Erscheinungsformen
Entwicklungsgeschichte
Gegenmaßnahmen

Eine Hausarbeit von
Michael Abbing
Matr. Nr.: 1524804
fürs Fach TKT
bei Prof. Dr. J. Ludwig
01/2002

HAW-Hamburg

1. Computerviren allgemein

a) Definition eines Computervirus

In der Biologie ist ein Virus ein Krankheitserreger, der keinen eigenen Stoffwechsel besitzt. Er greift stattdessen eigenständige Zellen an, nistet sich in ihnen ein und programmiert die DNA-Erbinformation der Wirtszelle um. Damit ist seine Analogie schon erschöpft.
Einen Computervirus kann man ein klein wenig mit dem biologischen Virus vergleichen. Er ist ein Stück Software, das sich ein Programm sucht und seinen Programmcode dort hineinkopiert. Gelangt das Wirtsprogramm zur Ausführung, kann der Virus aktiv werden in dem er z.B. Dateien löscht/ändert, Arbeitsabläufe stört, sich fortpflanzt oder gar den Computer zum Absturz bewegt.

b) Grobe Einteilung der Computerviren

Man könnte die derzeitigen Computerviren grob in drei Arten aufteilen:
Klassische Viren, Würmer und Trojaner.
Der **klassische Virus** ist ein Schadensprogramm, daß sich von Datei zu Datei auf einem Computer ausbreitet. Er muß dazu aktiviert werden, was meistens dadurch geschieht, daß der Benutzer unwissend eine infizierte Datei öffnet oder den Rechner hochfährt.
Die Absicht vieler Viren ist es, so viele Dateien wie möglich innerhalb eines Computers zu infizieren oder wichtige Funktionen zu blockieren. Eine Übertragung zu anderen Rechnern kann nur durch austauschbare Datenträger (Disketten etc.) oder als in Anhang einer E-Mail geschehen, so das die Verbreitungsgeschwindigkeit des klassischen Virus immer vom Benutzer abhängt.
Der **Wurm** dagegen ist ein Programm, daß sich von Computer zu Computer via Netzwerk/Internet selbsttätig weiterverbreitet und braucht daher kein Wirtsprogramm. Die Absicht der Würmer ist es also so viele Computer wie möglich innerhalb eines Netzwerkes zu befallen. Sie brauchen dabei keine menschliche Hilfe und verbreiten sich automatisch rasend schnell über das jeweilige Netzwerk.
Trojaner sind wiederum Programme, die sich als nützliche Anwendung tarnen, im Hintergrund aber ohne das Wissen des Anwenders eine Schadensroutine ausführen. Die Absicht vieler Trojaner ist es, unbemerkt so viele sensible Nutzerdaten wie möglich auszuspionieren. Werden vom Nutzer z.B. Passwörter fürs Onlinebanking oder Kreditkartennummern per Internet übermittelt, schreibt der Trojaner per Keylogging diese Daten mit und kann sie je nach Art des Virus seinem Programmierer per E-Mail unbemerkt zuschicken. Diese Funktionen können so weit gehen, daß der Autor des Trojaners durch Einrichten von sogenannten Backdoors einen Fernzugriff auf den infizierten Rechner hat und ihn kontrollieren kann.

c) Aufbau von Computerviren

Alle Computerviren haben einen festgelegten logischen Aufbau, der meistens aus drei Teilen besteht: *Reproduktionsteil, Erkennungsteil, Schadensteil*:

Mit dem **Reproduktionsteil** wird, auf welche Art auch immer, die Vermehrung des Virus durchgeführt.
Im **Erkennungsteil** wird geprüft, ob bereits die Infektion eines Programmes oder Systembereiches erfolgt ist. Die Verbreitung wird beschleunigt, wenn der Virus auf eine Infektion „verzichten" kann, weil sie logischer Weise bereits geschehen ist.
Jedes Wirtsprogramm wird deshalb nur einmal infiziert.

Die Entdeckung des Virus wird daurch 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.
Oft enthalten Viren noch einen **Schadensteil**, welcher außer der Inanspruchnahme von Speicherplatz im Hauptspeicher und auf Datenträgern noch sehr viel gemeinere Veränderungen im System vornimmt. Meistens werden Programme überschrieben/verändert, Dateien gelöscht/verschlüsselt, Hardware und Speicher angegriffen, oder aber auch einfach nur Meldungen und Geräusche ausgegeben. Durch Programmierfehler, Veränderungen des Betriebssystemes oder ähnliches können weitere Schäden als Nebeneffekte auch dann auftreten, wenn sie nicht absichtlich programmiert worden sind.
Manchmal sind die Schäden aber auch von bestimmten Bedinungen abhängig. Dann spricht man auch von einem **Bedinungsteil**, der den Schaden bei Ablauf eines bestimmten Datums oder ähnliches ausführt.
Bei jüngeren Viren gibt es oft auch noch einen **Tarnungsteil**, der Programmroutinen enthält, welche eine Entdeckung des Virus in infizierten Systemen erschweren sollen.

2. Computervirentypen

Eine genaue und eindeutige Zuordnung der verschiedenen Computerviren ist in der Regel nicht ganz einfach, da viele Viren in verschiedenen Mischformen auftreten. Es wurden aber im Laufe der Zeit bestimmte Begriffe definiert, die die Funktionsweisen der Viren und deren Hilfsprogramme kategorisch beschreiben:

ANSI-Viren: ANSI-Viren sind in Grunde genommen keine echten Viren, sondern eher Manipulationen der Tastatur- und Funktionstasten. Es handelt sich hierbei um Sequenzen, die in normalen Texten eingebunden wurden. Wird der Text angezeigt, so verändert sich die Tastaturbelegung. (statt „G" wird „Z" abgebildet etc.)

Construction-Kits: Construction-Kits sind Programme, mit deren Hilfe jeder „normale" User in der Lage ist sich eigene Viren zusammenzubauen. Da die erzeugten Viren

meistens recht primitiv sind und durch Antiviren-Programme schnell erkannt werden, stellen sie keine ernsthafte Gefahr da.

CMOS-Viren: Sie sind als sehr gefährlich einzustufen, da sie den externen CMOS-Speicher des Rechners (Speicher für Datum, Uhrzeit, Festplattenwerte, Größe des RAM) angreifen. Zwar kann sich der Virus nicht von dort aus starten oder speichern, aber er kann den CMOS manipulieren und löschen, so dass dies Systemabstürze zur Folge hat.

Dateiviren (TSR- oder Programm- oder COM-Viren): Diese sehr häufig verbreiteten Viren infizieren ausführbare Programme (.COM, .EXE, .OVL, .SYS, .BAT etc.) und können bei deren Abarbeitung aktiviert werden. Die Aktivierung des Viruscodes wird bei jedem Programmstart vorgenommen und wird durch den User durch die schnelle Ausführung kaum erkannt. Meistens sind diese Viren speicherresident, d.h. sie befinden sich im Hauptspeicher des Rechners und laufen im Hintergrund des Systems mit und warten darauf, daß der Anwender ein bisher nicht infiziertes Programm öffnet um es anzugreifen. In kürzester Zeit kann somit ein ganzes System infiziert werden.

Dropper/Bootssektor-Viren: Diese Viren verstecken sich im Bootssektor von Festplatten und Disketten sowie im MasterBootRecord (MBR). Sie können sich ebenfalls wie die Dateiviren von einem Datenträger resident in den Hauptspeicher verlagern und so permanent Schaden anrichten.

Direkt-Action-Viren: Diese Arten von Viren sind nicht speicherresident, benutzen jedoch den Hauptspeicher des Systems. Wird ein solcher Virus aktiviert, sucht er sofort nach anderen Programmen, die er infizieren kann. Anschließend übergibt der Virus die Kontrolle an das ursprüngliche Programm und entfernt sich aus dem Hauptspeicher. Diese Viren erfordern vom Programmierer nicht allzu hohe Fachkenntnisse und sind trotz großer Anzahl eher weniger verbreitet.

DIR-Viren/Verzeichnisviren: Diese Virusart manipuliert direkt die DOS-Verzeichnisse und keine Sektoren oder Dateien. Dies hat zur Folge, dass sich der Virus sehr schnell verbreitet, da schon ein DIR-Befehl ausreicht, um das Verzeichnis komplett zu infizieren.

DNS-Angriff: Bei einem DNS-Angriff erfolgt eine Umleitung einer Internetanfrage eines Nutzers an einen Rechner auf einen dritten Rechner, so daß auf diese Weise z.B. Passwörter ausspioniert werden können.

E-Mail-Bombing/Denial-Of-Sevice: Bei dieser Virenform überhäuft ein Angreifer ein Zielsystem mit Mails, so daß im Extremfall die normale Nutzung vom Mailprogramm nicht mehr möglich ist.

E-Mail-Viren: Diese Viren verstecken sich im Attachment von Mails übertragen sich bei deren Benutzung auf den lokalen Rechner.

Fast-Infektor-Viren: Die Fast-Infektor-Viren infiziert Dateien schon beim Öffnen oder Schließen. Startet der Anwender einen Virenscanner, während sich ein solcher Virus aktiv im System befindet, können nach dem Scanvorgang nahezu alle Dateien auf dem System infiziert sein. Sie verbreiten sich somit wie ein Lauffeuer auf dem Rechner, was wiederum die Systemperformance stark abbremst und somit die Infizierung vom User leicht erkennbar werden läßt.

Header-Viren: Diese Viren sind sehr selten heutzutage, da sie nur Programme angreifen, die einen „leeren" Programmkopf besitzen und nicht größer als 64 kB sind.

HLL-Viren: Diese Viren wurden ausschließlich in Hochsprachen programmiert und sind mehr oder weniger schwer zu erzeugen, da spezielle Fachkenntnisse vom Programmierer erforderlich sind. (Beispiele: HLLT (Tojan), HLLP (parasitic), HLLC (Companion), etc.)

Hoaxe: Hoaxe sind Meldungen oder Warnungen (meistens E-Mail) über Viren bzw. Malware (Sammelbegriff für schädliche Programme), die es gar nicht gibt. Die einzigen Schäden, die solche Meldungen verursachen, sind Verstopfung von Mailsystemen und ahnungslose Menschen in Panik zu versetzen.

HTML-Viren: Der erste HTML-Virus trat 1998 auf und versteckte sich in Form eines VB-Scripts (Visual Basic Script) in einer HTML-Datei und kann auch andere Dateien infizieren, indem er sich ebenfalls als Script in der Datei versteckt. Er arbeitet im Grunde genommen wie Script-Viren und benötigt mindestens Windows 98 mit installiertem Windows Script Hosting.

Hybrid-Viren: der Ausdruck Hybrid-Virus beschreibt Virusvarianten, die möglichst viele Mechanismen vereinen. So enthält z.B. ein Dateivirus einen speicherresidenten und einen Bootsektorvirus und ergibt somit in vereinter Form ein sehr gefährliches Programm.

IP Spoofing: Ein Angreifer erzeugt Datenpakete mit gefälschtem Absender (per E-Mail oder Netzwerk). Der Empfänger nimmt an, einen internen Nutzer vor sich zu haben und gibt dadurch Zugangsrechte frei.

Java Viren: Sie sind nur sehr selten und sehr inkompatibel, da die ganze Struktur von Java sehr umfangreich und nicht so leicht erlernbar ist.

Kernel-Viren: Sie sind eigentlich eine Mischung aus DIR- und Bootsektorviren und bisher ist von dieser Sorte erst ein Exemplar bekannt.

Keystroke Reader: Jeder Tastendruck eines Users wird durch ein in den Rechner eingeschmuggeltes Programm heimlich mitgelesen und aufgezeichnet. Dadurch lassen sich wichtige Daten ausspionieren.

Killerprogramme: Unter Killerprogrammen versteht man Viren, die nach einer bestimmten Anzahl von Infektionen eine Aktion auslösen. Der interne Zähler des Virus zählt von einem festgelegten Wert bis auf Null runter. Die darauf folgende Aktion ist je nach Exemplar unterschiedlich, meistens werden jedoch Dateien gelöscht oder verschlüsselt oder manipuliert.

Logische Bomben/Zeitzünder funktionieren ebenfalls wie Killerprogramme, indem nach einer bestimmten Aktion (erreichen eines Datums oder Löschen eines bestimmten Datensatzes) Schaden anrichten.

Labor/Research-Viren: Diese Viren sind kaum in „freier Wildbahn" anzutreffen, denn sie wurden Virenforschern zugespielt und befinden sich nur in deren Laboren. Der größte Teil aller Viren sind Laborviren.

Makro-Viren: Makroviren sind in Makros (d.h. in automatischen Programmabläufen) von Dokumenten, Tabellen und Grafiken u.a. enthalten. Sie können bei Weiterverarbeitung dieser Dateien mit den entsprechenden Anwendungsprogrammen (z.B. MSWord, MSExel etc.) aktiv werden. Dadurch, dass ihre Programmiersprache (Basic) leicht erlernbar ist, haben sich diese Viren in kurzer Zeit sehr weit verbreitet.

Partitionsviren: Diese Viren verändern die Partition direkt oder die Angaben des ersten logischen Sektors von Festplatten und werden bei jedem Systemstart sofort aktiv.

Polymorphe Viren: Im Grunde genommen verändern polymorphe Viren in einem bestimmten Rhythmus ihr „Aussehen", so daß sie für Virenscanner, die nach Erkennungsmustern arbeiten, nicht oder nur schwer entdeckt werden können.

Retroviren: Diese Viren sind darauf aus „Antivirenprogramme" anzugreifen. Der Härtegrad ist je nach Typ sehr unterschiedlich und sie erfordern vom Programmierer genauste Analysen über Schwachstellen in den jeweiligen Programmen.

Residente Viren: Kurz gesagt arbeiten diese Virenarten ständig im Hintergrund des Systems um nach zu infizierenden Dateien „Ausschau" zu halten. Sie sind sehr hartnäckig und in der Regel sehr schwer vom System zu entfernen.

Script-Viren: Diese relativ jungen Viren infizieren nicht nur VB-Scripts, sondern auch Netscape oder Java Scripts. Befindet sich so ein Virus auf dem System, werden alle Script-Dateien im Browser-Cache infiziert und sogar oft auf den Desktop kopiert, so daß der erstaunte Anwender oft „lustige" Icons auf seinem Bildschirm zu Gesicht bekommt. Wie bei den HTML-Viren funktionieren diese jedoch auch nur bei installiertem Windows-Script-Hosting.

Sendmail Bugs: Sendmailbugs sind trojanische Pferde, die in das zum verschicken von E-Mails wichtige Sendmail-Programm eingeschmuggelt werden und Passwörter ausspionieren.

Slack-Viren: Der Slack-Virus nutzt den ungenutzten Platz eines Festplatten-Clusters um sich unauffällig einzunisten. Dadurch wird verhindert, dass die Größe einer Datei verändert wird und somit dem Anwender nicht auffällt. Der Virus tritt allerdings nur selten auf und wird bei einem normalen Defragmentierungs-Vorgang der Festplatte gelöscht.

Slow-Infektor-Viren (Cavity): Sie sind im Prinzip das Gegenteil von den Fast-Infektors, da sie sich nur sehr langsam verbreiten. Diese Technik hat den Hintergrund Prüfsummenprogramme oder residente Wächterprogramme auszutricksen, indem sie die Programmdateien lediglich erst beim Erstellen oder Schreiben infizieren, und somit auch keine Prüfsumme vorliegt. Diese Viren sind im Gegensatz zu den Fast-Infektor-Viren relativ selten.

Stealth- oder Tarnkappenviren: Hier unterscheidet man zwischen Semistealth- und Fullstealth-Viren: Letztere verbergen die Tatsache, daß infizierte Dateien oder Sektoren verlängert oder verändert wurden, und somit für die Virensuch- und Prüfsummen-programme durch Täuschung unentdeckt bleiben. Die Semistealth-Variante verbirgt lediglich die Dateiverlängerungen, was jedoch nicht unbedingt weniger effektiv sein muß. Grundsätzlich wird der Bergriff „Stealth" heute immer noch für besonders raffiniert programmierte Virenvarianten benutzt.

Update-Viren: Bei dieser Gruppe von Viren sind neben den eigentlichen Funktionen auch noch Update-Routinen zu finden. Diese überprüfen ob der Virus schon vertreten ist und wenn ja in welcher Version. Ist die vorhandene Version älter, wird dieser durch die neue Version ersetzt.

Überschreibende Viren (Overwriting): Diese primitive aber auch gefährliche Virenform überschreibt direkt Programme oder Dateien und vernichtet sie dadurch meist vollständig. Da sie in den meisten Fällen nicht resident sind, suchen sie normalerweise nur im aktuellen Verzeichnis nach Opfern.

3. Geschichte der Computerviren

Nachdem die Viren-Arten und Begriffe nun erklärt wurden, soll ein Abriß in die Geschichte der Computerviren mehr ein Blick in die Motivation und „Sinnfrage" der Viren geben. Eine exakte und ausführliche Angabe des Erscheinens aller Virenarten und Typen würde den Rahmen dieser Ausarbeitung sprengen und so sind im Folgenden nur die wichtigsten und bedeutensten Daten aufgeführt.
Der Begriff des Computervirus entstand etwa in den Anfängen der 80'er Jahre und wurde 1981 von Professor Adelmann eingeführt, als er sich mit dem angehenden Doktoranden Fred Cohen unterhielt.
Die Theorie des Computervirus geht jedoch schon bis in die **40'er Jahre** zurück. Der ungarische Informatiker John von Neumann entwickelte damals schon die Theorie von selbstreproduzierenden Automaten. Erst Jahrzehnte später erfanden Anfang der **70'er Jahre** einige Mitarbeiter der Bell Laboratories ein Spiel mit dem Namen „Core Wars", dessen Ziel es war dem Gegner kostbare Rechenzeit zu stehlen. Dieses Spiel könnte man daher schon als ersten Wurm bezeichnen, wobei er in Gegensatz zu den heutigen Würmern auf die Hilfe des Programmierers angewiesen war, der ihn verbreiten mußte.
Eine Diplomarbeit, von Jürgen Kraus **1980** an der Uni Dortmund Fachbereich Informatik erstellt, wies zum ersten Mal auf die Möglichkeit hin, daß sich bestimmte Programme ähnlich wie biologische Viren verhalten können.
Er schilderte in dieser Arbeit die Konstruktion möglichst einfacher selbstreproduzierender Programme, jedoch wurde diese Arbeit nie veröffentlicht und verschwand im Archiv der Universität. Die ersten konkreten Würmer entstanden dann im Jahre
1982. Zwei Mitarbeiter des Xeros Alto Research Centers, Jon Hepps und John Shock, generieren Würmer für verteilte Rechenoperationen im internen Firmen-System. Ein Programmierfehler führte dazu, daß die Würmer außer Kontrolle gerieten und somit das komplette System zum Absturz brachten.
1983 stellte Fred Cohen den ersten funktionsfähigen Computervirus vor, welcher unter dem Betriebssystem Unix programmiert war. Dieser konnte die Systemprivilegien eines infizierten Programmes an jeden Benutzer weitergeben. Als Fred Cohen dann schließlich **1984** seine Diplomarbeit fertigstellte, war ihre Veröffentlichung sehr umstritten. Sie enthielt neben dem erwähnten Virus auch andere experimentelle Viren, so daß die Entwicklung in diesem Bereich rasant fortschritt.
1985 wurden dann über die damaligen BTX-Mailboxen Programme verteilt, welche die noch sehr mangelhafte Grafik verbessern sollten. Nach dem Start dieses Programmes, welches ein getarntes Trojanisches Pferd war, wurden jedoch alle Daten auf der Festplatte gelöscht und eine Bildschirmmeldung „Arf, Arf, Gotcha" abgebildet („Arf, Arf, ich hab dich"). In diesem Jahr wurde auch gleichzeitig ein Virus in Quelltextform durch die der Zeitschrift „Apples" veröffentlicht.
1986 zog die Zeitschrift „Computer persönlich" nach und veröffentlichte wiederum einen Virus in Quelltextform für den Apple II. Im Gegenzug verkaufte die Firma Apple seine Computer nur noch in Verbindung mit einem Antivirenprogramm, welches jedoch nur diese eine Virenfamilie finden und entfernen konnte. Gleichzeitig entwickelten zwei Software-Händler aus Pakistan einen MSDos-Boot-Virus namens „Brain", den sie ihren Software-Raubkopien anhängten. Durch den Verkauf dieser Kopien verbreitete sich der Virus über Europa bis nach Amerika, mit dem Ziel, daß sich so der Kunde an den Händler binden müßte.
Auf dem Großrechner an der TU-Berlin wurde der Virus namens "Virdem" gefunden, welcher in Deutschland entwickelt wurde.
1987 verbreitet sich der erste Wurm für IBM-Systeme. Der Wurm "Christmas EXCEC" zeigte einen Weihnachtsbaum und versendete sich heimlich per E-Mail weiter. An der LeHigh-Universität in Delaware, USA, wurde dann der erste speichresistente Virus „Lehigh" entdeckt und läutete somit eine neue Virengeneration ein. Ähnliche Ableger wie werden kurz darauf auch in Deutschland entdeckt.

Der wohl berühmteste Virus dieser Art, der "Freitag der 13."-Virus, oder auch „Jerusalem"-Virus , wird in Israel entdeckt. Dieser Virus war in der Lage an jedem Freitag den 13. alle .com und.exe Dateien zu löschen, und die Rechnergeschwindigkeit alle 30 Minuten zu verringern.
Der ebenfalls berüchtigte MBR-Virus (Master Boot Record) „Stoned" wird von einem Studenten aus Welligton, Neuseeland entwickelt.
Für andere Systeme treten auch die ersten Viren auf, so für den MAC (nVir, Peace), Amiga (SCA-Virus), Atari ST (PT, Alladin) und für UNIX (IBM MVS 370). Durch die Verbreitung eines Virus in Quelltextform für den Atari ST in der Zeitschrift „C't" werden erste Kritiken an der Veröffentlichung von Viren laut. Die Steigerung dessen wird **1988** durch die Veröffentlichung des ersten „Virenbaukastens" für den Atari ST erreicht. Mit Hilfe dieses Programms war nun jeder User in der Lage relativ einfach eigene Viren herzustellen. Ebenfalls wird der erste Antivirus-Virus entdeckt, welcher den Virus „Brain" erkennt und entfernt.
Robert Morris startet den ersten Internet-Wurm, welcher ca. 6000 Computer (10% aller Internet-Rechner) befällt. Er wird daraufhin zu 10000$ Geldstrafe, 3 Jahre auf Bewährung und 400 Stunden gemeinnütziger Arbeit verklagt. Zur gleichen Zeit wird „Cascade", der erste sich selbst verschlüsselnde Virus, in Deutschland aktiv.
1989 werden die ersten „Stealth" oder „Tarnkappen"-Viren entdeckt. Der „Frodo"-Virus z.B.war in der Lage seine selbstgemachten Veränderungen in der infizierten Datei zu verbergen.
Das erste Trojanische Pferd wird von der Firma PC Cyborg Corp. in den Umlauf gebracht: Durch ein Datenbankprogramm, welches per Diskette an die Teilnehmer einer AIDS-Konferenz verteilt wurde, wurde der Virus auf den Rechner installiert. Ein beiligender Lizenzvertrag wies darauf hin, daß bei längerer Benutzung des Programms eine Gebühr von knapp 400 $ zu zahlen sei, sonst würden alle wichtigen Dateien auf der Festplatte verschlüsselt werden. Während der Installation wurden allerdings schon Systemdateien umbenannt und das Trojanische Pferd auf die Festplatte gespielt. Durch einen im Virus enthaltenden Zähler wurden dann nach dem 90. Start des Programmes tatsächlich alle Daten auf der Festplatte verschlüsselt und somit zerstört. Die Firmeninhaber wurden daraufhin verurteilt und in eine geschlossene psychatrische Anstalt eingewiesen.
Um der rasanten Weiterentwicklung von Computerviren entgegenzuwirken, gibt es die ersten intenationalen Versuche Viren zu klassifizieren und in Zeitschriften und Büchern über Viren zu informieren. Die ersten gedruckten Viren-Informationsdienste entstehen (Virus Bulletin, Virus Telex) und mehrere Hersteller bringen Antiviren-Programme auf den Markt, die bis zu 44 Viren erkennen und entfernen können.
1990 treten die ersten polymorphen Viren wie "V2PX, „Virus-90" und „Virus-101" in freier Wildbahn auf. Diese Viren verschlüsseln sich auf andere Weise immer wieder neu, was das Entwickeln von Anti-Virenprogrammen erschweren soll.
Mit „Anthrax" und "V1"-Virus verbreiten sich die ersten mehrteiligen Viren recht erfolgreich.
Der „Whale" oder „Motherfish"-Virus war ebenfalls ein mehrteiliger Virus, der sich nicht nur selbst modifizieren und oligomorph verschlüsseln konnte, sondern auch noch Trankappen-Eigenschaften besaß. Er galt als größter, speicherresistente Virus überhaupt und soll angeblich von Virenforschern als Testvirus programmiert worden sein.
Eine neue Art von DOS-Virus (DIR-II-Virus) tritt auf, welcher nicht nur die Programme sondern auch die FAT-Einträge infiziert (Cluster-Virus). Ebenfalls wird das erste Viren-Construction-Kit für DOS-Anwender durch den „Verband deutscher Virenliebhaber" verbreitet und das erste trojanische Pferd für den Macintosh entdeckt.
1991 steigt die Anzahl der neu gefundenen Viren langsam exponentiell an. Der „Michelangelo"-Virus wird entdeckt und löst geradezu eine Hysterie aus. Es finden Wettbewerbe und Veranstaltungen zum Programmieren von Viren statt und es werden viele Zeitschriften speziell für Virenprogrammierer veröffentlicht. Außerdem wird ein Virus programmiert, der unter Novel-Netware Passwörter ausspionieren soll.
In Gegenzug wird durch die Gründung der Organisationen EICAR (European Institute for Antivirus Research) und CARO (Computer Antivirus Research Organisation) eine bessere Bekämpfung von Computer-Viren propagiert.

1992 bleiben die weltweit vorausgesagten Schäden durch den „Michelangelo"-Virus aus. Durch die Veröffentlichung der „Mutation Engine" durch den Programmierer „Dark Avanger" taucht jedoch ein neues Virenkit auf, mit dem es möglich ist aus einfachen Viren polymorphe Viren zu bauen. Die Verschlüsselungsroutine ändert sich dabei genau so wie die Instruktionen, um den Virus zu entschlüsseln.
Ebenfalls taucht der erste, aber leicht erkennbare, Windows-Virus „WinVir 1.4" auf und der erste Virus, der SYS-Dateien infiziert („Involuntary").
Über einen Datenkanal vom Sender Pro7 wird ein neuer polymorpher Virus übertragen. Er befand sich in einem Entpackungsprogramm vom McAfee-Virenscanner und verändert seine Struktur jedesmal komplett. Virenforscher brauchten viele Monate bis der Virus in ihren Suchprogrammen in allen Varianten erkannt wurde.
1993 tauchen fast jeden Tag etwa 20–30 neue Viren auf. Viele sind jedoch bekannt und durch die verbreiteten Constuction-Kits nur leicht verändert worden, und so tauchen schon von einigen Viren hunderte von Varianten auf.
Die Antiviren-Industrie gibt als Gegenschlag die erste „Wild-List" heraus (zu sehen z.B. bei Virus-Bulletin unter **{** HYPERLINK http://www.virusbtn.com/resources/wildlists/index.xml **}** oder unter {HYPERLINK "http://www.wildlist.org"}.). Der aus SanDiego stammende Programmierer „LittleLog" verbreitet seinen Virus „SatanBug" in Washington DC, er wird jedoch durch die Behörden nachverfolgt und aufgedeckt.
1994 benutzt ein Programmierer das Internet, um seinen Virus „Kaos4" zu verbreiten indem er ihn in eine Newsgroup platziert.
Ebenfalls taucht ein neuer Virus auf, der wesentliche Unterschiede zu seinen Vorgängern hat. Er verteilt seine variable Entschlüsselungsroutine über das gesamte infizierte Programm, er kann sich sowohl in Dateien, Bootsektoren und MasterBootRecords einnisten, er verschlüsselt zwei Sektoren der Festplatte mit einen variablen Schlüssel und verfügt über Stealth-Techniken, die das Erkennen zusätzlich erschweren. Diese „One Half" oder „Free Love"-Viren werden als multipartite Viren bezeichnet und sind ebenfalls speicherresistent.
Der Kernel-Virus „3APA3A" ist auch eine neue Virenform, die den Bootsektor und eine Systemdatei infiziert.
In England verbreitet sich der „SMEG.Paragon"-Virus und Scotland Yard stellt den Autor Christopher Pile (Synonym „Black Baron"). Er wird wegen Computerkriminalität in 11 Fällen verurteilt und bekennt sich im November
1995 für schuldig (18 Monate Haft).
Es entstehen mit „Concept" und „DMV" die ersten Makro-Viren, die keine ausführbaren Programmdateien mehr infizieren, sondern Dokumente des Textverarbeitungs-programmes „WinWord". Diese recht leicht in Assembler programmierbaren Viren sind gleichzeitig auch die ersten systemübergreifenden Viren, da WinWord sowohl auf dem PC wie auch auf den Macintosh benutzt wurde.
1996 wird auch der erste polymorphe Virus für Windows entdeckt und der „Boza"-Virus, der erste Virus für Windows 95, taucht auf. In Alaska und Afrika tauchen die ersten Excel-Makro-Viren auf, die Tabellen von Microsoft-Excel infizieren.
Ende 1996 wird die Zahl der PC-Viren auf über 10.000 Varianten geschätzt. Dadurch, daß die Produktion neuer Macintosh-Viren fast zum Stillstand gekommen ist und Systeme wie „Unix" und „Linux" kaum Viren zulassen, wird immer mehr deutlich, wie anfällig offene Systeme wie DOS sind.
1997 tauchen die ersten „mIRC"-Script-Würmer auf. Die von den Programmierern geschriebenen mIRC-Scripte verbreiten sich automatisch wurmartig unter den Benutzern der Internet Relay Charts. Die Zahl der Makro-Viren für WinWord nimmt rasant zu, da unter anderem eine WinWord verwendete Systemdatei OLE2.dll fehlerhaft ist und somit Microsoft den schnellen Anstieg größtensteils selber verursacht. Der erste Linux-Virus wird vom Antivirenprogramm-Hersteller McAfee entdeckt.
1998 taucht eine Weiterentwicklung des Excel-Virus auf namens "XF.Paix.A", der nicht nur wie ein klassischer Makro-Virus funktioniert sondern auch noch ein spezielles Formelblatt benutzt, welches bösartige Codes enthalten kann.

Der im März von Carl F. Neitker veröffentlichte Virus „Netbus" ermöglichte Hackern einen Fernzugriff auf den infizierten Rechner und im April werden die ersten Viren für MSAccess 97 entdeckt, worauf ähnlich Viren für alle MSOffice Anwendungen folgen.
Im Juni wird der bösartige, aus Taiwan stammende, Virus "W95.CIH" entdeckt, der am 26.April versucht das Bios eines Computers zu überschreiben, was oft einen kompletten Hardwaretausch zur Folge hat. Kurz darauf tauchen die ersten AOL-Trojaner auf, die Informationen von AOL-Usern stehlen und deren E-Mail-Adressen mit infizierten Dateien überfluten.
Im August veröffentlicht die Hackergang „Cult of the Dead Cow" ein getarntes Fernsteuerungsprogramm, welches sowohl die Überwachung des infizierten Rechners ermöglichte, als auch Programme ausführen konnte.
Der erste von vielen in Visual Basic geschriebenen Script-Viren „VBS.Rabbit" wird losgelassen und der virus „HTML.Prepend" beweist, daß es mit VBScript möglich ist, HTML-Dateien zu infizieren.
Im März **1999** verbreitet sich ein Virus namens „W97M.Melissa.A" mit sehr schneller Geschwindigkeit weltweit. Er infiziert Word-Dokumente und versendet sie per E-Mail an bis zu 50 Adressen aus dem Outlook-Adressbuch. Viele Mailserver brechen zusammen und der Autor David L. Smith wird verhaftet.
Im April wird "Netbus2Pro" als kommerzielles Programm veröffentlicht. Der Autor Carl-F. Neikter verlangt für sein Produkt Geld, um Antivirushersteller davon abzuhalten, es als Virus zu melden. Die Hersteller fügen trotzdem eine Erkennungsroutine ein, da es sich um ein bösartiges Programm handelt.
Der im Vorjahr entdeckte Virus "WIN95.CIH" wird pünktlich am 26.April aktiv. Die größten Schäden werden im asiatischen Raum gemeldet, jedoch unternimmt China bzw. Taiwan keine rechtlichen Maßnahmen gegen den Autor Chen Ing-Hau.
Ein sich wie „Melissa" ähnlich schnell verbreitender Wurm „Explorer.zip" wird in Israel entdeckt. Er zerstört Dateien der MSOfficeanwendeungen wie DOC, XLS, PPT, C ,CPP und ASM.
Im Juli bringt die „Cult of the Dead Cow"-Gruppe die 2. Version ihres Fersteuerungsprogramms heraus, welches nun auch Windows NT-Rechner infizieren kann.
Der polymorphe und speicherresidente Virus „W32/Kriz" wird im August entdeckt. Er wird nur einmal im Jahr am 25.12 aktiv und ist in der Lage das Flash-Bios zu überschreiben, den CMOS-Speicher zu löschen/zerstören und alle Dateien in allen Laufwerken zu löschen. David L. Smith bekennt sich schuldig, Autor des Melissa-Virus zu sein.
Im November wird der erste nur durch lesen einer E-Mail aktiv werdende Virus „VBS.Bubble.Boy" entdeckt. Er nutzt einen Fehler in einer Microsoft-Programmbibliothek aus, durch den das Abspeichern und Starten einer Anlage unnötig wird.

Die von vielen Menschen befürchtete Jahr-**2000**-Katastrophe bleibt aus und existierende Y2K-Viren bleiben weitgehend wirkungslos. „VBS.Bubbleboy" wird im April in freier Wildbahn entdeckt.
In Juni breitet sich der „VBS.Loveletter, der als „I love you"-Virus bekannt wurde, mit rasend schneller Geschwindigkeit (noch schneller als „Melissa") aus. Er sorgt für die bisher größte Virenkatastrophe weltweit und läßt zahlreiche Mailserver zusammenbrechen und infiziert hunderttausende von Computern.
Es folgen viele Varianten dieses Virus und bei Entdeckung ensteht jeweils ein großer Medienrummel.
Im Juli wird eine Weiterentwicklung der VBS-Viren entdeckt, die mit SHS-Dateien arbeitet (Shell Scrap). Sie nutzt die OLE-Fähigkeiten von Windows, um sich in einer scheinbaren Textdatei zu verbergen.
Ähnlich wie der „I love you"-Virus sorgt im August der „W32.Pokey.Worm" für Aufregung , welcher sich ebenfalls als E-Mail Anhang über Outlook Express verbreitet.
Im September wird der erste Trojaner für Kleincomputer bz. PDA`s (Personal Digital Assistent) entdeckt, der beim Synchronisationsprozeß auf die Geräte gelangt. Er wurde versehentlich in Schweden von einem Beschäftigten an der Universität von Gavle entwickelt.

Pünktlich zur Weihnachtszeit verbreitet sich „Navidad.exe" zwar nicht besonders schnell, aber dennoch gefährlich auf jede Art von Windows-Rechnern.

2001 nimmt die Verbreitung der E-Mail-Viren immer mehr zu. Im Februar erscheint der „VB.SST@mm"-Virus als "AnnaKournikova.jpg.vbs" E-Mail-Anhang. Er kopiert sich beim Öffnen des vermeintlichen Bildes in die Windows-Directory und verschickt sich anschließend weiter per Outlook.
Auch „W32/Naked" verschickt sich als getarnter Anhang (diesmal eine Flash-Animation) und infiziert im März diverse Rechner, bei denen er verschiedene Windows- und Systemverzeichnisse löscht und das System unbrauchbar werden läßt.
Die Massenmailer „CodeRed" und „CodeRedII" nutzen im Juli eine Sicherheitslücke in der WebSoftware „InternetInformation Server" von Microsoft aus und installieren eine Backdoor ins System, durch die Hacker das System kontrollieren können.
Der Wurm „W32/SirCam" ist der erste Wurm mit integriertem Mailserver (SMTP-Engine) und verbreitet sich ebenfalls im Juli. Er platziert sich ins Systemverzeichnis und wird jedesmal aktiviert, wenn der Anwender ein Programm mit der Dateiendung .exe starten will. Außerdem kann er sich selbsttätig auf andere Laufwerke und Netzwerke kopieren und verschickt sich per Outlook nicht nur selbst, sondern auch noch zusätzlich persönliche Dateien, die er auf den infizierten Rechnern gefunden hat.
Im September rast der aggressive Wurm „Nimda" durchs WWW und verbreitet sich per E-Mail und kann sich zudem über das Internet auf fremden Rechnern einnisten. Für seine Verbreitung sind keine Benutzerinterventionen mehr erforderlich und seine er führt abermals zu einer hohen Belastung des Internetverkehrs. Er läßt diverse Internetseiten zusammenbrechen und kompromittiert die Sicherheit des File-Systems indem er die lokalen Laufwerke im Netz freigibt.
Der speicherresidente Internetwurm „W32.Badtrans.B@mm" nutzt im November ebenfalls die bekannten Sicherheitslücken der Outlook-Programme. Er registriert sich nach der Infektion als Systemservice und ist in der Lage eingehende E-Mails zu beantworten, Passwörter auszuspionieren und installiert einen zusätzlich einen Keylogger.
Im Januar **2002** taucht „JS/Gigger" in vielen Chatforen auf und infiziert alle teilnehmer die sich dort aufhalten. Er verändert anschließend die autoexec.bat und überschreibt alle dateien mit der Endung .ASP, .HTM. und HTML.
Ebenfalls taucht der erste „Klez"-Wurm auf, der jedoch durch seine geringe verbreitung als „LowRisk" eingestuft wird.
Im Februar verbreitet sich der Wurm „Yarner", der als angebliche 0190-Warn-E-Mail die Festplatten der infizierten Rechner mit sinnlosen Daten überschreibt.
Ein als gefährlich eingestufter Virus macht im März auf sich aufmerksam. „W32/MyLife.b" tarnt sich in E-Mail-Anhängen als karikativer Bil Clinton Bildschirmschoner und infiziert nach Öffnung den Rechner und nimmt Änderungen in den Systemverzeichnissen und der Registry vor. Außerdem verschickt sich dieser Wurm automatisch per Outlook als E-Mail mit dem Text " No Virus found. MCAFEE.Com", so daß sich der Empfänger in trügerischer Sicherheit wiegt.
Im April tauchen die ersten gefährlichen Varianten des „KLEZ" E-Mail-Virus auf, der nicht etwa wie bei dem „I Love You"-Virus eine bestimmte Betreffzeile enthält, sondern diese immer wieder neu generiert, so das mittlerweile über 40 solcher Varianten bekannt sind. Ist der Rechner einmal infiziert, versucht der Virus das antivirenprogramm auszuschalten, was jedoch nur bei den älteren Versionen gelingt.
Im Juni wird eine neue E-Mail-Viren Spezies entdeckt, die sich über ganz normale Bilddateien verbreitet. „W32.Perrun" benötigt keine ausführbaren Progammcodes und Scripte mehr, kopiert sich nach Infektion auf alle JPG-Bilddateien und verschickt sich automatisch per E-Mail weiter.
Der Virus „Frethem" verbreitet sich im Juli sehr schnell, da er die bekannten Sicherheitslücken bei Outlook Express und Internet-Explorer nutzt und als verführerrische Passwort-Knacker-E-mail auftaucht. Außerdem lädt er automatisch ein Trojanisches Pferd aus dem Netz, welches sich dann wiederum automatisch auf dem Rechner installiert.

Für die sonst von Virenwarnungen verschont gebliebenen Linux-User wird im August ein gefährlicher Virus namens „Slapper" entdeckt, der in Form eines trojanischen Pferdes eine Backdoor Funktion auf Linux-Internet-Servern installiert und somit das System für Hacker frei zugänglich macht.
Auch der Virus „Bugbear" ist im Oktober in der Lage infizierte Rechner zu bespitzeln, in dem er Eingaben über die Tastatur registriert und die Daten an den Hacker weiterleitet. Zudem nutzt er die bekannten Microsoft Sicherheitslücken und verbreitet sich rasend schnell durch automatisches Weiterversenden per Outlook.
Ein jetzt vor einigen tagen im November aufgetauchter Virus „Roron" aus Bulgarien, wird ebenfalls als sehr gefährlich eingestuft. Er enthält eine bekannte Backdoorfunktion für Hacker und kann unter Umständen Inhalte auf der Festplatte löschen.

4. Maßnahmen und Werkzeuge zur Virenbekämpfung

Wie aus der Entwicklungsgeschichte der Computerviren ersichtlich, bietet das Internet die beste Verbreitungsmöglichkeit für Computerviren. So gesehen sind fast alle modernen Computerviren auch gleichzeitig E-Mail-Viren in Kombination mit anderen Virenarten. Die meisten Viren nutzen die bekannten Sicherheitslücken bei Betriebssystemen von Microsoft und somit sind hauptsächlich Windows-User Opfer von Virenbefall. Dies liegt natürlich auch daran, dass der unmotivierte Hacker so viele Rechner wie möglich angreifen möchte und Windows als Betriebssystem mit Abstand am weitesten verbreitet ist.
Waren es früher noch Viren-Programme, die per Diskette ins System gelangten oder aus dem Anhang von E-Mails heraus installiert werden „mußten", sind es heute bei den modernen Viren die Anhänge, die man nur anzuschauen braucht. Damit reicht es auch nicht mehr aus das viel gescholtene Programm Outlook-Express zu umgehen und die E-Mails direkt vom E-Mail-Konto aus zu lesen und zu kontrollieren.
Die erste Maßnahme ist deshalb die absolute Eigenkontrolle seines E-Mail-Kontos zu besitzen und verdächtige, unbekannte E-Mails ohne sie zu Öffnen gleich zu vernichten.
Die Newsletter von Antivirenprogrammen waren bisher auch immer eine sichere Maßnahme zur aktuellen Virus-Information, jedoch könnten diese auch manipuliert sein (wie vor einigen Tagen bekannt wurde, als ein Antivirus-Newsletter vom Hersteller Kapersky einen Virus enthielt).
Ganz allgemein ist die „Trennung" vom Internet natürlich eine sehr sichere Preventions-maßnahme, so daß man sich vielleicht für den Internet-Verkehr einen billigen Zweitrechner zulegen sollte, auf dem keine wichtigen Daten vorhanden sind.
Ebenfalls eine wichtige und eher allgemeinere Maßnahme ist das permanente Sichern von Daten. Macht man regelmäßige Backups, so ist man vor der ernsthaftesten Viren-Gefahr, das Vernichten aller Daten, sicher.
Selbstverständlich ist natürlich auch das Meiden von Raubkopien (hoher Risikofaktor) und man sollte darauf achten, dass alle erstellten Dateien und Disketten schreibgeschützt sind (Rechtsklick/Eigenschaften). Diese Maßnahme macht den Angriff durch einige Viren oft wirkungslos.
Da die modernen Viren in ihrer Struktur immer komplexer geworden sind und durch ihre Tarnmechanismen für den normalen User kaum erkennbar sind, sollte man die Virenüberwachung einem Antivirus-Programm (AV) überlassen. Diese Programme gibt es in verschiedenen Variationen sowohl als Freeware wie auch kostenpflichtig und beinhalten oft folgende Elemente:
Scanner sind die meistverwendeten AV-Elemente und untersuchen die Dateien nach virenspezifischen Zeichenketten oder nach Jokerzeichen, die auf mehrere Virenvarianten passen und somit den Scanner flexibler machen. Der auf den System befindliche Virus muß dem Programm aber schon bekannt, um ihn finden zu können, und so sind die älteren Scanner oft gegen polymorphe Viren machtlos. Neuere Scanner verwenden

deshalb Ansätze von künstlicher Intelligenz und heuristische Methoden um gegen unbekannte Viren besser gewappnet zu sein. In diesem Fall erhält der Benutzer aber oft keine Information über den Virus sondern muß auf Grund der erkannten Symptome und einer Wahrscheinlichkeitsaussage des Scanners selbst entscheiden ob eine Infektion vorliegt oder nicht. Ein ständiges Updaten der aktuellen Virusdefinitionen vom Hersteller ist deshalb unablässig um eine sichere Arbeitsweise des Scanners zu garantieren.
Speicheresidente Scanner sind eine spezielle Form der herkömmlichen Scanprogramme. Sie werden bei einem Programmstart oder Datenzugriff seitens des Benutzers aktiv und scannen die betroffenen Files.
Heueristische Scanner arbeiten nach dem Prinzip der Fuzzy-Logic und analysieren Programme auf deren Funktion und Aufbau. Werden hier verdächtige Funktionen erkannt, schlägt der Scanner Alarm wenn die untersuchte Datei mehrere beinhaltet.
Monitor-Programme sind im Gegensatz zu Scannern speicherresidente Programme und warten im Hintergrund auf virenspezifische Aktivitäten. Wird eine Aktivität festgestellt, fragt das Programm den User ob diese legitim ist und wenn nicht, deutet dieses evtl. auf einen Virus hin. Einige der oben genannten Virenarten sind aber wiederum in der Lage diese Art vom AV`s zu übergehen und daher reicht ein Monitorprogramm als alleiniger Virenschutz meistens nicht aus.
Checksummenprogramme oder Integrity-Checker sind Programme, die von Datenabschnitten Checksummen erstellen. Diese Datenabschnitte können Bootsektoren, Dateigrößen, Programme usw. sein. Diese Checksummen werden mit einer von Zeit zu Zeit neu erstellten Checksumme verglichen und lassen so evtl. Veränderungen erkennbar werden, die auf einen Virus hindeuten können. Des weiteren weisen diese nützlichen Programme auch auf nicht durch Viren manipulierte Dateien hin und bemerken beispielsweise auch Datenverluste durch eine alte Festplatte.

Die heutigen etablierten AV`s wie Norton Antivirus oder McAfee bieten meistens alle aufgeführten Elemente in einem großen Programm an. Dieses ist natürlich kostenpflichtig und spätestens nach einem Jahr muß man die nächste Rechnung für das Updaten und herunterladen von neuen Virusdefinitionen bezahlen. Dabei ist aber immer noch keine vollständige Garantie geboten, das diese Programme, trotz regelmäßiger Updates, auch jeden Virus erkennen können. Es empfiehlt sich daher auch mal andere evtl. kostenlose AV`s auszuprobieren und die einzelnen Elementarfunktionen auch einzelnen spezielleren Programmen zu überlassen. Die Maßnahme, neben dem Haupt-AV auch noch ein zweites Programm zu Hilfe zu nehmen, kann auch eine noch höhere Sicherheitsgarantie geben.

Wird ein AV benutzt, so sollte man noch auf einige Einstellungen achten, die man eigentlich bei jedem Programm vornehmen kann. Ist ein Monitor-Modul enthalten, sollte dies unbedingt immer im Hintergrund mitlaufen um einen permanenten Virenschutz gerade beim Downloaden von Dateien aus dem Internet zu gewährleisten.
Ebenfalls sollte man den Process-Viewer, der teilweise in AV`s oder auch im Windows-Betriebssytem integriert ist, einschalten. Dieser überprüft die sog. „Laufenden Prozesse" und meldet verdächtige Aktivitäten, so daß auf diese Art Trojaner und andere Malware entdeckt werden können.
Wichtig ist auch das Ausschalten der automatischen Virenentfernung, da diese oft Probleme bereiten kann. Eine missglückte Entfernung kann zu erheblichen Schäden im Betriebssystem führen, und daher sollte die Rückfrageoption eingestellt werden, bei der immer noch die Möglichkeit einer vorherigen Datensicherung besteht. Anschließend sollte der Virenscanner erneut gestartet werden und die Entfernung des Virus zugelassen werden.
Der Schutz vor Makroviren kann durch Aktivierung des programmeigenen Makroschutzes erhöht werden (z.B bei Office97 Programmen und neuer unter Optionen einstellbar). Scriptviren lassen sich durchs deinstallieren von Windows Script Hosting vermeiden.

Reicht der Schutz von AV`s dennoch nicht aus und verkehrt man mit vertraulichen Daten im Internet (z.B. Onlinebanking etc.), so empfiehlt es sich noch eine zusätzliche Personal Firewall einzurichten. Diese Programme überprüfen im einfachsten Fall, ob die eingegebene Internetadresse als sicher gekennzeichnet und der Zugriff gestattet ist oder

nicht (diese Funktion enthalten auch einige Internetbrowser). Bessser ist jedoch noch eine darüber hinausgehende Kontrolle der gesendeten Daten und eine Blockierung oder zumindest eine Freischalt-Option für die Übertragung von Java-Applets, Active-X-Controls und Cookies. Auch ein Scannen des Ports und damit das Ausspionieren von Rechnerinformationen sollte eine Firewall verhindern können. Richtig konfiguriert, blockt die Firewall alle Verbindungen von außen ab und sperrt damit potentielle Angreifer durch Trojanische Pferde und Backdoors ab. Als Nebeneffekt kann sie auch Aktivitäten von „Werbe-Robotern" entlarven, denn immer mehr kostenlose Software enthält versteckte Funktionen, die häufig unbemerkt Werbebanner auf den Rechner schicken.

Grundsätzlich gilt es sowohl bei AV`s und Firewalls, erst mal alle Sicherheitsfunktionen zu aktivieren und dann trotz der vielen auftretenden Alarmmeldungen Ruhe zu bewahren. Beim näheren Untersuchen der Fehlermeldungen wird man dann ganz schnell merken, welche berechtigt sind und welche nicht und entwickelt somit ein gewisses Verständnis für die Funktionweise des Programmes. Auf diese Art man nun selbst die Chance seine eigenen, für sich relevanten, Sicherheitseinstellungen auszusuchen und sein System optimal zu schützen.

Quellen:

{ HYPERLINK http://www.symantec.de **}**
{ HYPERLINK http://www.mcafee.com **}**
{ HYPERLINK http://www.trojaner-info.de **}**
{ HYPERLINK http://www.heise.de **}**
{ HYPERLINK http://www.jurpc.de **}**
{ HYPERLINK http://www.wdr.de **}** (Virenticker)
{ HYPERLINK http://www.vhn.haitec.de **}**
{ HYPERLINK http://www.fh-trier.de **}**
{ HYPERLINK http://www.antivirus-online.de **}**
{ HYPERLINK http://www.sicherheit-im-internet.de **}**