

<b>Inhaltsverzeichnis</b>	Seite
1. Vorwort	-1-
2. Wie entstand der erste Computer Virus?	-1 + 2-
3. Definition eines Computer Virus	-4-
3.1 Wie werden Computer Viren erzeugt?	-4 + 5-
3.2 Wie verbreitet sich / arbeitet ein Computer Virus?	-5 + 6-
3.3 Computer Virus Typen	-6 - 10-
3.3.1 Typen Eigenschaften	-10 - 12-
4. Wer schreibt Computer Viren und warum?	-12-
5. Aktueller Virenstand	-13-
5.1 Was bedeutet "in the wild"?	-13-
6. Fazit	-13 + 14-
7. Quellen	-14-

## **1. Vorwort**

Schon als ich meinen ersten eigenen Computer, eine echt alte Kiste wohlgerneht, bekam, faszinierte mich einfach alles rund herum und ich glaube der Gedanke, später auch Informatik zu studieren, hat sich über die Jahre hin in meinem Kopf festgesetzt.

Als es dann in der Schule darum ging ein Fach für die Facharbeit festzulegen, viel mir das wahrlich nicht schwer und ich wählte Informatik in der Hoffnung, dass ich nicht einer derjenigen werden würde, die ihre Arbeit in dem zweit-gewählten Fach schreiben müssen.

Die Themenwahl jedoch, war wirklich nicht so einfach wie ich mir das vorgestellt hatte. In der Informatik gibt es so viele interessante Bereiche, derer es sich lohnen würde sie genauer unter die Lupe zu nehmen. Doch als ich mich entsinnte, dass ich schon auf meinem aller ersten Computer einen Virus hatte (Parity Boot Virus) und ihn auch heute noch auf der ein oder andere alten Diskette finde, kam mir in den Sinn wie gerne ich früher schon gewusst hätte, wie denn diese Viren genau funktionieren.

## **2. Wie entstand der erste Computer Virus?**

Bereits Anfang der Siebziger Jahre, lange vor der Zeit des PCs, schrieben Administratoren monströser Computer, die meistens die Größe eines Zimmers hatten, kleine Programme um mit ihnen die sogn. "CORE WARS" auszutragen. Derjenige der es mit seinem Programm schaffte, die Gegnerprogramme aus dem Speicher zu werfen, hatte gewonnen. Von dieser recht spielerischen Benutzung der Programmierung war es nur noch ein kleiner Schritt hin zu dem ersten "richtigen" Computervirus.

Als dann am Anfang der achtziger Jahre IBM den ersten gesellschaftstauglichen Computer entwickelte und auch Comodore ihren Homecomputer C64 herausbrachten, begann der begabte amerikanische Computerspezialist Fred Cohen 1984 die Geschichte des "wahren" Computer Virus mit seiner Schrift "Computer

Viruses, Theorie and Experiments". Er programmierte ausserdem in nur 8 Stunden ein Exemplar, das zu Beispiel Zwecken neben seiner Arbeit einer Gruppe von Spezialisten vorgeführt werden sollte. Trotz anfänglicher Skepsis mussten die Spezialisten schnell eingestehen, nachdem der von Cohen erschaffene Virus ohne Probleme ein "gesichertes" System austrickste und in kürzester Zeit vollkommene Kontrolle über dieses hatte, dass die Effizienz eines sich selbst reproduzierenden Virus enorm ist.

### **3. Definition eines Computer Virus**

Der ursprüngliche Begriff "Virus" kommt aus dem Griechischen und bedeutet in etwa "das Gift".

Ein Computer Virus ist nach dem großen PC & Internet Lexikon 2001 von Data Becker *"eine von Menschenhand geschaffene Programmsequenz, die - in ein Programm einpflanzt - sich reproduziert, indem sie das Wirtsprogramm zur weiteren Verbreitung des virulenten Codes veranlasst"*. Diese Definition ähnelt inhaltlich der von Fred Cohen formulierten klassischen Definition, die besagt, dass ein Virus ein Programm ist, das andere Programme infizieren kann, indem es diese so modifiziert, dass sie eine eventuell modifizierte Kopie von ihm enthalten.

Beide Definitionen besagen, dass ein Programm als Virus klassifiziert werden kann, wenn es die Fähigkeit hat, sich durch Infektion zu verbreiten, wobei eine Funktion direkten Schaden anzurichten, nicht erforderlich ist. Das heisst gleichzeitig, dass ein Destruktives Programm nicht unbedingt ein Virus sein muss.

#### **3.1 Wie werden Computer Viren erzeugt?**

Ältere Viren wurden oft in Assembler geschrieben, jedoch ist Assembler nicht mehr die allerneueste Sprache. Tatsächlich ist es für die heutige Generation der Virusprogrammierer praktischer und auch einfacher eigene Viren in C++ oder Delphi zu schreiben, da zum einen aufgeblasene Dateien unter Windows weniger auffallen und zum anderen der Festplattenplatz und der Arbeitsspeicher immer grösser und billiger werden. Doch

zum Pech der Viren-Entwickler oder zum Glück der PC-/Internetbenutzer ist es schwieriger einige Virusarten in einer der Hochsprachen zu schreiben anstatt in Assembler, was dann vom Entwickler eine gewisse Programmiererfahrung benötigt. Doch nicht alle bestehenden Viren sind neue Viren, viele sind nur Varianten eines tatsächlich existierenden Virus mit einer kleinen Veränderung, die aber seine eigentliche Funktionalität (Replikation etc.) nicht beeinträchtigt.

Ausserdem widmen sich einige Virusprogrammierer seit geraumer Zeit nicht mehr nur dem Programmieren eines oder ihres Virus, sondern fertigen sogn. Virus-Kits an, womit "Möchtegern-Virusprogrammierern" die Möglichkeit geschaffen wurde mit Hilfe dieser Kits eigene Viren zu erschaffen. Da sich jedoch die Kit-Viren anhand des erzeugten Viruscodes der Virusgeneratoren ähneln, steuern diese Kits nur zum Anstieg der Gesamtzahl aller Viren, jedoch nicht zum Anstieg der Viren "In the Wild" (siehe 5.1) bei.

Doch scheint es auch immer noch Leute zu geben, die glauben, dass Computerviren genau wie ihre Namensvettern, die biologischen Viren, spontan auftreten und sich selber entwickeln. Doch allzu Realitätsfern liegen sie damit eigentlich gar nicht, da es durchaus Variationen gibt (besonders seit der Entstehen der Makroviren 1995), die sich ohne menschliches Zutun, nach ihrer Replikation und Infizierung geändert haben. Die ursprüngliche Version eines Virus musste bisher dennoch von jemandem geschrieben werden. Doch theoretisch wäre es möglich, dass ein Virusprogramm ohne direkte menschliche Einwirkung erzeugt werden könnte, wenn eine Betriebsumgebung generelle Verbreitung finden würde. Doch bisher scheint dies noch nicht der Fall zu sein.

### **3.2 Wie verbreitet sich / arbeitet ein Computer Virus?**

Früher konnten sich Viren größtenteils nur per Diskette verbreiten, doch mittlerweile ist besonders der Dateiaustausch per Internet das effizientere Verbreitungsmedium. Wer glaubt, dass er durch Originalsoftware nicht infiziert werden kann, täuscht sich gewaltig, da auch in solchen Paketen häufig Viren, wenn auch unabsichtlich, integriert sein können. Doch die grösste Gefahr droht vor allem beim Herunterladen von

Programmen, welche unwissentlich schon verseucht sind, und beim Öffnen des Anhangs einer E-Mail, die von einer unbekanntem Adresse geschickt wurde.

Zum technischen Aufbau eines Virus lässt sich sagen, dass es (wie unter 4.3 und 4.3.1 beschrieben) viele verschiedene Virenarten und Eigenschaften gibt, die aber trotzdem fast alle aus mindestens drei Grundkomponenten bestehen. Zum einen hat der Virus eine infizierende Routine, auch Infektorteil genannt, welcher für ein korrektes Identifizieren und Infizieren des Wirtprogramms sorgt. Diese Routine sucht alle möglichen Wege für eine Infektion, tarnt alle verdächtigen Aktivitäten, damit der Virus nicht erkannt wird, und führt, falls vorhanden, eine Schadensroutine (Payload) aus. Als Auslöser bezeichnet man das Wirtsprogramm, welches er schon infiziert hat, da der Virus erst durch den Start der Wirtsdatei "ausgelöst" / aktiv werden kann. Es kann aber auch vorkommen, dass die Auslösebedingung z.B. eine bestimmte Datums- oder Zeitangabe ist und mit einem zerstörerischem Payload kombiniert, bezeichnet man diese Routine dann auch als logische Bombe. Die dritte und letzte Standardkomponente bezeichnet man als Statusroutine, welche ein mehrfaches Infizieren einer Datei unterbinden soll und dazu in der Regel ein einziges Flag-Bit in die Wirtsdatei setzt, welches der Virus vor der Infektion überprüft.

### **3.3 Computer Virus Typen**

Man kann Computerviren bequem in fünf Hauptarten einordnen, doch leider kann nicht jeder Virus als eine der fünf Arten klassifiziert werden, da es immer "spezielle" Viren gibt.

#### **Bootsektor- und Partitionsviren (BSIs - Boot Sector Infectors)**

Boot-Viren verankern sich zumeist im ersten physikalischen Sektor, dem Boot-Record (DBR), einer Diskette oder im Master Boot Record (MBR), welcher manchmal auch als Partitionssektor bezeichnet wird, einer Festplatte. Ist eine Festplatte partitioniert, so ist der erste Sektor jeder Partition der Boot-Record, in welchem ein Programm die Bootfähigkeit des Datenträgers überprüft und bei Erfolg die Kontrolle an das Betriebssystem übergibt. Da jedoch sowohl der MBR als auch der DBR meistens nicht genügend Platz für den Eindringling bieten, verschiebt dieser zumeist jenes Programm

an einen anderen Ort des Datenträgers und ersetzt es durch eigene Routinen, oder patched es teilweise einfach um.

Wird jetzt beim Start des Computers der jeweilige Bootsektor nach Grundinformationen abgefragt, startet der im Bootsektor verankerte Virus automatisch mit und infiziert, während er aktiv ist, die Bootsektoren aller nicht schreibgeschützten Datenträger (Festplatten, Disketten usw.).

Der Boot-Virus macht heute nur noch einen sehr geringen Teil der Gesamtanzahl der "In the Wild" (siehe 6.1) Bedrohungen aus. Selbst dieser Anteil schwindet immer mehr und neue BSIs gibt es kaum noch, was wohl auch an der Computer Technisierung der Privaten Haushälter liegt und Daten nicht mehr per Diskette, sondern vermehrt per E-Mail und Netzwerken ausgetauscht werden. Ausserdem kann auch sehr gut die Tatsache, dass Bootsektor Viren eindeutig schwieriger zu programmieren sind als Makroviren und Skriptviren eine Rolle an ihrem Rückgang spielen. Trotz alledem sollte man überaus vorsichtig sein, da besonders alte Boot-Viren, die z.b. noch auf einer alten unformatierten Diskette im Bootsektor schlummern, in Umgebungen für die sie nicht geschrieben wurden einen weitaus grösseren Schaden anrichten können, als sie ursprünglich sollten.

### **Dateiviren (parasitische Viren)**

Dateiviren infizieren ausführbare Dateien (.exe- , .bat- und .com-Dateien unter Dos / unter Windows ausserdem noch DLLs, Overlay-Dateien, VxDs und andere Klassen von Treibern und sogar bestimmte Screensaver und Font-Dateien).

Man unterscheidet in der Familie des Dateivirus zwischen überschreibenden und nicht überschreibenden Viren. Der überschreibende Virus (overwrite virus) ersetzt / überschreibt den vorhandenen Code einer infizierten Datei mit seinem eigenem. Der nicht überschreibende Virus (anhängender Virus), der auch als Linkvirus bezeichnet wird, hängt seinen virulenten Code hinten an den Code des Wirts an oder setzt sich selbst vor den Wirtscod, wobei die ausführbare Datei zumeist weiterhin funktionsfähig bleibt. Dennoch kann es passieren, dass durch schlechte Programmierung oder durch Inkompatibilitäten mit der Codebasis von der Wirtsdatei diese zerstört wird. Wird eine infizierte Datei ausgeführt, so startet der Virus automatisch mit und versucht meistens

sofort, weil er schnell das ganze System kontrollieren will, andere erreichbare Dateien zu infizieren.

Der Dateivirus ist die häufigst vorkommende Virenart, wobei sie trotz alledem nicht sehr erfolgreich ist und ihr Anteil an der Gesamtanzahl der "in the wild" Viren (siehe 6.1) ist sehr gering, obwohl man trotzdem noch erwähnen muss, dass diejenigen Viren, die es "in der Wildnis" überlebt haben sich erstaunlich gut verbreiten.

### **Mehrteilige-(Hybrid-)Viren (Multipartite Virus)**

Hybrid-Viren verfügen über mehr als einen Infizierungsmechanismus. Das bedeutet das z.b. Boot-Sektoren als auch ausführbare Binärdateien infiziert werden können und das der Virus damit viel flexibler ist. Da der Aufwand eine solche Art zu programmieren viel höher ist, kommt es nicht selten vor das die Hybriden über bestimmte Tricks verfügen, um sich vor aufspürenden Programmen zu verstecken und sich vor der Entfernung zu schützen.

### **Makroviren**

Makros sind im Wesentlichen Methoden zur Modifizierung der Anwendungsumgebung.

Man kann einen Makrovirus zwar als eine spezielle Art eines Dateivirus ansehen, doch unterscheidet er sich zum einen darin, dass er nicht die Datendatei ändert, sondern lediglich die Umgebung und zum anderen weil er keine ausführbaren Dateien infiziert. Besonders erfolgreich sind Makroviren in den Microsoft Office Anwendungen, da diese den ausführbaren Code (Makros) in der Datendatei zulassen. Hat ein Virus erst mal eine Datei infiziert, "verseucht" er meist auch gleich die Stamm-Dokumentvorlage und infiziert damit automatisch alle neuerstellten Dokumente mit. Weniger anfällig hingegen sind jene Anwendungen, die Daten und ausführbaren Code trennen. Besonders die Mächtigkeit der Makrosprache und ihren Funktionen wie z.b. sich selbst kopieren, DOS- und sogar Windows-API-Befehle aufrufen, sich mit einer Read-only-Funktion für nachträgliche Untersuchungen unzugänglich zu machen und vielen mehr lässt auf das wahre Schadenspotential schliessen.

Anfänglich wurden die Makroviren noch als Scherz abgetan, doch als die Entwicklung und die Anzahl der neu entstandenen Viren drastisch zunahm überstieg die Anzahl, der Makroviren, durch keinen Schutzmechanismus gehindert, schnell die der anderen Virenarten. Neuere Versionen verhalten sich noch viel geschickter und einige der polymorphen Makroviren (siehe 4.3.1) schaffen es lange aktiv zu bleiben, ohne die Normal.dot (Standard-Dokumentvorlage unter Word) zu verändern.

### **Scriptviren**

Der Script-Virus besteht hauptsächlich aus VBScript oder JScript, da diese im Gegensatz zu beispielsweise JavaScript viele E/A-Funktionen anderer Variationen im Visual-Basic-Bereich bieten. Oft profitieren Scriptviren von Schwachstellen im Internet Explorer oder einfach falscher Konfiguration. Der virulente Code versteckt sich meistens im Sourcecode anderer VBS-Skripts und/oder in HTML-Seiten. Wird eine Seite im Internet aufgerufen und die Script-Dateien ausgeführt, erfolgt die Infektion des Systems.

Momentan haben Scriptviren jedoch in der Praxis weniger Bedeutung und sind auch viel weniger verbreitet als ihre Artgenossen.

Bei jeder der zuvor aufgeführten Viren Arten gibt es sowohl böswillige als auch weniger schädliche Viren. Vom Prinzip her ist zwar jeder Virus böswillig, da alle Viren Festplattenplatz, Arbeitsspeicher und/oder Prozessorzeit in Anspruch nehmen, aber trotzdem muss man zwischen Viren unterscheiden, die nicht nur alleine auf Replikation aus sind, wobei sie keinen direkten Schaden anrichten, sondern auch Dateien und/oder das System mutwillig zerstören. Es gibt trotz alledem auch noch weitere Ausnahmefälle, in denen z.B. ein nur auf Infizierung und Vermehrung programmierter Virus eigentlich unbeabsichtigt dem System schadet, doch liegt das dann meistens an der inkompetenten Programmierung oder der Inkompatibilität zwischen der Umgebung für die der Virus geschrieben wurde und der Umgebung in der er derzeit aktiv ist.

Des Weiteren gibt es noch eine Art von Viren die im Sinne der allgemeinen Definition von Cohan überhaupt gar keine Viren sind, doch in vielen Fachbüchern trotzdem

erwähnt werden. Die sog. Hoax (Scherz oder Ulk) Viren sind Virenwarnungen, die z.B. per E-Mail dazu auffordern die Meldungen an alle bekannten Adressen weiter zu leiten. Der Virus besteht eigentlich nur darin, dass sehr viele Mail-Boxen mit sinnlosen Informationen voll gestopft werden.

### **3.3.1 Typen Eigenschaften**

Die folgenden Eigenschaften kann man nicht unbedingt auf bestimmte Viren-Arten beschränken, da jede Art theoretisch eine oder mehrere dieser Eigenschaften haben kann.

#### **Tarnkappen Viren (Stealth-Viren)**

Vom Prinzip her ist jeder Virus eine Art Tarnkappen Virus, da er normalerweise versucht unentdeckt zu bleiben, um die Wahrscheinlichkeit sich effizient zu vermehren zu erhöhen. Ein Virus mit Stealth-Eigenschaften kann über verschiedene Funktionen verfügen seine Anwesenheit zu vertuschen. Zumeist versucht er zu verbergen, dass er Dateien oder Sektoren manipuliert hat und gaukelt dem anfragendem System eine unberänderte Umgebung vor, indem er die Umgebung vor der Infektion speichert und bei Anfrage bestimmter Informationen durch das Betriebssystem nicht mit den aktuellen Daten antwortet, sondern die zuvor gespeicherten benutzt. Um aber die Zugriffe auf den infizierten Wirtscodes zu erkennen und die Täuschung auszuführen, muss trotzdem ein Teil des Viruscodes resident im Speicher sein.

Dadurch, dass eine Virenart sich mit solchen Stealth-Eigenschaften verbirgt, erhöht sie ihre Überlebenschancen grundlegend und kann sich daher auch wesentlich besser als normale Viren verbreiten.

#### **Polymorphe Viren**

Normale Viren hängen an jeden neu infizierten Wirt den gleichen Code an wie beim Vorgänger. Nicht jedoch ein Polymorpher Virus. Die ersten Viren dieser Art beschränkten sich darauf z.B. die Reihenfolge der Anweisung bei jedem neuen Wirt zu

verändern oder fügten Ballast-Bytes und Scheinanweisungen ein um den angehängten / vorgestellten Code anders aussehen zu lassen. Neuere Polymorphe Viren verfügen über ausgeklügelte variable Verschlüsselungen, die zum einen die Menge des nicht veränderten Codes verringern (der code der zum Verschlüsseln benutzt wird) und zum anderen meist mehrere Millionen verschiedene Verschlüsselungen des virulenten Codes erzeugen können.

Ein weiterer Trend war die Entwicklung sogn. polymorpher Verschlüsselungshilfen, mit denen andere Virusprogrammierer die Möglichkeit hatten ihre Eigenkreation mit einer polymorphen Eigenschaft zu versehen. Der einzigste Nachteil dieser fremd-programmierten Engines war es, dass wenn eine bekannt wurde, alle Viren die seine Verschlüsselungshilfen benutzten zuverlässig gefunden wurden, was wahrscheinlich der Grund dafür ist, dass die Verbreitung dieser Viren nicht so hoch war wie erwartet.

### **Tunnelnde Viren**

Arten die residente Wächterprogramme, also Wächter die an sensiblen Interrupts des System auf der Lauer liegen und illegale Aufrufe registrieren und den Benutzer warnen, umgehen, nennt man "tunnelnde" Viren. Ein solcher Virus wartet nicht im Speicher bis ein Interruptaufruf geschieht um dann einen neuen Wirt zu infizieren, sondern er verfolgt innerhalb des Speichers den Weg, den ein solcher Aufruf nehmen würde und sucht im BIOS nach dem Anfang des Original-Interrupthandlers, wo er dann direkt diese Adresse aufruft. Es gibt aber Wächterprogramme die dieses sogn. "Interrupt Tracing" unterbinden können.

### **Speicherresidente Viren (TSR Viren)**

Beim Aufruf einer Infizierten Datei gelangt der Virus in den RAM-Speicher des Systems. Hinterlässt er dort dauerhaft Teile seines Codes so "residiert" er quasi im RAM des Computers, daher auch der Name. Ist der Eindringling erstmal im Speicher kann er sogar nach Beendigung des Wirtsprogramms, nachdem er sich zumeist Zwischen verschiedene Interrupts, über die die Steuerung des Systems erfolgt, gesetzt hat, Objekte infizieren, auf die im späteren Verlauf zugegriffen wird.

Fast alle lebensfähigen Boot-Sektor-Viren sind speicherresident, da sie sonst nur bei Ausführung der Boot-Sequenz aktiv sein würden und damit kaum die Möglichkeit hätte andere Boot-Sektoren zu infizieren.

### **Direct Action Viren**

Im Gegensatz zu den Speicherresidenten Viren, kann ein Direct Action Virus nur zur Laufzeit des Wirtsprogrammes andere Dateien/Sektoren infizieren. Meistens durchsucht der Virus vorhandene Laufwerke bzw. Verzeichnisse nach möglichen Wirten und versucht diese zu verseuchen. Dadurch das ein Virus direkt handelt, und sich nicht erst im Speicher des Computer einnistet, bleibt ihm jedoch die Möglichkeit verwehrt die Stealth-Technik zu benutzen, da er keine Kontrolle über Anfragen hat und sie diese dann auch nicht manipulieren kann. Ein Vorteil eines Direct Action Virus ist es jedoch, das er definitiv nicht auf im Speicher residierende Wächter trifft und daher von ihnen unerkannt bleibt.

## **4. Wer schreibt Computer Viren und warum?**

Hauptsächlich handelt es sich um männliche Programmierer, was evtl. für den einen oder anderer etwas verwunderlich erscheinen kann, doch nach der Studie von Sarah Gordon hat sich ergeben, dass an Viren, die es geschafft haben "in the wild" zu überleben, tatsächlich nie weibliche Programmierer eine wichtige Rolle gespielt haben. Es gibt ausserdem gewisse Stereotype, die mit der Programmierung von Viren in Verbindung gebracht werden, doch treffend und eindeutig wird ist keines von ihnen. Es kann auch sehr viele verschiedene Gründe geben Viren zu schreiben, ob es nun der Spassfaktor für Jugendliche ist oder ob es Racheakte sein soll. Jedoch lässt sich alles nicht wirklich eindeutig bestimmen und wenn man sich damit länger auseinandersetzen würde, würde man wahrscheinlich genug Stoff für eine eigene Facharbeit erhalten. Für diejenigen, die dieses Thema trotzdem stark interessiert, kann ich nur die beiden Texte „The Generic Virus Writer I + II“ von Sarah Gordon empfehlen, die sich einige Jahre verstärkt damit auseinander gesetzt hat.

## 5. Aktueller Virenstand

Derzeit gibt es ungefähr 50.000 – 60.000 Viren, je nachdem wie Sie messen. Nach der WildList Organization sind davon 199 im März 2002 „In-the-Wild“. In der Ergänzungsliste stehen ausserdem noch 421 Viren, die schon einmal „In-the-Wild“ waren oder Anwärter dafür sind. Einer der Medienaktivsten Viren war in der vergangenen Zeit der „i love u – Virus“.

### 5.1 Was bedeutet » in the wild « ?

Nach dem Konferenzartikel Counting Viruses (Virus Bulletin 1999) von Paul Ducklin heisst es:

*"Ein Virus wird dann als In-the-Wild-Virus betrachtet, wenn er sich als Ergebnis normaler alltäglicher Vorgänge auf und zwischen den Computern nichts ahnender Benutzer verbreitet. Das bedeutet, dass Viren, die einfach nur existieren, sich aber nicht ausbreiten, nicht als In-the-Wild-Viren betrachtet werden."*

Das bedeutet auch, dass Viren die sich innerhalb der Forschungsumgebung von z.B. Anti-Virus-Herstellern befinden, auch nicht zu den abgekürzt ItW-Viren zu zählen sind. Auch wenn ein Vires in einem vx-Bulletin-Board oder einer Website verfügbar ist, bedeutet dies nicht, dass er "in der freien Wildbahn" ist.

Die WildList Organization, die sich speziell nur mit dem Problem Viren in freier Wildbahn befassen, definiert einen ItW-Virus noch strenger, da mindestens zwei oder mehr Virusspezialisten, die mit der WildList Organization in Verbindung stehen, auf einen Virus aufmerksam gemacht haben müssen, damit dieser in die "WildList" aufgenommen wird. Das bedeutet natürlich, das die WildList nicht unbedingt alle ItW-Viren zu einer bestimmten Zeit umfasst, dafür enthält sie aber auch nur Viren, die wirklich "in der Wildniss" ihr Unwesen treiben.

## 6. Fazit

Da immer mehr Haushalte „online“ gehen und der Datenaustausch per Internet immer weiter zunimmt, wird das Thema Computer Viren auch noch sehr lange aktuell bleiben. Je länger sich sowohl private als auch kommerzielle Anwender ahnungslos oder mit der Einstellung „Ich bekomme keinen Virus! Ich doch nicht!“

mit dem Thema Sicherheit befassen, desto öfter wird sich solch ein Debakel wie mit dem „i love u – Virus“ wiederholen. Auch haben die Virenprogrammierer noch längst nicht alle Möglichkeiten ausgeschöpft und es wird in der Zukunft sicherlich neue Viren geben die über ganz neue Tarnungsmöglichkeiten verfügen und sich aufgrund des nicht vorhandenen Schutzes rasend ausbreiten werden.

## 7. Quellen

### **Bücher:**

Felix Martin, "Virus Report '98"  
Data Becker, Dr.Andreas Voss, "Das große PC & Internet Lexikon 2001"  
Data Becker, wolfram Gieseke, "Viren bekämpfen!"  
anonymous, "hacker's guide"  
anonymous, "der neue hacker's guide"

### **Internet:**

20.03.2002:  
[www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/edv/viren/pcviren.htm](http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/edv/viren/pcviren.htm)  
<http://home.t-online.de/home/adolf.merz/referate/software/sonstige/rfswvirt.htm>

23.03.2002:  
[www.badguys.org/papers.htm](http://www.badguys.org/papers.htm) (The Generic Virus Writer I + II)  
[www.fuhs.de/buch/](http://www.fuhs.de/buch/)

01.04.2002:  
<http://temp.wildlist.org/WildList/200203.htm>