Malware

Daten- und Virenumgang

Vielen Leuten sind Computer-Viren bekannt und haben sogar ihren PC infiziert und Daten verloren. Der häufigste Grund für eine Infektion besteht darin, dass je mehr Leute an ihm arbeiten oder spielen und immer wieder neue Software einschleusen, desto grösser ist die Gefahr einen Virus einzufangen. Das Gefärdungspotential von Viren kann recht unterschiedlich sein: Es reicht von den eher unauffälligen Plattenplatzdieben, die sich einfach an jede ausgeführte Programmdatei anhängen, bis zu solchen Exemplaren, die Dateien verschwinden lassen oder gar die Hardware beschädigen und damit grossen wirtschaftlichen Schaden anrichten können.

Woran merkt man, dass man sich einen Virus gefangen hat? Leider bleiben Viren häufig lange Zeit unbemerkt, was dazu führen kann, dass immer mehr Programme auf der Festplatte oder auf Disketten infiziert werden. Die Konsequenz daraus sollte sein, auch bei unauffälligem Verhalten Ihres PCs regelmässig ein Virenprüfprogramm einzusetzen. Wenn Ihr Anwendungsprogramm sich jedoch ungewöhnlich verhält, unerklärliche Datenverluste eintreten oder Ihr Bildschirm plötzlich ein verändertes Aussehen zeigt, sollte bei Ihnen die Alarmglocke läuten!

Viren werden meist über Disketten oft unbekannter Herkunft, aber auch von externen Softwareservern übertragen. Administratoren solcher Server übernehmen meist keine Garantie für Virenfreiheit ihrer Produkte.

Oberstes Gebot bei der Übernahme von Programmen und Daten von anderen Personen, auch vertrauenswürdigen, sollte es sein, vor Benutzung solcher Daten einen Test auf Virenfreiheit mittels eines Virenscanners durchzuführen. Aber auch das ist ein trügerischer Schutz vor einer Infektion, denn ein Virenscanner wird immer als Reaktion auf bereits vorhandene Viren entwickelt bzw. weiterentwickelt, d. h. erst wenn man einen Virus entdeckt hat, kann man Identifizierungs- und Schutzmechanismen gegen ihn entwickeln. Da auf der Welt täglich mehrere neue Computerviren produziert werden und Updates von Virenscannern in der Regel mehrere Monate hinterherhinken, ist der PC-Anwender Hunderten von neuen Viren schutzlos ausgeliefert.

Der beste Schutz gegen Viren ist daher eine Reihe von **Verhaltensregeln**, die ich Ihnen zur Beachtung empfehlen möchte:

- Verwenden Sie nur Programme von Personen, die Ihnen vertrauenswürdig sind!
- Verwenden Sie nur Originalsoftware, lehnen Sie die Benutzung von illegalen Kopien ab!
- Verleihen Sie keine Disketten, machen Sie besser Kopien der Daten und Verzichten Sie auf eine Rückgabe
- Sollten Sie dennoch Disketten verliehen haben, prüfen Sie diese nach Rückgabe unbedingt auf Virenbefall mit einem Virenscanner!
- Wenn es sich nicht verhindern lässt, dass auch andere Leute mit Ihrem PC arbeiten, setzen Sie häufig Virenscanner ein, und zwar möglichst die aktuellsten Versionen!
- Achten Sie darauf, dass Sie niemals eine nicht mehr benötigte Diskette in Drive A: lassen! Bei einem Neubooten Ihres Rechners wird meist zuerst von Drive A: zu booten versucht, so dass von einer Diskette, auf der sich sonst nur Daten befinden mögen, deren Boot-Sektor aber infiziert ist, automatisch der Virus in Ihr System eingeschleust wird.
- Nach dem Herunterladen von Software von externen Servern über das Netz sollten Sie die erhaltene Datei auf Viren untersuchen!
- Machen Sie regelmässig Backups von Ihren wertvollen Daten!
- Was ist zu tun, wenn Sie einen Virus identifiziert haben oder auch nur den Verdacht haben, dass Ihr PC von einem Virus befallen ist? Lassen Sie auf keinen Fall weitere Programme laufen, sondern beginnen Sie sofort mit der Virensuche! Ein Virenscanner sollte am besten von einer virenfreien, schreibgeschützten, bootfähigen Diskette gestartet werden, denn auch ein Virenscanner auf Festplatte kann selbst von einem Virus befallen sein.

Virenarten

Dateiviren

- Infektion: Dateiviren hängen sich an .COM und an .EXE Dateien an oder ersetzten diese teilweise. Diese Virenart infiziert Programme in der Regel, wenn sie ausgeführt werden, während sich der Virus im Arbeitsspeicher befindet. In anderen Fällen werden Dateien infiziert, wenn sie geöffnet werden.
- Auswirkungen: Dateiviren löschen Dateien oder machen sie mindestens unbrauchbar.
- Vorschlag: Scannen sie heruntergeladene Dateien mit einem Antivirenprogramm, bevor sie öffnen oder ausführen.

Bootsektorviren

- Infektion: Das Virus kommt über eine infizierte Diskette oder andere externe Flashlaufwerke (USB-Sticks) in den PC. Jede Festplatte hat einen Bootsektor. Beim Starten der Diskette oder des externen Flashlaufwerks (USB-Stick) wird das Startprogramm des Bootsektors infiziert.
- Auswirkungen: Viele Varianten, da es verschiedene Viren dieser Art gibt.
- Vorschlag: Auch hier sollten sie diese externen Festplatten mit einem Antivirenprogramm scannen.

MBR (Master Boot Record) Viren

- Infektion: Ein MBR-Virus wird auf dieselbe Weise übertragen wie ein Bootsektorvirus (durch Starten des Computers mit einer infizierten Diskette im Laufwerk.) Wenn das Startprogramm gelesen und ausgeführt wird, gelangt der Virus in den Arbeitsspeicher und infiziert den MBR der Festplatte.
- Auswirkungen: Viele Varianten, da es verschiedene Viren dieser Art gibt.
- Vorschlag: Auch hier sollten sie diese externen Festplatten mit einem Antivirenprogramm scannen.

Mehrteilige Viren

- Infektion: Mehrteilige Viren sind eine Kombination aus den bisher vorgestellten Virenarten. Sie infizieren sowohl Dateien als auch Bootsektoren bzw. MBRs. Diese Virenart ist noch ziemlich selten, aber die Anzahl der Vorkommnisse wächst ständig.
- Auswirkungen: Alles möglich, denn es ist abhängig vom Virus den man abgefangen hat.
- Vorschlag: Auch hier sollten sie diese externen Festplatten mit einem Antivirenprogramm scannen.

„Hoax“-Viren

- Infektion: E-Mail
- Auswirkungen: ein Scheinvirus, es verunsichert den Benutzer oder fordert den Benutzer auf das Virus weiter zu versenden
- Vorschlag: Falls sie ein E-Mail erhalten indem steht sie sollen es weiterverschicken, machen sie das auf keinem Fall. Sie löschen die Mail lieber.

Makroviren

- Infektion: Makroviren infizieren keine Programme, sondern Dateien von Textverarbeitungen, Tabellenkalkulationen und Datenbanken. Ein Makrovirus ist in einer Dokumentvorlage gespeichert. Indem sie die Datei öffnen aktivieren sie Ihn.
- Auswirkungen: Ab diesem Zeitpunkt wird jedes Dokument, das Sie neu erstellen und speichern automatisch mit dem Makrovirus infiziert. Öffnet nun ein anderer Benutzer ein infiziertes Dokument, wird das Makro auch auf dessen Computer übertragen. Makroviren können Schäden in gleichem Umfange anrichten wie Computerviren schlechthin.
- Vorschlag: Scannen sie die Dateien die sie öffnen. Es gibt mit Microsoft Word 03 folgende Einstellungen gegen Makroviren: Klicken Sie im Menü Extras auf Optionen. Klicken Sie danach auf die Registerkarte Allgemein, und aktivieren Sie dann das Kontrollkästchen Makrovirus-Schutz.

HTML- Viren

- Infektion: Diese Viren sind auf Hacker-Websites deponiert und wurden erstellt um Löcher im Sicherheitssystem des MS Internet-Explorers offenzulegen. Indem sie auf solche Seiten gelangen, werden sie, falls ihr Firewall diese Seiten nicht sperrt, infiziert.
- Auswirkungen: Überschreibt oder ersetzt teils ganze Internetseiten.
- Vorschlag: setzen sie ihre Sicherheitsstufe ihres Internet Explorers auf „sehr hoch“. Oder vermeiden sie solche Internet-Seiten.

Trojanische Pferde

- Infektion: Infiziert den Computer beim Ausführen von Programmen aus dem Internet, die als harmlose Spiele oder Hilfetools getarnt sind.
- Auswirkungen: Sie vermehren sich nicht, löschen aber Dateien, geben Daten im Netzwerk frei, löschen Verzeichnisstrukturen usw. dies variiert je nach Virus dieser Art.
- Vorschlag: Vermeiden Sie Downloads von unbekannten Herausgebern. Scannen sie das Programm lieber, bevor sie es ausführen.

Würmer (Worms)

- Infektion: Ein Wurm kann überall angehängt werden. Beim Öffnen einer Datei, bei der ein Wurm angehängt wurde, infiziert sich Ihr Computer.
- Auswirkungen: Der Wurm vermehrt sich rasant und legt so das Netzwerk und den PC lahm. Es führt zum Zusammenbruch eines ganzen Netzwerks.