

# VIREN und Co

Vor kurzem hat der sogenannte

## **"I Love You"-Virus**

zugeschlagen und weltweit Schäden in Milliardenhöhe angerichtet. Zwischenzeitlich machen auch verschiedenen Ableger von diesem Virus die Runde. Die Gefahr ist offenkundig und wird sich nach unserer Einschätzung durch Nachahmer / Mitläufer noch extrem verstärken.

Vor allen Dingen sind mangelnde Information über Funktionsweise und Verbreitungsmöglichkeiten von Viren eine der Hauptursachen für die Sorglosigkeit der Firmen und Anwender bei der Behandlung dieses Problems und führt daher zu immer grösseren Verunsicherungen bei den Betroffenen.

Um diese Verunsicherung zu minimieren, möchten wir allen Cyberforum-Mitgliedern diese Informationen zukommen lassen.

Roland Graber (Ingenieurbüro Graber)

Sie können sich dieses Dokument auch unter

**[www.graber.de/aktuelle.htm](http://www.graber.de/aktuelle.htm)**

bzw direkt unter

**[www.graber.de/infos/vireninfo.doc](http://www.graber.de/infos/vireninfo.doc)**

vom Internet herunterladen.

Dieses Dokument dient lediglich der Information und erhebt keinen Anspruch auf Vollständigkeit.

# VIREN und Co

## Allgemeine Infos - Entwicklung

Ein Virus folgt einfachen Grundregeln:

- **Infizieren**
- **Verteilen**
- **Aktionen ausführen**

Die Aktionen können harmloser Natur sein (einfache Meldung) oder auch erhebliches zerstörerisches Potential beinhalten (BIOS , Festplatte, Daten, Programme löschen). Selbst die Zerstörung von Hardware ist möglich.

Die schnell fortschreitende Entwicklung in der Softwareindustrie eröffnet Virentwicklern immer neue Möglichkeiten. In den Anfangszeiten (DOS) wurden Viren meist per Diskette verbreitet. Am beliebtesten waren die BOOT-Sektorviren. Besser und schwerer zu erkennen waren die Viren, welche sich an Programmen anlagern konnten.

Mit der Einführung neuer Betriebssysteme (wie z.B. Windows) wurden die Methoden ausgefeilter. Virenprogramme konnten jetzt besser versteckt werden (z.B. als Treiber, Programme, automatisch startende Hintergrundprogramme, ...).

Mit der zunehmenden Vernetzung wurden natürlich auch die Verbreitungsmöglichkeiten verbessert. Viren konnten durch verschiedene Lockangebote (Trojanische Pferde), wie z.B. einen Screensaver oder spezielle Spiele im Internet den Anwendern untergeschoben werden. Ein schönes Beispiel ist das aktuelle Trendspiel **Moorhuhn**. Kurz nach dessen Erscheinung wurden schon infizierte Versionen auf verschiedenen Servern angeboten.

Die Aktivierung der Viren findet hier noch auf die klassische Art- und Weise statt. Ein infiziertes **Programm** wird gestartet und somit der Virus aktiviert und das System infiziert.

Ein geradezu "**einmaliger Innovationssprung**" ist die Einführung von skript- und makrobasierten Programmen. Erstmals wurde es möglich, auch passiven Dokumenten (z.B. einem Textdokument) ausführbare Komponenten zuzuordnen. Einer der Vorreiter auf diesem Gebiet war Microsoft mit der integrierten Skriptsprache VBA (bzw. VBS), welche in vielen Microsoftprodukten integriert wurde (Word, Excel, ...). Die Funktionalität der Programme wurde hierdurch erheblich erweitert (insbesondere für Entwickler). Hierdurch wurde es erstmalig möglich, Viren nicht nur über Programme sondern **auch über Dokumente** selbst zu verbreiten.

Das Problem hierbei ist, dass **VBA alles erlaubt**, von der Ausgabe von einfachen Meldungen bis hin zur **kompletten Löschung aller Dateien** auf der Festplatte !

Die Erstellung eines entsprechenden Virenprogrammes in Word, wurde aufgrund eines integrierten Skriptrecorders selbst für Nichtentwickler auf einfache Art und Weise möglich.

**!!! Die Makro-Viren waren geboren !!!!**

Innerhalb kürzester Zeit erschien eine grosse Anzahl derartiger Viren. Selbstverständlich erschienen im *Nachhinein* verschiedene Patches und Programme um solche Makroviren erst gar nicht zuzulassen (der Benutzer wird vorab gewarnt !?!?!), indem meistens die Makrofähigkeit abgeschaltet wird !!!

Mit Einführung von Windows 98 wurde der Explorer in die Windows-Oberfläche integriert und Active Scripting wurde eingeführt. Active Scripting ist ein Mechanismus zur Ausführung von Script-Dateien, wie JavaScript und (innerhalb des Internet-Explorers) VBScript. Die entsprechenden Dateien (VBScript) haben die Endung **\*.VBS**. Diese Dateien werden als reine Textdateien übertragen und werden vom Betriebssystem interpretativ ausgeführt.

### **Ein Skript kann wirklich alles**

Programme ausführen, Dateien löschen, ... (s.o.).

## **Der "I LOVE YOU"-Virus**

Hier kommt jetzt das "I Love You"-Virus zum Einsatz. Eine interessante Nachricht mit einer angehängten VBS-Datei wird als eMail verschickt. Klickt der Empfänger die entsprechende Datei an, dann wird ihm die Möglichkeit gegeben, diese Datei zu sichern oder zu öffnen. Bei vielen Outlook-Konfigurationen wurde diese Sicherheitsmeldung deaktiviert und ein direktes Öffnen initiiert.

Ein Öffnen/Ausführen der Datei bewirkt jedoch die Ausführung des Virus (VBS-Datei) und schon kann dieser sein zerstörerisches Werk beginnen:

**Verteilen:** Der Virus (Skript) liest das Adressbuch von Outlook und schickt allen Personen eine gleichlautende eMail mit dem Virus als Anhang. Der Empfänger hält somit die empfangene eMail als vertrauenswürdig, da die eMail von einer bekannten Person kommt. Das Misstrauen des Empfängers sinkt und die Wahrscheinlichkeit der Verbreitung erhöht sich !!!

**Aktion:** Der Virus löscht (nach aktuellem Informationsstand) alle Bild und Wavedateien und eventuell auch Programme und kann somit als sehr aggressiv eingestuft werden.

**Bemerkung:** Das Speichern der Datei ist relativ unkritisch. Wird jedoch die VBS-Datei geöffnet (Doppelklick genügt), dann wird er aktiviert. Die Ablage des Virus als Textdatei (Programmcode ist direkt sichtbar) erklärt auch, warum es innerhalb **weniger Minuten** möglich ist, einen Ableger des Virus unter anderem Namen (wie z.B. motherday) zu generieren.

## Weitere sicherheitsrelevante Informationen

Selbstverständlich sorgt die Entwicklung im Internetbereich wiederum für weitere Möglichkeiten. Ein schönes Beispiel für die Integration und Adaption neuer Technologien sind die sogenannten **ActiveX**-Komponenten und **JavaApplets**. Während ActiveX-Komponenten im wesentlichen nur im Internetexplorer von Microsoft unter Windows laufen, sind Java-Applets konzeptuell auf jeder Plattform verfügbar.

Die Konzeption von ActiveX im Internetbereich mag schon etwas bedenklich stimmen. ActiveX-Komponenten sind im wesentlichen ausführbare Programme, welche bei Bedarf vom Server auf den lokalen Rechner geladen und ausgeführt werden. Die Ausführung erfolgt dann zwar sehr schnell aber Sicherheitsaspekte wurden nur rudimentär berücksichtigt. Um es klar und deutlich zu sagen.

### **Eine ActiveX-Komponente kann Ihre Daten im Hintergrund transferieren und auch die Festplatte löschen**

Beispiele, wie fremde Rechner ausspioniert und komplette Datenbestände ohne Wissen des Anwenders übertragen und gelöscht wurden, wurden zur Genüge in der Presse bekannt. Diesbezüglich wurden von Microsoft Nachbesserungen durchgeführt indem eine Zertifizierung solcher Komponenten eingeführt und verschiedene Warnlevel bzgl. deren Benutzung etabliert wurden.

### **Die Verantwortung für die Verwendung wird also im wesentlichen dem Anwender überlassen.**

(Unbedarfte Anwender sind meist froh, dass ihr System läuft und werden sich wohl kaum darauf einlassen die jeweiligen Programme je nach gesichteter Internetseite umzustellen !!!)

ActiveX-Komponenten sollten daher **nur in vertrauenswürdigen Umgebungen** eingesetzt werden. Dies ist einer der Hauptgründe, warum ActiveX-Komponenten meist im Intra- und Extranet, jedoch nicht im allgemein zugänglichen Internet verwendet werden.

**Java-Applets** sind speziell vorkompilierte Komponenten, welche auf den Rechnern der Anwender interpretativ ausgeführt werden. Ein Sicherheitskonzept wurde schon im Vorfeld berücksichtigt (Sandbox). Die Sicherheit ist um ein vielfaches höher als bei ActiveX und die Java-Applets laufen auf jedem Browser und Betriebssystem. Die Ausführung ist jedoch langsamer als die bei ActiveX-Komponenten. Dennoch wurden und werden immer wieder Fälle bekannt, bei denen Sicherheitslöcher entdeckt wurden, welche zur Spionage genutzt werden konnten.

## Typen von Viren und Technologien

### BOOT-Sektor-Viren

In DOS-Zeiten waren die Bootsektor-Viren die am häufigsten auftretenden Viren. Diese Viren lagern sich im Bootsektor einer Diskette an. Der Bootsektor wird normalerweise dazu genutzt ein Betriebssystem von Diskette zu laden. Wird der Rechner eingeschaltet und ist (auch zufällig) eine infizierte Diskette eingelegt, dann wird der Rechner infiziert. Jede weitere Diskette welche zum Beschreiben eingelegt wird, kann dann automatisch infiziert werden.

#### Vorbeugung

(Bester Schutz) Stellen Sie im BIOS-Setup die Startup-Sequenz so ein, dass immer zuerst von der Festplatte gebootet wird. Selbst wenn eine bootfähige Diskette beim Einschalten im Laufwerk liegt, wird das entsprechende Virenprogramm nicht aktiviert. Die Verbreitung kann nur noch durch das ein komplettes Kopieren der Diskette erfolgen. Viele BIOS-Einstellungen erlauben auch die automatische Überprüfung der BOOT-Sektoren (aktivierter Virenschutz).

Prüfen Sie immer vor dem Einschalten des Rechners, ob eine Diskette eingelegt ist und entfernen Sie diese.

Aktivieren Sie grundsätzlich den Schreibschutz von Disketten, wenn von diesen nur gelesen werden soll. Hierdurch wird verhindert, dass ein Virus (welcher sich schon auf dem Rechner befindet) weiter verbreitet wird.

#### Erkennung:

Diese Viren sind am leichtesten erkenn- und beseitigbar.

### Programmiviren

Diese Viren nisten sich in ausführbaren Programmen (EXE, COM, ...), indem Sie sich indem Sie die Startup-Sequenzen modifizieren und sich in die ausführbare Datei einschreiben.

Die Verbreitung war insbesondere in DOS-Zeiten beliebt, da dort keine Installation kompletter Programme erfolgten, sondern einzelne ausführbare Programme (EXE-Dateien) einfach auf den Rechner aufgespielt wurden.

#### Vorbeugung

Spezielle Antivirenprogramme, Geschützte Partitionen und Netzwerke für ausführbare Programme.

#### Erkennung

Manchmal an der geänderten Programmgröße oder geändertem Erstellungsdatum. Gut programmierte Viren berücksichtigen jedoch diese Effekte.

## MAKRO-VIREN und Skripts

Viren, welche von makrofähigen Programmen an entsprechende Dokumente angelagert werden.  
Beispiele sind:

.DOC (Worddateien), .XLS (Exceldateien), ...

### Vorbeugung

Deaktivieren der Makrofähigkeit (falls möglich). Installation spezieller Sicherheitspatches des Herstellers.  
Speziell für Outlook (Aktivieren der Sicherheitsnachfrage beim Öffnen).

## ActiveX

Verbreitung über Programme oder über Internetseiten. Netscape Browser (Version 4.0) lässt entsprechende ActiveX-Komponenten erst gar nicht zu.

### Vorbeugung

Deaktivieren der ActiveX, bzw. nur zertifizierte ActiveX-Komponenten oder höchster Sicherheitsstandard im Internetexplorer.

### Erkennung

Entsprechende Meldung des Internetexplorers bei angepasster Sicherheitsstufe lässt auf vorhandenen ActiveX-Komponenten schliessen.

## JAVA-Applets

Bessere Sicherheit als ActiveX. Es wurden jedoch immer wieder Sicherheitslücken bekannt..

### Vorbeugung

Deaktivieren von **Java**, bzw nur auf verlässliche Seiten surfen.

## Active Scripting, JavaScript, VBScript

Erlaubt die Ausführung interaktiver Skripte (Batchdateien) mit Zugriff auf alle (freigegebenen) Systemfunktionen. Zentraler Einstiegs- und Angriffspunkt für Viren vom Typ "**I Love you**".

### Vorbeugung

Deaktivieren von **Active Scripting im Internetexplorer**. Kein Öffnen von \*.**VBS**-Dateien (VBScripts) im eMail-Programm.

(Bei hohen Sicherheitsanforderungen auch die Ausführung von JavaScript einschränken bzw. deaktivieren.)

## Notiz am Rande

Betrachtet man sich die Möglichkeiten, welche die integrierten Skriptsprachen und Zugriffe auf Outlook bietet, dann kann man eigentlich nur froh sein, dass "I LOVE YOU" bzgl. der Verbreitung nicht noch einen Schritt weiter gegangen ist. Entsprechende Möglichkeiten werden wir an dieser Stelle jedoch nicht diskutieren, um entsprechende Personen nicht auf dumme Gedanken zu bringen.

## Zusammenfassung

Nachfolgend finden Sie verschiedene Empfehlungen.

- Sorgen Sie dafür dass Ihr Rechner von der Festplatte bootet und nicht zuerst über Diskette
- Nur lesbare Disketten mit Schreibschutz versehen
- Entkoppeln Sie (wenn möglich) den Kommunikationsrechner von den anderen Rechnern indem sie entsprechende Zugriffsrechte einstellen.
- Deaktivieren Sie "Active Scripting" im Internetexplorer
- Deaktivieren Sie (wenn Sie den Internetexplorer nutzen) die Ausführung von ActiveX-Komponenten bzw. aktivieren Sie die höchste Sicherheitsstufe.
- Deaktivieren Sie die Ausführung von Java (falls nicht unbedingt nötig)
- Öffnen Sie auf keinen Fall angehängte Dateien / Dokumente im eMail-Programm (insbesondere Outlook) mit folgenden Endungen

**\*.VBS, \*.DOC, \*.XLS, \*.EXE, \*.COM, \*.BAT**

***Prinzipiell betrifft dies jedes Dokument, welches beim Öffnen ein registriertes Programm aktiviert, das skript- oder macrofähig ist und seine Skripts/Macros in den Dokumenten selbst ablegt !!!***

Wenn Sie sich bzgl. Urheber und Inhalt des Dokumentes sicher sind, dann können Sie die Datei öffnen. Wenn Sie nicht sicher sind, dann sichern Sie sich ab, indem Sie sich mit dem Absender in Verbindung setzen. Desgleichen gilt für Dateien, welche Sie vom Internet herunter geladen haben.

- Installieren Sie Antivirenprogramme
- Besorgen Sie sich die entsprechenden Patch-Programme der relevanten Produkte (Word, Excel, Outlook, ...)
- Informieren Sie ihre Mitarbeiter

© 2000 Ingenieurbüro Graber, D-76316 Malsch, [www.graber.de](http://www.graber.de)