Computerviren

# Geschichte der Computer-Viren

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

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

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

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

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

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

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

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

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

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

Bisher waren die Programmierer von Anti-Virus-Software in der Lage, den Vorsprung der Viren-Programmierer im Wettlauf mit der Zeit immer relativ rasch einzuholen. Es ist aber zu befürchten, dass die Zeitspanne zwischen Auftreten eines neuen Virus und der Erstellung des passenden Gegenmittels immer länger wird. Daher sollte geprüft werden, ob nicht vom Gesetzgeber der Veröffentlichung von Viren-Code und insbesondere der Verbreitung von Viren-Baukästen ein wirksamer Riegel vorgeschoben werden kann.

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

# Definitionen und Wirkungsweisen

Computer-Viren gehören zu den *Programmen mit Schadensfunktionen* . Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Daten oder Programmen sicherlich von grösster Tragweite. Solche Funktionen von Programmen können sowohl unbeabsichtigt als auch bewusst gesteuert auftreten.

Die Definition eines Computer-Virus bezieht sich nicht unmittelbar auf eine möglicherweise programmierte Schadensfunktion:

*Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.*

Die Eigenschaft der Reproduktion führte in Analogie zum biologischen Vorbild zu der Bezeichnung «Virus». Die Möglichkeiten der Manipulation sind sehr vielfältig. Besonders häufig sind das Überschreiben oder das Anlagern des Virus-Codes an andere Programme und Bereiche des Betriebssystems, wobei dies immer so geschieht, dass zunächst der Virus-Code und dann erst das ursprüngliche Programm ausgeführt wird.

## Aufbau eines Computer-Virus

1. **Reproduktionsteil**

Mit diesem Programmteil wird die Vermehrung des Virus durchgeführt.

1. **Erkennungsteil**

Im Erkennungsteil wird geprüft, ob bereits die Infektion eines Programms oder Systembereichs erfolgte. Die Verbreitung wird beschleunigt, wenn der Virus auf eine Infektion «verzichten» kann, weil sie bereits geschehen ist. Jedes Wirts-Programm wird daher nur einmal infiziert. Die Entdeckung wird damit auch verzögert, da durch mehrfache Anlagerung des Virus-Codes die Dateien sonst so gross werden, dass sie entweder nicht mehr ausführbar sind oder aber dem Benutzer die Grössenveränderung schneller auffällt.

1. **Schadensteil**

In einigen Viren ist absichtlich eine Schadensfunktion programmiert, meist das Überschreiben oder Verändern von Programmen oder Daten, oder aber auch nur die Ausgabe von Meldungen und Geräuschen auf dem Rechner. Dieser Programmteil kann fehlen, aber auf jeden Fall entsteht Schaden durch Inanspruchnahme von Speicherplatz im Hauptspeicher und auf Datenträgern. Durch Programmierfehler, Veränderungen des Betriebssystems oder ähnliches können weitere Schäden als Nebeneffekte auch dann auftreten, wenn sie nicht absichtlich programmiert sind *(siehe auch 1.3* Computer-Viren und Betriebssysteme*).*

1. **Bedingungsteil**

Sowohl die Verbreitung als auch die Schadensfunktion können von Bedingungen abhängig programmiert sein, z. B. tritt bei einigen Viren der Schaden an einem bestimmten Datum oder bei einer bestimmten Anzahl von Aufrufen ein. Auch dieser Teil kann fehlen.

1. **Tarnungsteil**

Hierunter fallen Programmroutinen, um die Entdeckung des Virus im infizierten System zu erschweren. Dieser Teil ist meist nur bei neueren Viren zu finden.

Obwohl Computer-Viren prinzipiell bei jedem Computertyp und Betriebssystem denkbar sind, erlangten sie bei IBM-kompatiblen Personalcomputern (PC) die grösste Bedeutung. Bei den hier am meisten verbreiteten Betriebssystemen (MS-DOS, PC-DOS, DRDOS, NOVELL DOS etc.) wurden Anfang 1994 weltweit rund 4000 Viren (einschliesslich Varianten) gezählt. Entsprechend vielfältig sind weitere Merkmale und Eigenschaften.

## Grundtypen von Computer-Viren

1. **Boot-Virus**

Als «Booten» bezeichnet man das Laden des Betriebssystems. Hierbei werden u. a. Programmteile ausgeführt, die zwar eigenständig sind, sich aber in sonst nicht zugänglichen und im Inhaltsverzeichnis der Disketten und Festplatten nicht sichtbaren Sektoren befinden. Boot-Viren überschreiben den Boot- oder Partition-Sektor mit ihrem Programm. Der originale Inhalt wird an eine andere Stelle auf dem Datenträger verlagert und dann beim Start des Computers anschliessend an den Virus-Code ausgeführt. Dadurch startet der Computer scheinbar wie gewohnt. Der Boot-Virus gelangt jedoch bereits vor dem Laden des Betriebssystems in den Arbeitsspeicher des Computers und verbleibt dort während der gesamten Betriebszeit. Er kann deshalb den Boot-Sektor jeder nicht schreibgeschützten Diskette infizieren, die während des Rechnerbetriebs benutzt wird, und sich auf diese Weise auf andere Computer übertragen.

Bei Computer-Netzen verwendet der File-Server in der Regel ein anderes Betriebssystem als MS-DOS. Boot-Viren können sich über diese Computer dann nicht ausbreiten. Der Boot-Versuch kann jedoch schon wichtige Systembereiche des Server-Betriebssystems zerstören.

1. **File-Virus**

Die meisten File-Viren lagern sich an Programmdateien an. Dies geschieht jedoch so, dass beim Aufruf auch hier der Virus-Code zuerst ausgeführt wird und erst anschliessend das originale Programm. Dadurch läuft das Programm anschliessend wie gewohnt und der Virus wird nicht so schnell entdeckt. Es sind jedoch auch primitivere, überschreibende Viren bekannt, die sich so an den Anfang des Wirts-Programms setzen, dass dies nicht mehr fehlerfrei läuft.

**Weitere Typen von Computer-Viren sind im** Anhang E - Glossar **erläutert.**

## Vorgang der Infektion

Computer-Viren sind nicht selbständige Programmteile, die als «Wirt» immer ein Programm oder programmähnliche Speicherbereiche des Betriebssystems benötigen. Über Daten-Dateien können sich Viren daher nicht verbreiten.

1. **durch Boot-Viren**

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

Deshalb kann auch der Boot-Versuch von einer im Laufwerk A: vergessenen Daten-Diskette eine Infektion bewirken. Wenn man nach der Fehlermeldung (Text ist dabei vom Hersteller, der Sprache und von der Version des Betriebssystems abhängig)

**«Kein System oder Laufwerksfehler 🡪 Wechseln und Taste drücken»**

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

1. **durch File-Viren**

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

# Computer-Viren und Betriebssysteme

Die unter 1.1 erwähnte Grundsatzarbeit zu Computer-Viren von Fred Cohen wurde mit Beispielprogrammen unter dem Betriebssystem UNIX belegt. In der Praxis besteht jedoch die grösste Bedrohung unter dem Betriebssystem MS-DOS und kompatiblen. Dies liegt sicherlich vorwiegend daran, dass es die grösste Verbreitung sowohl im professionellen als auch im privaten Bereich hat. Dadurch gibt es wesentlich mehr Personen, die auf dieses Betriebssystem Zugriff haben. Auch das Konzept von MS-DOS ist in vielen Aspekten einfacher und damit aus Sicht eines Programmierers leichter zu beherrschen. Während unter UNIX Programme oft erst für eine bestimmte Hardware «generiert» werden müssen, liegen sie unter MS-DOS normalerweise in lauffähiger Form vor. Auch andere Computer-Betriebssysteme liegen hinsichtlich ihrer Verbreitung deutlich hinter MS-DOS. Es haben sich jedoch neben dem eher auf grösseren Computern anzutreffenden UNIX auch einige Betriebssysteme für die preiswertere Hardware der IBM-kompatiblen Computer stärker verbreitet.

Von den unter Kapitel 1.7 angeführten Makro-Viren abgesehen, sind Computer-Viren sehr eng an die jeweilige Computer-Hardware und das jeweilige Betriebssystem gebunden. Sie laufen nicht auf unterschiedlichen Mikroprozessoren, d. h., IBM-kompatible, auf der Basis des Prozessors 8086 der Firma Intel (und kompatible) arbeitende Viren können sich z. B. auf Macintosh-Computern nicht in gleicher Weise ausbreiten. Ähnliches gilt für die von MS-DOS abweichenden Betriebssysteme auf den IBM-kompatiblen Computern, z. B. LINUX.

Ausserdem bestehen zwischen Boot- und Datei-Viren Unterschiede bei der Verbreitung: Boot-Viren werden durch das Laden des Betriebssystems («Booten») oder den Boot-Versuch von einer infizierten Diskette auf den Boot - oder Partition-Sektor der Festplatte übertragen, Datei-Viren durch den Start eines infizierten Programms. Ist ein anderes Betriebssystem installiert, so können Boot-Viren zwar trotzdem die Festplatte infizieren, sich dann aber nicht weiter ausbreiten. Selbst in den DOS-Emulatoren bzw. sogenannten DOS-Boxen der anderen Betriebssysteme sind sie dann nicht wie sonst im Speicher resident . Wie im Kapitel 2 - Vorbeugende Massnahmen noch erläutert wird, kann man eine Infektion mit Boot-Viren jedoch bei modernen Computern durch Umstellung der Boot-Reihenfolge vollständig vermeiden.

Einige Datei-Viren von MS-DOS laufen in den bei den anderen Betriebssystemen vorhandenen DOS-Boxen. Diese wurden geschaffen, damit die vielen vorhandenen DOS- und Windows-Programme unter den abweichenden Betriebssystemen laufen können. Daher funktionieren auch einige Viren, insbesondere die einfacheren, die nicht aufwendig programmierte Eingriffe in das Betriebssystem vornehmen.

Tests mit den Betriebssystemen LINUX, OS/2 und WINDOWS NT, die z. T. andere Datei-Systeme verwenden, bestätigten die obigen Aussagen. Daher können übliche DOS-Viren-Suchprogramme auch weiterhin genutzt werden und sie bieten auch ausreichend Schutz (***Aktualität vorausgesetzt***).

Eine besondere Rolle nimmt WINDOWS ein, weil dies kein eigenständiges Betriebssystem ist, sondern eng mit MS-DOS verbunden arbeitet. Trotzdem sind spezielle Windows-Viren selten, und sie werden im Allgemeinen von den üblichen Suchprogrammen ebenfalls gefunden. Da hier die unter MS-DOS vorhandene Beschränkung des verfügbaren Speichers auf 640 kByte wegfällt, haben speicherresidente Anti-Virus-Programme für Windows eine neue Qualität erreicht *(siehe* Kapitel 2.3.3*).*

Einige Verbreitung vorwiegend im professionellen Bereich haben Hochleistungs-Computer (sogenannte Workstations) gefunden, die mit anderen als Intel-Prozessoren und kompatiblen arbeiten (z. B. RISC-Prozessoren). Computer-Viren für diese Rechner sind nur in geringer Zahl, oft nur für akademische Zwecke geschrieben und nicht oder nur selten in der Praxis bei Anwendern zu finden. Nachfolgend werden einige Betriebssysteme hinsichtlich der Bedrohung durch Computer-Viren betrachtet.

© 1997 by BSI – Bundesamt für Sicherheit in der Informationstechnik  
Godesberger Allee 183£  
53175 Bonn

[[Fügen Sie auf der ersten Seite unterhalb des Bildes ein Inhaltsverzeichnis ein. Danach löschen Sie diese zwei Zeilen.]]