

## COMPUTER - VIREN

- Virus                                    Ein Virus ist ein Programm, das geschrieben wurde, um einen Computer negativ zu beeinflussen, indem es ohne Wissen des Benutzers die Arbeitsweise des Computers verändert.
- Boot Viren                            Diese Programme sind im BootSektor von startbaren Datenträgern (Boot-Record 512Byte Langer Code)
- Programm Viren                    Diese Viren hängen sich an Programme an und werden durch die Weitergabe von Programmen oder via E-Mail verbreitet.
- Makro Viren                         Viren die auf den Programmierumgebungen von Standard Anwendungen basieren
- Wurm Viren                         Diese Programme können sich selbständig auf andere Systeme übertragen (replizieren)
- Hoaxes                                Sind Computerviren, die keine sind (sog. "Hoaxes") und weitere Falschmeldungen und Gerüchte.
- Trojanisches Pferd                Meistens verfügen Trojanische Pferde über ein für Anwender sehr nützliche Funktion. Die schädliche Funktion läuft lediglich im Hintergrund ab,
- Schutz vor Viren                    Anti-Virus Software wie Norton AntiVirus der sich via Internet UpDaten lässt (1 Jahr im Kaufpreis inbegriffen)  
Firewall's sind keine AntivirenGarants oder nur sehr schlechte!!

### Virus:

Ein Virus ist ein Softwareprogramm, das geschrieben wurde, um einen Computer negativ zu beeinflussen, indem es ohne Wissen des Benutzers die Arbeitsweise des Computers verändert.

Viren haben meist zwei Funktionen:

Viren verbreiten sich selbst von einer Datei zur nächsten. Technisch wird dieser Vorgang als Selbstvervielfältigung und -verbreitung bezeichnet.

Der Virus bewirkt die von seinem Erzeuger beabsichtigten Symptome oder Schäden. Häufige Schäden sind das Löschen von Datenträgern, die Beschädigung von Programmen oder einfach das Erzeugen von Verwirrung und Durcheinander. Man bezeichnet dies als Auftrag des Virus, der je nach Lust und Laune des Erzeugers harmlos oder gefährlich sein kann.

### Boot Viren

Diese Viren sind auf Boot Sektoren von Festplatten oder Disketten. Wenn sich eine infizierte Diskette im startbaren Laufwerk A: befindet, so wird bei einem Boot Versuch das Boot Programm ausgeführt, das dann meldet: "Kein Betriebssystem gefunden weiter mit jeder Taste". Und schwups schon ist der Virus von der Diskette auf die Festplatte C: hinüber transferiert worden. Nach einem Neustart des PC's ab der Festplatte C: ist der Virus aktiv. Nun wird jede Diskette die ins Laufwerk A: gesteckt wird sofort mit dem Virus versehen! Oh oh?

### Programm Viren

Da Programme durch das Betriebssystem gestartet werden liegt nichts näher, als sich an Programme anzuhängen. Dies kann als effektives Infizieren von .EXE oder .COM (.SYS & .OVL) Dateien angesehen werden. Wird eines dieser infizierten Programme ausgeführt, so wird der Virus aktiv und arbeitet aus dem Arbeitsspeicher, es werden nun alle weiteren Programme die gestartet werden ebenfalls infiziert.

## Makro-Viren

Mitte 1995 schlug daher der Word-Makro-Virus "Concept" wie eine Bombe ein, denn bis dahin galt im allgemeinen, dass Viren nur ausführbare Programme infizieren. Zu der enormen weltweiten Verbreitung trug unter anderem Microsoft selber bei, indem unbeabsichtigt mehrere tausend CD's mit infizierten Dokumenten verschickt wurden.

## Wurm-Viren

Ein *Computer-Wurm* setzt sich aus einer Anzahl von Prozessen, den Wurm-Segmenten, zusammen. Diese sind auf die Rechner eines Netzwerks verteilt und haben die Möglichkeit, gemeinsam bestimmte Leistungen zu erbringen.

Ein *Wurm-Segment* ist ein eigenständiger Prozess, der die Fähigkeit besitzt, eine eventuell modifizierte Abbildung von sich selbst über das Netzwerk auf einen anderen Rechner zu übertragen und dort zu aktivieren. Die erzeugten Abbildungen müssen diese Eigenschaft ebenfalls besitzen. Das Verhalten aller zugehörigen Segmente bestimmt das Verhalten eines Computer-Wurms. Die Ausbreitung der Wurm-Segmente erfolgt im Gegensatz zu einem Computer-Virus ohne eine Infektion von Dateien.

Diese Definition enthält keinerlei Aussagen über den Zweck eines Computer-Wurms oder die mit einem Einsatz beabsichtigte Wirkung. Sie beruht auf technischen Verfahren und Eigenschaften, die charakteristisch für diese Art von Programmen sind. Es fallen also sowohl konstruktive als auch destruktive Ansätze unter diese Einordnung

**Beispiel:** Die Attacke des Nimda-Wurms ist offenbar vorbei. Zurück bleiben Schäden in einer Höhe von mindestens 4 Milliarden USD. Betroffen waren unter anderem die Online-Dienste der Fernsehsender ZDF und 3Sat und die Deutsche Bank.

Unter [www.sixworx.de](http://www.sixworx.de) kann jeder Internet-Nutzer testen, ob sein eigenes Windows-System gegen den Virus resistent ist. Startet der eigene Rechner nach dem Aufruf der Seite das Windows-Programm "Notepad", bedeutet dies, dass das System nicht sicher ist.

Die Indizierung durch Nimda wird auf 2 Mio. Rechner geschätzt. Es stehen dem Virus 4 verschiedene Möglichkeiten der Attacken zu Verfügung.

Experten sind sich darüber einig, dass Nimda der bisher ausgefeiltste Virus war. Sicher ist auch, dass die Folgen von Nimda schwerwiegender gewesen wären, hätte es vor wenigen Wochen den Code-Red-Virus nicht gegeben.

## Hoaxes

Die Situation - Seit Jahren kursieren Warnungen vor (angeblichen) Viren, die sich per Email verbreiten sollen. Diese "Warnungen" werden meist von gutgläubigen Unsern verbreitet, die diese per Email von ihresgleichen erhalten haben.

Fakt ist... , ... dass alle diese Warnungen keinen ernstzunehmenden Hintergrund haben (was die Gefährlichkeit der vermeintlichen Viren angeht).

Diese Warnungen werden **Hoaxes** genannt (*engl.* hoax, *altengl.* hocus: Scherz, Falschmeldung). Vielmehr stellen diese "Warnungen" die eigentlichen Viren dar, denn sie richten erheblichen Schaden an, in dem sie Menschen verunsichern und Arbeitszeit binden. Ausserdem belasten sie durch ihre nicht geringe Zahl das Internet durch nutzlosen Datenverkehr (zugegeben, da gibt es noch mehr Dinge, auf die das zutrifft).

Generell werden **nie echte** Viruswarnungen auf diese Weise in die weite Welt geschickt! Sehr wohl können aber Viren in Dateianhängen (Attachments) von Emails enthalten sein.

## Trojanisches Pferd

Trojanische Pferde sind Programme, die eine schädliche Funktion beinhalten. Nicht selten verfügen Trojanische Pferde über ein für Anwender sehr nützliche Funktion. Die schädliche Funktion läuft lediglich im Hintergrund ab, ohne das dieses bemerkt wird. Trojaner spähnen z.B. Passwörter, Kreditkartendaten oder andere sensible Daten aus oder erlauben die Fernsteuerung des Rechners.

**Schutz vor Viren**

Als erstes ist eine Antivirus Software zu verwenden die immer auf dem neusten Stand ist. Weiter sind alle Notwendigen Patch (Software-Korekturen) zu installieren. Es sind möglichst viele sicherheitsrelevante Anpassungen vorzunehmen. Z.B. Administrator mit Gast-Recht, DOS Kommandos in sep. Verzeichnis mit Admin Schutz usw...