Kopien, falls möglich.
Trojanisches Pferd	Nein. Der Begriff "Trojanisches Pferd" bezieht sich manchmal auf das Programm, das den zerstörerischen Code enthält. Häufiger wird damit jedoch auf die gesamte .COM- oder .EXE-Datei Bezug genommen.	Nein. Die meisten trojanischen Pferde werden aktiv, wenn Sie ausgeführt werden und zerstören häufig die Struktur des aktuellen Laufwerks (FATs, Verzeichnis usw.). Während dieses Vorgangs vernichten sie sich selbst.
Bug, Logische Bombe, Zeitbombe	Ja. Programmierer können kein Bug schreiben, ohne auch anderen Programmcode zu schreiben (faireshalber muss gesagt werden, dass die meisten Programmierer nicht absichtlich Bugs produzieren). Logische Bomben und Zeitbomben werden aber absichtlich in den ansonsten "guten" Programmcode eingefügt.	Nein. Der Programmcode hat normalerweise besseres zu tun als sich zu reproduzieren. Logische Bomben und Zeitbomben möchten verborgen bleiben. Nur ihre Auswirkung soll sichtbar werden. Bugs können alles mögliche anrichten, aber sie vermehren sich nicht.

Und andere ……

Falscher Alarm	Ein falscher Alarm ist kein Virus. Ein falscher Alarm liegt dann vor, wenn Sie glauben, einen Virus zu haben, ohne dass dies wirklich so ist. Manchmal haben die Betroffenen lediglich Probleme mit einem Hard- oder Software-Fehler, lassen ein paar Diagnoseprogramme laufen, schliessen danach die Möglichkeit eines Hard- oder Software-Fehlers aus, ziehen die Schlussfolgerung, dass ein Virus vorliegen muss, und gehen im weiteren Verlauf ihrer Massnahmen von dieser Annahme aus. Noch häufiger allerdings ist ein falscher Alarm Ergebnis einer Anti-Virus-Software.
Scherz-programme	Ein Scherz ist etwas, das lustig ist. Jetzt ist es natürlich so, dass etwas, was der eine lustig findet, für den andern nicht unbedingt lustig ist. Alles nur eine Frage des Humors. Ein Programm tut so, als würde es Ihre Festplatte formatieren, und gibt hinterher bekannt, dass alles nur ein Ulk war. Lustig, oder etwa nicht? Alles nur eine Frage des Humors.
Beschädigte Programme	Einige Dateien sind schlicht und einfach defekt (möglicherweise aufgrund eines Hardware-Fehlers) und bringen den Computer zum Absturz, sobald sie ausgeführt werden. Aus unerfindlichen Gründen enden solche Dateien manchmal in Virussammlungen, wenn diese Sammlungen nicht sehr sorgfältig gepflegt werden.
Möchtegern-Viren	Der eine oder andere Virenprogrammierer ist ein schlechterer Programmierer, als er wahrhaben möchte, und schreibt ein Programm, das mit Sicherheit ein Virus hätte werden sollen, aber aus irgendeinem Grund so schwerwiegende Programmfehler enthält, dass der Virus überhaupt nicht funktioniert. Solche missglückten Viren werden in dem Glauben losgelassen, dass niemand sie je testen würde (vielleicht wurden manche davon noch nicht einmal von ihrem Urheber getestet). Einer der dabei typischen Fehler besteht darin, Dezimal- und Hexadezimalschreibweise falsch zu verwenden, wodurch im Quellcode möglicherweise fälschlicherweise mit "int 21" statt mit "int 21h" (was der Dezimalzahl 33 entspricht) auf den DOS-Funktionsinterrupt verwiesen werden soll.

Viren lassen sich in der Regel in drei verschiedene Arten einteilen:

Name	**Was wird infiziert?**
Dateivirus	Ausführbare Dateien (Programmdateien). Können über Netzwerke andere Dateien infizieren.
Makrovirus	Datendateien. Können über Netzwerke andere Dateien infizieren.
Boot-Virus	Boot-Sektoren von Festplattenlaufwerken und Disketten. Können nicht über Netzwerke infizieren.

Da ein Makrovirus Dateien infiziert, ist er technisch gesehen ein Dateivirus. Im Gegensatz zu den traditionellen Viren hat er es jedoch auf Datendateien abgesehen. Die Verbreitung der Makroviren nimmt ständig zu. Deshalb werden sie hier als eigene Kategorie behandelt.

METHODEN

Möglicherweise haben Sie auch schon von anderen Begriffen wie "Polymorph", "Stealthing" gehört. Dabei handelt es sich nicht um Virenarten, sondern um bestimmte Methoden, mit denen sich Viren vor Virensuchprogrammen verbergen möchten.

Polymorphismus

Die am häufigsten verwendete Art von Anti-Virus-Programm ist der Scanner, der nach einem Repertoire von Viren sucht. Für den Virenprogrammierer ist dies das Produkt, das er am liebsten täuschen würde. Ein polymorpher Virus ist eine Methode, von dem keine zwei Kopien an irgendeiner Stelle, gemeinsame Byte-Folgen enthalten. Daher kann ein solcher Virus nicht einfach anhand einer bestimmten Byte-Folge erkannt werden, sondern es muss eine wesentlich komplexere und schwierigere Aufgabe bewältigten werden, um ihn ermitteln zu können.

Stealthing

Wenn ein Virus speicherresident werden kann (was auf 99 % aller in der Computerwelt auftretenden Viren zutrifft), dann kann er mindestens einen der Interrupts abfangen. Wenn es sich um einen Bootsektorvirus handelt, dann missbraucht er den Interrupt 13h (Lesen von/Schreiben auf Datenträger). Wenn es sich um einen Stealth-Virus handelt und ein beliebiges Anti Virus Programm den Bootsektor zu lesen versucht, sagt sich der Virus "Aha, da will einer den Bootsektor sehen. Ich werde einfach dort, wo ich ihn abgelegt habe, den Original-Bootsektor lesen und dann statt des infizierten Bootsektors den Inhalt des Originals präsentieren". Dadurch fällt dem anfragenden Programm nichts Ungewöhnliches auf.
Solche Tarnfähigkeiten sind jedoch häufiger bei Bootsektorviren als bei Dateiviren zu beobachten, da es bei einem Bootsektorvirus viel einfacher ist, eine Tarnroutine zu programmieren.

WEITERE VIREN DIE KEINE SIND

Einige Programme werden dennoch als Viren bezeichnet. Doch nach der genauen Definition sind dies keine Viren. Ihnen fehlt die Eigenschaft sich zu kopieren oder haben keinen Host.

Companion- Viren

Wenn Sie eine COM- und eine EXE-Datei mit demselben Dateinamen haben und diesen Dateinamen eingeben, führt DOS stets vorzugsweise die COM-Datei aus. Die Companion-Viren nutzt diesen Umstand, und erstellen für jede Ihrer EXE-Dateien eine gleichnamige (sozusagen begleitende) COM-Datei. Wenn Sie dann versuchen, Ihr EXE-Programm auszuführen, wird statt dessen das COM-Programm, also der Virus, ausgeführt. Wenn der Virus das, was er tun sollte, abgeschlossen (und beispielsweise einen weitere COM Datei für eine weitere EXE Datei erstellt) hat, startet er das EXE-Programm, damit alles ganz normal zu funktionieren scheint.

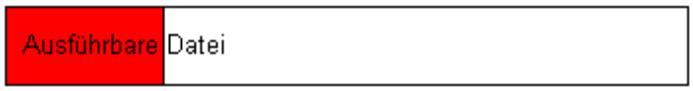
überschreibende Viren

Ein überschreibender Virus überschreibt einfach jede Datei, die er infiziert, mit sich selbst, wonach das betreffende Programm nicht mehr funktioniert. Da dies ein absolut augenscheinlicher Effekt ist, konnten sich überschreibende Viren noch nie besonders erfolgreich ausbreiten. Doch stellt sich die Frage, welche Datei ist Überschreiben.

DATEIVIRUS

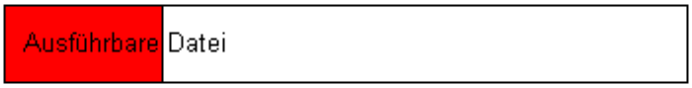
Ein Dateivirus hängt sich an eine Programmdatei (den Host) an und verwendet verschiedene Verfahren, um andere Programmdateien zu infizieren.
Die drei grundlegenden Verfahren zur Infizierung von ausführbaren Dateien sind:

Überschreiben, Voranstellen und Anhängen.

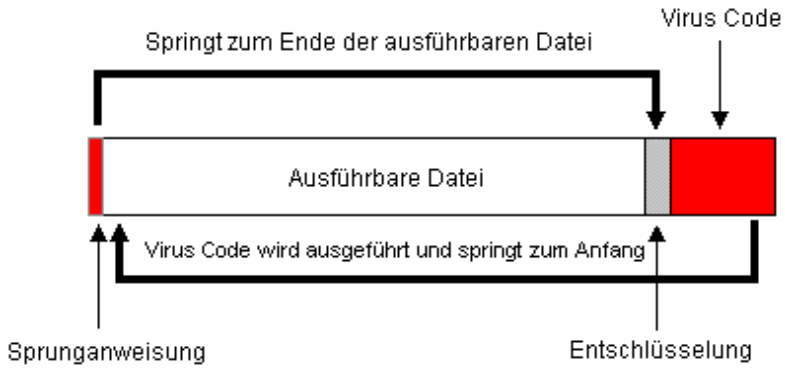


Ein überschreibender Virus setzt sich am Anfang eines Programms direkt über den ursprünglichen Programmcode und beschädigt so das Programm. Das Programm kann nicht mehr ausgeführt werden. Wenn Sie es versuchen, wird lediglich eine weitere Datei befallen.

Diese Viren sind leicht zu erfassen und können von Benutzern und Unterstützungspersonal einfach zerstört werden, so dass sie sich kaum ausbreiten können. Die Wahrscheinlichkeit, dass sich ein solcher Virus auf Ihrem Rechner befindet, ist sehr gering.



Die reine Form dieses Virus setzt einfach den gesamten Virencode vor das infizierte Originalprogramm. Wenn Sie ein Programm ausführen, das von einem solchen Dateivirus befallen wurde, wird vor dem Programm zunächst der Viruscode ausgeführt.



Ein anhängender Virus setzt eine Sprunganweisung an den Anfang der Programmdatei, verschiebt den ursprünglichen Anfang der Datei an das Dateiende und setzt sich selbst zwischen das ursprüngliche Dateiende und den ursprünglichen Dateianfang. Wenn Sie dieses Programm ausführen möchten, ruft die "Sprunganweisung" den Virus auf, und der Virus wird ausgeführt. Der Virus verschiebt dann den ursprünglichen Dateianfang an die richtige Position und das Programm wird ausgeführt.

Dies war ein kurzer Überblick darüber, wie sich ein Virus an eine Programmdatei anhängt. Zur Infizierung werden verschiedene Verfahren verwendet. Die meisten Dateiviren nisten sich im Arbeitsspeicher ein, so dass sie alle Aktionen überwachen und auch andere Programmdateien befallen können. Andere Dateiviren wiederum infizieren durch "Direktangriffe", d.h. sie infizieren eine Programmdatei, wenn auf diese Datei zugegriffen wird.

Es gibt noch viele andere Verfahren, aber in der Regel nisten sich die Viren im Arbeitsspeicher ein. Für einen speicherresidenten Dateivirus ist es sehr einfach, andere Programmdateien zu infizieren. Er wartet bis die jeweilige Programmdatei ausgeführt wird, und hängt sich dann an diese Datei an. Die Datei ist dann infiziert (d.h. ein "Host oder Trägerdatei") und infiziert weitere Programmdateien.

BOOT-VIRUS

Boot-Viren infizieren System-Boot-Sektoren (SBS) und Master-Boot-Sektoren (MBS). Der MBS befindet sich auf allen physischen Festplattenlaufwerken. Unter anderem enthält er Informationen zur Partitionstabelle (Informationen über die Aufteilung des physischen Datenträgers in logische Datenträger) und ein kurzes Programm, das die Partitionsinformationen interpretiert und so erfährt, wo sich der SBS befindet. Der MBS ist ein Betriebssystem. Der SBS enthält unter anderem ein Programm, das ein Betriebssystem sucht und ausführt.

Da diese Systembereiche während des Boot-Vorgangs auf allen IBM-kompatiblen PCs gelesen werden, sind Boot-Viren vom Betriebssystem unabhängig und deshalb in der Lage, sich schneller und wirksamer zu verbreiten als Dateiviren.

MAKROVIRUS

Zwischen August und November 1995 wurden vier Makroviren und ein trojanisches Pferd für Makros entdeckt und die Zahl der entdeckten Makroviren steigt weiter an. Man geht davon aus, dass man bis Dezember 1997 100 Makroviren kennen wird. Die Unterschiede zwischen Makroviren und traditionellen Dateiviren liegen beim Host (Datendateien) und dem Replikationsverfahren (Verwendung von anwendungseigenen Makro-Programmiersprachen). **Diese Unterschiede machen die neue, ernstzunehmende Bedrohung der Datensicherheit aus.** Denken wir ausserdem an die zunehmende Verwendung von OLE (Object Linking and Embedding) sowie den explosionsartig angestiegenen Zugang zu Netzwerken, E-Mail und dem Internet als Datenaustauschmedien, sind die Aussichten nicht gerade rosig.

Wie funktioniert er?

Traditionelle Dateiviren sind nicht auf die Infektion von Datendateien aus, da sich diese zur Verbreitung nicht eignen. Datendateien werden nämlich nicht "ausgeführt", sondern "gelesen" und "bearbeitet". In den letzten Jahren wurden in den Unternehmen jedoch offene Systeme eingeführt, die den Austausch von Daten vereinfachen. Darunter leidet wiederum die Datensicherheit. Makroviren nutzen es für sich aus, dass viele Anwendungen Makro-Programmiersprachen enthalten. Diese Sprachen gewähren Benutzern (und Virenautoren) eine grössere Flexibilität und

mehr Einflussmöglichkeiten auf die Anwendung als jemals zuvor. Oft werden Makroviren nicht früh genug erkannt, da viele Benutzer mit den Feinheiten der Makros nicht vertraut sind. Als Folge ist die Infektionsrate durch Makroviren viel grösser als die durch traditionelle Datei- und Bootviren.

Bis jetzt ist das Hauptangriffsziel von Makroviren die Makrosprache WordBasic, die Sprache innerhalb von Microsoft Word.

VORAUSSAGEN FÜR DIE ZUKUNFT

Man erwartet einen explosionsartigen Anstieg der neuentwickelten Makroviren und der Zahl der lokalen und globalen Infektionen. Man befürchtet auch, dass Viren gängige Makrosprachen für sich ausnutzen und so anwendungsunabhängig werden.

(Gegenwärtig ist Microsoft Word am häufigsten von Infektionen durch Makroviren betroffen, da die meisten Makroviren in WordBasic geschrieben sind.) Ausserdem geht man davon aus, dass Makroviren polymorphe Verfahren und Stealthing Methoden anwenden

DER BOOT-VORGANG

Um die Wirkungsweise der Boot-Viren zu verstehen, muss zunächst einmal der Boot-Vorgang untersucht werden.

Das BIOS (Basic Input/Output System), das den Boot-Vorgang steuert, wird mit Einschalten des Stroms eingeleitet.

Als nächstes wird nach dem Einschalten der Selbsttest POST (Power on Self Test) ausgeführt. Er stellt sicher, dass der Computer richtig funktioniert. Eine Funktion von POST, die bestimmt alle Benutzer kennen, ist die Zählanzeige zur Grössenbestimmung des RAM-Speichers (Random Access Memory) Ihres Rechners.

Als letzte Aktion leitet POST den Boot-Vorgang ein. Zunächst wird festgestellt, ob sich eine Diskette im Diskettenlaufwerk befindet. Wenn ja, wird der System-Boot-Sektor auf der Diskette gelesen und der Rechner versucht, von Diskette zu booten.

Wenn die Diskette nicht bootfähig ist (weitere Einzelheiten siehe unten), wird die folgende Meldung auf dem Bildschirm angezeigt:

```
Non system-disk or disk error.
Replace and strike any key when ready.
```

In der Regel ist keine Diskette eingelegt und es wird der Master-Boot-Sektor auf dem Festplattenlaufwerk gelesen. Danach wird der System-Boot-Sektor gelesen und das Betriebssystem gestartet.

Der gleiche Vorgang wird auf Rechnern mit DOS, Windows, Windows 95, Windows NT und OS/2 ausgeführt. Unterschiede treten erst auf, wenn die Betriebssysteme selbst geladen werden.

BOOTFÄHIGE DISKETTE

Bei der Formatierung einer Diskette wird ein System-Boot-Sektor erstellt. Die Diskette kann zwei Aufgaben haben:
Speichern von Programm- und Datendateien oder Verwendung als bootfähige Diskette.

Bootfähig ist eine Diskette dann, wenn mit ihr der Boot-Vorgang von der Festplatte umgangen werden kann. Stattdessen wird der Boot-Vorgang von Diskette ausgeführt.

Zur Erstellung einer bootfähigen Diskette müssen Sie die Diskette entweder mit der Option "System" (/S) formatieren oder den DOS-Befehl SYS auf die Diskette anwenden.

Eine formatierte Diskette verfügt immer über einen System-Boot-Sektor, unabhängig davon, ob die Diskette bootfähig ist oder nicht. Ein Boot-Virus ist im

SBS beheimatet, d.h. alle formatierten Disketten können mit einem Boot-Virus infiziert sein.

SO INFIZIERT EIN BOOT-VIRUS

Wenn eine Diskette im Laufwerk A: eines Rechners belassen wird und CMOS so eingerichtet ist, dass es zunächst von Laufwerk A: und dann von Laufwerk C: bootet, wird der SBS der Diskette gelesen. Enthält der SBS einen Boot-Virus, wird dieser aktiviert, speicherresident, infiziert die Systembereiche des Festplattenlaufwerks und versucht, andere Disketten mit Schreibzugriff, auf die zugegriffen wird, zu infizieren.

Viele Benutzer lassen Disketten in den Laufwerken, wenn sie den Rechner ausschalten und erinnern sich nicht daran, wenn sie den Rechner am nächsten Tag wieder einschalten. Boot-Viren kommen deshalb heutzutage von allen Viren am häufigsten vor.

WIEVIELE VIREN GIBT ES?

Anbietern von Anti-Virus-Programmen wird diese Frage ständig gestellt. Die Frage ist aus mehreren Gründen schwer zu beantworten:

1. Es gibt keine zentrale Stelle, die die Zahl der Viren zählt.

2. Jeden Tag kommen neue Viren hinzu. Einige Experten meinen, dass die Zahl der neuen Viren exponential ansteige, andere sehen einen quadratischen Anstieg. Wenn wir in der Lage wären, alle zu zählen, wäre das Ergebnis nur für kurze Zeit, vielleicht einen Tag lang, gültig.

3. Basierend auf einem Virus entdecken wir häufig viele Varianten und oft besteht innerhalb der Gemeinschaft der Virenforscher Uneinigkeit darüber, wie "Variante" zu definieren ist.

4. Es gibt keine standardisierte Benennungskonvention für Viren. Als Folge tauchen für denselben Virus mehrere verschiedene Bezeichnungen auf.

Dies führt zur der Frage, wie Viren zu ihren Bezeichnungen kommen. Manchmal fügen Virenautoren Text in den Virus ein, der den Namen für den Virus oder den eigenen Namen wiedergibt (z.B. Der Virus XXX ist da; Grüsse von yyy). Meistens jedoch werden die Namen von den Leuten vergeben, die die Viren entdecken.

VIREN IN FREIER WILDBAHN

Virenforscher kennen zwar Tausende von Viren, nicht alle müssen Sie jedoch beunruhigen. Die meisten dieser Viren kommen nur in Forschungslaboren vor und nur die verbleibende Handvoll befällt tatsächlich Heim- und Unternehmenscomputer auf der ganzen Welt.

Virenforscher sprechen von zwei Virenkategorien: Viren, die "in freier Wildbahn" auftreten und Viren "im Zoo".

Viren "in freier Wildbahn" wurden ausserhalb der Forschungslabore entdeckt. Diese "wildernden" Viren machen ca. 10% der bekannten Viren aus und sind diejenigen, mit denen Sie und Ihr Unternehmen sich auseinandersetzen sollten.

Am Anfang waren die Computer untereinander noch nicht sehr gut verbunden und Computerviren konnten sich nur langsam ausbreiten. Dateien wurden über Bulletin-Board-Systeme (BBS) oder über Disketten übertragen. Die Übertragung von infizierten Dateien und Boot-Sektoren war demzufolge geografisch beschränkt.

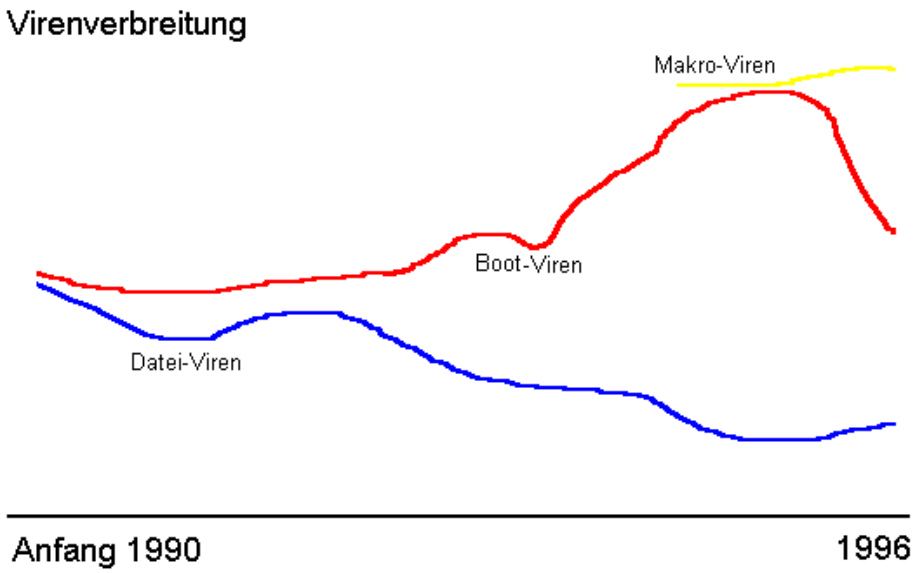
Mit der zunehmenden Verbindung von Computern, hauptsächlich der Computer am Arbeitsplatz, in Netzen erweiterten sich auch die Grenzen für die Computerviren. Zuerst kam das lokale Netzwerk (LAN), dann das Weitbereichsnetz (WAN) und nun das Internet. Die verbreitete Verwendung von E-Mail hat ebenfalls dazu beigetragen, dass die Zahl der Infizierungen durch Makroviren rasant angestiegen ist.

Wir leben heute in einer Gesellschaft, in der globale Technologien an erster Stelle stehen und globaler Handel über Kommunikationswege getätigt wird. Computer sind ein integraler Teil dieser Technologie und auch die Informationen, die sie speichern (ebenso wie der bösartige Code, den sie unwissentlich enthalten), werden global.

Es ist also heute viel wahrscheinlicher sich einen Virus einzufangen als noch vor zwei Jahren. Heute sind jedoch andere Arten von Viren gängig als vor zwei Jahren.

Steve White, Jeff Kephart und David Chess vom IBM Thomas J. Watson Research Center verfolgen die Entwicklung der Viren und haben (unter anderem) herausgefunden, dass die Vorherrschaft von bestimmten Virenarten teilweise durch die Änderungen bei Betriebssystemen bedingt ist.

Kurz zusammengefasst zeichnet sich folgender Trend ab:



BETRIEBSYTEME

Als Viren zum ersten Mal in Erscheinung traten, war MS-DOS das einzige bedeutende Betriebssystem. Windows brauchte einige Jahre um sich zu behaupten, d.h. Viren breiteten sich in MS-DOS aus. Tatsächlich sind fast alle Dateiviren (ausschliesslich Makroviren) MS-DOS-basiert.

Obwohl OS/2 kurz nach Erscheinung der Viren eingeführt wurde, ist OS/2 als Betriebssystem nicht so gängig wie DOS. Deshalb war und ist es unwahrscheinlicher, dass Virenautoren selbst mit OS/2 arbeiten und auch wenn OS/2-Viren häufig geschrieben würden, wären sie nicht so weitverbreitet wie MS-DOS-Viren. Gegenwärtig sind nur zwei OS/2-Viren bekannt.

Sowohl Windows 95 als auch Windows NT werden immer wichtiger. Beide sind rückwärts kompatibel mit MS-DOS und damit auch rückwärts kompatibel mit MS-DOS-Viren. Die Architektur der neuen Betriebssysteme stellt die Viren jedoch vor interessante Herausforderungen.

Schauen wir uns die Viren in MS-DOS, Windows, OS/2, Windows 95 und Windows NT einmal an.

MS-DOS

Da die Makroviren, die bis heute aufgetreten sind, Datendateien infizieren, die von Windows-Anwendungen erzeugt und gelesen werden, stellen Makroviren auf Rechnern, die nur über MS-DOS verfügen, kein Problem dar.

Traditionelle Dateiviren und Boot-Viren gedeihen auf MS-DOS-Rechnern, da MS-DOS nicht über eigene Sicherheitsfunktionen verfügt. Viren haben deshalb freien Lauf bei der Infizierung von Speicher und Programmdateien, wie unter Dateivirus beschrieben.

WINDOWS

Als Windows eingeführt wurde, mussten Benutzer bei der Interaktion mit dem Computer umlernen. Die Bilder auf dem Bildschirm waren farbiger, das Navigieren innerhalb eines Programms wurde einfacher und direkter und die Aussicht, zwischen Aufgaben umschalten zu können, ohne die jeweiligen Programme beenden zu müssen, war sehr aufregend.

Da DOS "unterhalb" von Windows ausgeführt wird, können Dateiviren Rechner infizieren, die Windows ausführen, jedoch ist ihre Lebensspanne sehr kurz. Im allgemeinen können Dateiviren die ausführbaren Dateien von Windows infizieren, aber dann arbeiten dieses Dateien in der Regel nicht richtig. Ungeduldige Benutzer werden entweder die ausführbaren Dateien ersetzen oder, wenn sie frustriert genug sind, Windows neu installieren. Das reicht schon aus, um den traditionellen Dateivirus umzubringen.

Makroviren und Boot-Viren erleideten jedoch nicht dasselbe Schicksal. Makroviren werden bis heute so geschrieben, dass sie Windows-Anwendungen angreifen.

Deshalb ist das Vorhandensein von Windows erforderlich. Die breite Akzeptanz von Windows zusammen mit der Tatsache, dass Makroviren statt Programmdateien eher Datendateien infizieren (siehe Makrovirus), hat dazu geführt, dass ein Makrovirus, Macro.Word.Concept, heute zu den zehn verbreitetsten Viren gehört.

Der eigentliche Boot-Vorgang auf einem Windows-Rechner unterscheidet sich nicht von dem eines reinen DOS-Rechners. Deshalb werden Boot-Viren durch Windows nicht behindert und verbreiten sich weiter, indem sie Festplattenlaufwerke infizieren, speicherresident werden und dann Diskettenlaufwerke infizieren.

OS/2

Wie bereits oben erwähnt, ist OS/2 nicht so weit verbreitet wie Windows und andere Betriebssysteme von Microsoft. Aufgrund seiner Konzeption ist OS/2 jedoch trotzdem anfällig auch für Viren, die nicht OS/2-spezifisch sind.

Im Gegensatz zu Windows, wird OS/2 nicht über MS-DOS ausgeführt. OS/2 ist ein leistungsstarkes 32-Bit-Betriebssystem, das DOS-Anwendungen, Windows-Anwendungen und eigene OS/2-Anwendungen unterstützt. Um DOS-Anwendungen ausführen zu können, ist OS/2 mit VDMs (virtuellen DOS-Maschinen) ausgestattet. Wie der Name besagt, sehen die VDMs für DOS-Programme wie DOS aus. Deshalb kann ein infiziertes DOS-Programm andere DOS-Programmdateien innerhalb dieses VDM infizieren, nicht jedoch DOS-Programme in anderen VDMs. Die neu infizierten DOS-Programmdateien können dann weitere Programmdateien infizieren, die in VDMs zukünftig noch gestartet werden. Auf diese Weise setzt sich der Infektionsweg fort.

Wenn Windows-Anwendungen, die Makrosprachen enthalten, auf einem OS/2-Rechner ausgeführt werden, ist der OS/2-Rechner genauso anfällig für Makroviren wie ein Windows-Rechner.

Noch einmal - da der Boot-Vorgang vor dem Laden des Betriebssystems auf allen IBM-kompatiblen Rechnern gleich ist, können Boot-Viren auch OS/2-Rechner infizieren. OS/2 behandelt Disketten anders als DOS und Windows. Die Wahrscheinlichkeit, dass der Boot-Virus sich nach der Infektion der Festplatte ausbreitet, ist auf einem OS/2-Rechner niedriger als auf einem Rechner mit Windows oder DOS. Das Risiko besteht eher in den Aktionen, die der Boot-Virus auf der Festplatte ausführt. Wenn der Boot-Virus über eine Ladung verfügt, kann man davon ausgehen, dass diese auch abgegeben wird, unabhängig davon, ob Disketten infiziert werden konnten.

OS/2 unterstützt zwei Dateisysteme: FAT (File Allocation Table - Dateizuordnungstabelle) und HPFS (High Performance File System - Leistungsfähiges Dateisystem). Sie können nur eines oder beide verwenden. HPFS ist ausgefeilter und speichert Informationen an verschiedenen Orten. Ein Boot-Virus, der nur auf FAT eingerichtet war, kann schwerwiegende Folgen für ein HPFS-System haben.

WINDOWS 95

Im Gegensatz zu Windows und DOS sind in Windows 95 Sicherheitsfunktionen integriert. Diese Funktionen sind jedoch nicht ausreichend, um Windows 95 gegen Viren zu schützen. Gegenwärtig gibt es einen Virus, der speziell für Windows 95 geschrieben wurde (der Boza-Virus). Darüber hinaus verfügt die Netzwerkumgebung der Workgroup von Windows 95 über keinen Schutz auf Dateiebene, was die Virenverbreitung unterstützen kann.

Windows 95 hat, was die Systemarchitektur und die Vireninteraktion betrifft, viele Merkmale mit OS/2 gemeinsam:
Wie OS/2 ist Windows 95 ein 32-Bit-Betriebssystem, das DOS-Anwendungen, Windows-Anwendungen und eigene Windows 95-Anwendungen unterstützt.

Ähnlich wie die VDMs von OS/2, hat Windows 95 VMs (virtuelle Maschinen) — eine virtuelle System-Maschine mit unterschiedlichen Adressbereichen für Win32-Anwendungen und einem gemeinsamen Adressbereich für alle Win16-Anwendungen sowie eigene virtuelle Maschinen für einzelne DOS-Anwendungen.

Dateiviren können sich auf einem Windows 95-Rechner mühelos ausbreiten, da DOS-Programmdateien unter Windows 95 nur der Beschränkung unterliegen, dass sie nicht direkt auf die Festplatte schreiben können.

Die einzelnen DOS-VMs nehmen die Charakteristiken des Systems von dem Punkt ab an, an dem die Maschine gestartet wurde. Da Windows 95 zunächst dieselben Programme ausführt wie ein reiner DOS-Rechner, ist es möglich, dass ein infiziertes Programm während des Startvorgangs andere Programmdateien innerhalb dieser VM infizieren kann. Darüber hinaus würde ein beim Startvorgang infiziertes Programm in allen VMs aktiviert, die zukünftig gestartet würden. Auch wenn Programmdateien einer VM keine Programmdateien einer anderen VM infizieren können, ist es doch möglich, dass eine infizierte Programmdatei irgendwann einmal auf eine eigene VM geladen wird und dabei den Infektionsweg fortsetzt.

Die bis zum jetzigen Zeitpunkt geschriebenen Makroviren greifen Datendateien an, die von häufig auf Windows 95 ausgeführten Win16- und Win32-Anwendungen erstellt und gelesen werden. Die Folge davon ist, dass auf Windows 95 Infektionen durch Makroviren verbreitet sind.

Da der Boot-Vorgang für Windows 95 bis zu einem gewissen Punkt dem für DOS- oder Windows-Rechner entspricht, können Boot-Viren die Festplattenlaufwerke von Windows 95-Rechnern infizieren. Beim Laden von Windows 95 werden Boot-Viren jedoch häufig deaktiviert und können sich nicht verbreiten. Allerdings können Boot-Viren, die eine Ladung führen, diese Ladung abgeben, auch wenn sie sich vorher nicht reproduziert haben.

WINDOWS NT

Wie in den Abschnitten zu OS/2 und Windows 95 erläutert, unterstützt Windows NT DOS-Anwendungen, Windows-Anwendungen und eigene Windows NT-Anwendungen. Wie Windows 95 ist auch Windows NT mit DOS und Windows rückwärts kompatibel. Auch wenn NT über robustere Sicherheitsfunktionen verfügt als Windows 95, kann es trotzdem von Dateiviren befallen werden, die sich dort

verbreiten. DOS-Anwendungen werden in eigenen VDMs (virtuellen DOS-Maschinen) ausgeführt und Dateiviren können innerhalb der VDM funktionieren. Einige DOS-Dateiviren arbeiten vielleicht unter NT nicht in der beabsichtigten Weise, aber die NT-Sicherheitsfunktionen halten Dateiviren bestimmt nicht davon ab, weitere Dateien zu infizieren.

Auch Windows NT (wie Windows 95) unterstützt Anwendungen, die Makrosprachen enthalten. NT ist deshalb genauso anfällig für Makroviren wie reine Windows-Rechner.

Da Rechner mit Windows NT auf die gleiche Weise booten wie DOS-Rechner (bis zu dem Punkt, an dem NT aufgerufen wird), können Boot-Viren die Festplattenlaufwerke von NT infizieren. Wenn diese Boot-Viren jedoch versuchen, sich im Speicher einzunisten, werden Sie von NT gestoppt und können keine Disketten infizieren. Auf diese Weise wird auch der Infektionsweg gestoppt, der Benutzer muss jedoch trotzdem mit möglichen Nebeneffekten, die die Boot-Viren auf das System haben —destruktive Ladungen oder Falschbehandlung des Boot-Bereichs von NT, die das Laden von NT verhindert), fertig werden.

SCHUTZ

Die meisten denken bei Lösungen zur Bekämpfung von Viren sicherlich an Virensuchprogramme. Suchprogramme sind die am leichtesten erhältliche, jedoch nicht die einzige Art der Virenbekämpfung.

Man sollte die Lösungsmöglichkeiten vielleicht unter folgenden Gesichtspunkten erörtern:

- Was ist nötig, um den Virus zu erkennen?
  - allgemeine Methoden
  - spezielle Methoden

und

- Wann wird der Virus entdeckt?
  - vor der versuchten Infizierung
  - nach der Infizierung

Ein Virus kann anhand allgemeiner oder spezieller Methoden erkannt werden. Allgemeine Methoden suchen nach virenkonformen Verhaltensweisen und nicht nach bestimmten Viren. Auf diese Weise können sogar neue Viren entdeckt werden und es besteht keine Notwendigkeit, das verwendete Tool häufig zu aktualisieren. Da allgemeine Methoden nach Verhaltensweisen und nicht nach bestimmten Viren suchen, wird normalerweise der Name der Viren nicht angegeben. Statt dessen wird lediglich eine Warnung an den Benutzer ausgegeben, dass wahrscheinlich ein Virus vorhanden ist. Einige schrecken vor dieser Methode zurück, da sie falschen Alarm verursachen kann. (indem z.B. ein nicht vorhandener Virus erkannt oder ein vorhandener Virus nicht erkannt wird).

Weiter werden die folgenden allgemeinen Methoden angewendet:

- Prüfsumme und Integritätsüberprüfung
- Heuristik
- Köder
- Verhaltensblockierung

Spezifische Methoden vertrauen auf zuvor gewonnene Kenntnisse über den Virus. In diesem Fall kann das Tool sowohl einen vorhandenen Virus erkennen als auch diesen Virus identifizieren. Das Tool muss häufig aktualisiert werden. Die meisten Benutzer möchten gerne wissen, mit was sie es zu tun haben, und um das herauszufinden ist es am besten, das Wesen der Bestie genau zu bestimmen. Aus diesem Grund bevorzugen viele Benutzer dieses Verfahren, aber letzten Endes finden Sie keinen Gefallen daran, dass das Tool sehr häufig aktualisiert werden muss.

Und auch werden folgende spezifische Erkennungsmethoden eingesetzt:

- Bedarfsgesteuerte und zeitgesteuerte Suche
- Suche in Echtzeit

Ein weiterer, nicht minder wichtiger Gesichtspunkt betrifft den Zeitpunkt der Virenerkennung. Alle Benutzer stimmen wahrscheinlich darin überein, dass die Viren idealerweise davon abgehalten werden sollen, Dateien zu infizieren. Die nächste Stufe wäre die, alle Bereiche zu erkennen, die bereits infiziert wurden.

Im folgenden wird untersucht, wo die obengenannten Methoden fehlschlagen:

Methode	Diskussion der Virenerkennung
Prüfsumme und Integritätsüberprüfung	Beide Methoden speichern Informationen zu (hoffentlich) nicht infizierten Dateien an einen bestimmten Ort. Überprüfungen des aktuellen Status der Dateien gegen die gespeicherten Informationen werden in regelmässigen Abständen durchgeführt. Bei festgestellten Änderungen wird eine Warnmeldung ausgegeben. Diese Methode entdeckt die Viren nach der Infizierung.
Heuristik	Bei dieser Methode werden die Dateien und Boot-Bereiche in einem allgemeinen Sinn untersucht, um zu bestimmen, ob der Code virenkonform aussieht. Heuristische Untersuchungen erkennen Viren nach der Identifizierung.
Köder	Bei dieser Methode werden bestimmte Dateien als Köder ausgelegt, die bei vorhandenem Virus infiziert werden. Köder erkennen Viren bei der Infizierung und geben eine Warnung aus.
Verhaltens-blockierung	Diese Methode analysiert das Verhalten aller Verarbeitungsaktionen und stellt dadurch fest, ob sich die Summe der Teile zu einer viruskonformen Aktion verbindet. Wenn ja, wird die Aktion gestoppt, bevor es zu einer Infizierung kommen kann. Verhaltensblockierung erkennt Viren vor der Infizierung.
Bedarfsgesteuerte und zeitgesteuerte Suche	Diese Methode sucht zu bestimmten Zeiten nach bestimmten Viren. Auf diese Weise können Viren immer erst nach der Infizierung erkannt werden.
Suche in Echtzeit	Bei dieser Methode wird ein Suchprogramm verwendet, der Erkennungsprozess findet jedoch gleichzeitig mit anderen Computerprozessen, wie z.B. dem Kopieren einer Datei, statt. Als Folge erfahren Benutzer von vorhandenen Viren, bevor diese ausgelöst werden können.

Wie Sie sehen, gibt es keine einzelne Lösung, die alle Ihre Anforderungen an die Virenerkennung erfüllen könnte.

Das Thema der Virenentfernung ist ähnlich komplex. Viele Betroffene haben eine enggesteckte Vorstellung von Virenentfernung wenn die Datei gelöscht oder die Festplatte formatiert wird, ist der Virus weg. Beachten Sie jedoch, dass diese drastischen Massnahmen häufig nicht nötig sind und dass die sinnvolle Virenentfernung lediglich den Virencode entfernt und eine benutzbare Datei und/oder ein intakter Boot-Bereich übrig bleibt.

Einige der oben aufgeführten Erkennungsmethoden können auch Virenentfernung ausführen (nach der sinnvollen und "gesunden" Methode):

Methode	**Diskussion der Virenentfernung**
Prüfsumme und Integritätsüberprüfung	Kann Viren entfernen.
Heuristik	Kann manchmal Viren entfernen.
Köder	Kann keine Viren entfernen.
Verhaltensblockierung	Kann Viren aus dem Speicher und Boot-Viren von Disketten entfernen.
Bedarfsgesteuerte und zeitgesteuerte Suche	Kann manchmal Viren entfernen.
Suche in Echtzeit	Kann manchmal Viren entfernen.