

Vorbeugen ist besser als den Schaden später zu beheben

Bei der Zusammenstellung dieser Hinweise und Tipps kann man nicht jeden Einzelfall und jede PC-Konfiguration berücksichtigen. Sie sind auch nicht für "Profis" gedacht, sondern für PC-Nutzer, die beginnen, sich mit dieser Materie auseinander zu setzen.

Eines noch vorab: Es gibt keine hundertprozentige Sicherheit - im Leben nicht und natürlich auch nicht im Internet oder beim Umgang mit Computern generell (das ist ebenso banal, wie es wahr ist).

Kein Virens Scanner erhebt ernsthaft den Anspruch, vor jeder Gefahr zu schützen, keine Firewall kann wirklich jeden Angriff abwehren und kein noch so ausgeklügeltes Sicherheitskonzept macht Ihren Computer zu einer für immer uneinnehmbaren Festung. So bitten wir um Verständnis, dass auch wir natürlich keine Garantie oder Haftung übernehmen können, dass die hier vorgestellten Ratschläge in jedem einzelnen Fall auch die erhoffte Wirkung zeigen. Der Faktor Mensch stellt dabei immer noch die sicherheitsbedenklichste Komponente dar.

Tipp 1:

Installieren Sie auf jedem PC einen Virens Scanner. Viele Hersteller kommerzieller Anti-Viren-Scanner bieten "Testversionen" ihrer Programme an, die jedoch nur zeitlich begrenzt einsetzbar sind. Sie scheiden natürlich als Dauerlösung aus. Wenn Sie den Einsatz eines "Freeware"-Scanners erwägen, sollten Sie bedenken, dass diese bei "exotischeren" Viren, Scannen verschachtelter Archive und gepackter Dateien, Update-Häufigkeit, Support, Handbüchern usw. - gemessen an den kommerziellen Produkten - oft nur die zweitbeste Lösung sind. Suchen Sie den für Ihre Bedürfnisse **richtigen Virens Scanner**, denn: Den perfekten Scanner gibt es nicht. Sie kommen also um einen Blick in entsprechende Testberichte nicht herum. Diese Zeit sollten Sie sich nehmen. Achten Sie auf die Erkennungsraten auch bei "Trojanern" und "Würmern" (besonders in gepackten Dateien), auf eine geringe Systembelastung, eine möglichst hohe Update-Frequenz und die Qualität der sog. "Heuristik", die hilft, auch bisher nicht bekannte Viren zu entdecken (die aber auch Fehlalarme produzieren kann).

Tipp 2: Führen Sie regelmäßig Updates der Antivirensoftware durch. Jeden Monat tauchen bis zu 300 neue und immer raffinierter getarnte Viren auf. Die Anbieter von Anti-Viren-Software reagieren auf neue Schädlinge umgehend mit aktualisierten Versionen ihrer Scan-Dateien. Ein "Uralt-Scanner" hat kaum Chancen, diese neuen Viren zu entdecken und zu entfernen. Die sog. **Wächter-, Monitor- oder Guard-Funktion** Ihres Virens Scanners sollte stets aktiviert sein. Es handelt sich dabei um einen Virens can im Hintergrund des laufenden Systems, z.B. beim Öffnen einer Datei. Wenn Sie mehrere Anti-Viren-Programme installieren, sollten Sie unbedingt sicherstellen, dass stets nur ein "Hintergrundwächter" seinen Dienst tut. Sind mehrere Scanner gleichzeitig aktiv, können sie sich gegenseitig blockieren oder gar das System zum Absturz bringen!

Tipp 3: Scannen Sie Ihre Festplatte(n) in regelmäßigen Abständen. Die meisten Virens Scanner bieten die Möglichkeit, Scans in bestimmten Zeitintervallen automatisch zu starten. Möchten Sie das nicht, sollten Sie den Scan mindestens einmal pro Woche von Hand starten.

Konfigurieren Sie den Virenschanner aber so, dass er nicht nur bestimmte, sondern - auch wenn es etwas länger dauert - **ALLE** Dateien Ihrer Festplatte prüft. Der Scanner sollte darüber hinaus für jeden Prüflauf ein Protokoll erstellen.

Stellen Sie Ihren Scanner so ein, dass er einen Virus nicht selbständig löscht, sondern immer nachfragt, was zu tun ist.

Zurzeit verbreiten sich mehr als 90% aller Viren über eMail. Deshalb sind die folgenden Hinweise besonders wichtig:

Tipp 4: Konfigurieren Sie Ihr Mailprogramm so, dass Dateianhänge nicht automatisch geöffnet oder ausgeführt und alle eingehenden Mails nicht als HTML-, sondern als reine Text-Mails geladen werden. Durch das Lesen einer Text-Mail kann Ihr System nicht infiziert werden - die Gefahr lauert in den (ausführbaren) Dateianhängen bzw. im HTML-Code. Deaktivieren Sie also die automatische Vorschau-funktion, da diese einigen Schadprogrammen den selbständigen Start ermöglicht.

Tipp 5: Machen Sie es sich zur Gewohnheit, **JEDEN** Dateianhang einer eMail ungeöffnet in einem separaten Verzeichnis zu speichern, und ihn zuerst mit Ihrem Virenschanner zu prüfen. Auch eine eMail mit einer vertrauenswürdigen Absenderadresse kann ein Schadprogramm enthalten! Es ist nämlich möglich, dass sich der Absender einen Virus "eingefangen" hat, ohne es bisher bemerkt zu haben, oder es ist ein sog. "Wurm" aktiv, der von sich aus verseuchte Mails versendet. Es gibt sogar die Möglichkeit, Absenderadressen zu fälschen.

Wichtig: Software-Firmen oder Anbieter von Internet-Diensten verschicken grundsätzlich keine Updates o.ä. per eMail !!!

Sprechen Sie - soweit möglich - den Austausch von Dateien per eMail vorher ab und laden Sie Mails von unbekanntem Absendern und/oder deren Betreff in einer Fremdsprache abgefasst ist, erst gar nicht vom Mailserver herunter. Meiden Sie Mailprogramme, die sich nicht entsprechend konfigurieren lassen.

Übrigens: Als eMail Programm muss es nicht immer das mit "Windows" gelieferte "Outlook Express" sein.

Unterbinden Sie in Ihrem Browser die Ausführung von Java und JavaScript oder erlauben Sie die Nutzung dieser Funktionen nur ausgewählten Webseiten. Gänzlich deaktivieren sollten Sie das besonders kritische ActiveX (von seriösen Webseitenbetreibern wird es ohnehin immer seltener eingesetzt - die einzige Situation, in der Sie es tatsächlich brauchen, ist das "Windows-Update"). Tipp: Es gibt Browser, die von Haus aus nicht mit ActiveX arbeiten und die sich auch nicht von den ebenfalls kritischen "Visual Basic Scripten" beeindrucken lassen. Zusatzprogramme wie z.B. "Proxomitron" oder "WebWasher" können einige der möglicherweise schädlichen aktiven Inhalte blockieren. Diese Programme wurden ursprünglich als Werblocker entwickelt, können mittlerweile aber viel mehr (besonders das "Proxomitron").

Setzen Sie immer die neueste Version Ihres Browsers und Ihres Email-Programms ein und installieren Sie umgehend alle sicherheitsrelevanten Updates. Konfigurieren Sie die Sicherheitseinstellungen dieser Programme sorgfältig und überprüfen Sie diese Einstellungen von Zeit zu Zeit.

Prüfen Sie generell **ALLE** aus dem Internet heruntergeladenen Programme und Dateien gleich nach dem Download mit Ihrem Virens Scanner - das geht meist über das Kontextmenü (Rechtsklick auf die Datei) und dauert nur wenige Sekunden! Es versteht sich von selbst, dass Sie fremde externe Datenträger (nicht nur die entsprechenden Dateien, sondern den ganzen Datenträger) auf Viren prüfen sollten, bevor Sie Programme oder Dateien von ihnen auf Ihre Festplatte kopieren.

Ein guter Schutz vor Bootsektorviren ist es, die Bootreihenfolge im BIOS so einzustellen, dass beim Start des Systems immer vom Betriebssystem-Laufwerk (i.d.R. Laufwerk "C:\") gebootet wird und nicht von einem auswechselbaren Datenträger (z.B. einer Diskette) mit noch ungeprüfem Bootsektor.

Erstellen Sie mindestens zwei Bootdisketten (oder eine bootfähige CD-ROM) und stellen Sie sicher, dass diese virenfrei sind. Bei einem Virenbefall oder einer anderen Fehlfunktion haben Sie mitunter nur mit Hilfe einer solchen Diskette oder CD-ROM noch Zugriff auf Ihr System! Die meisten Virens Scanner bieten die Möglichkeit, spezielle Startdisketten für den Notfall zu erstellen. Davon sollten Sie Gebrauch machen, denn beim Versuch einen Virus zu entfernen, wird der Virens Scanner möglicherweise diese Disketten benötigen. Vergessen Sie nicht, auch diese Notfalldisketten regelmäßig zu aktualisieren. Öffnen Sie danach den Schieberegler an den Disketten, so dass nicht mehr auf sie geschrieben werden kann.

Nutzen Sie **weitere Programme** wie z.B. "TrojanCheck", Ad aware, Spyware , Hijack This oder "WinPatrol". Diese Programme prüfen permanent Windows-Bereiche wie den Autostartordner auf Veränderungen und können diese Veränderungen bei Bedarf wieder rückgängig machen. Solche Änderungen können durch normale Installationen oder Updates entstehen, aber eben auch durch Schadprogramme. Verlassen Sie sich dagegen nicht auf Instrumente wie die "Systemwiederherstellung" oder den "Systemdateischutz" der neueren "Windows"-Betriebssysteme. So hilfreich die in bestimmten Situationen auch sind, zur Abwehr von Viren sind sie nicht geeignet!

Deinstallieren Sie den "Windows Scripting Host" (es sei denn, Sie sind sicher, dass Sie ihn unbedingt brauchen). Der WSH ermöglicht die Ausführung der sog. "VB-Scripte", mit deren Hilfe u.a. Arbeitsabläufe automatisiert werden können - eine ideale "Spielwiese" für Virenprogrammierer. Alternativ können Sie auch ein Programm (z.B. "ScriptDefender" oder "NoScript") nutzen, das die Ausführung von Scripten erst auf Nachfrage gestattet

Einige Schadprogramme wurden explizit geschrieben, geheime Passwörter oder andere Zugangsdaten zu stehlen (bekanntermaßen auch ein beliebter Sport unter Kollegen). Auch wenn es mühsam ist und es niemand gerne tut: Ändern Sie von Zeit zu Zeit Ihre Passwörter.

Es gibt keine Datenquelle, die vor Viren sicher ist. Viren waren schon in Original- oder vorinstallierter Software enthalten, wurden von Wartungstechnikern unbeabsichtigt eingespielt oder über Heft-CDs oder Home-Pages namhafter Firmen (natürlich ebenfalls unbeabsichtigt) verbreitet. Das beim Verwenden von Raubkopien oder dem Download von Dateien aus dubiosen Quellen allerbeste Chancen bestehen, sich einen Virus oder ein anderes Schadprogramm einzufangen, muss ohnehin jedem klar sein. So wurden z.B. zeitweilig mit einem Schadprogramm verseuchte Versionen des beliebten PC-Spiels "Moorhuhn" in Umlauf gebracht. Eine weitere unsichere Quelle ist das File-Sharing der (Musik-)Tauschbörsen.

Speziell zu beachten bei "Trojanischen Pferden"

Methode "Überprüfung der Ports mittels Netstat"

Da die meisten Trojaner im Hintergrund auf eine Internetverbindung des Rechners "warten", belegen diese einen Port. Die Ports kann man mittels des Programmes "netstat" überprüfen. Das Programm befindet sich von Haus aus auf jedem Windows-System.

Rufen Sie die MS-DOS-Eingabeaufforderung auf und geben Sie bitte folgenden Befehl ein:
netstat -a

Diese Prüfung mittels Netstat sollte auf jedenfall nur im Offlinemodus durchgeführt werden, d.h. es darf keine Verbindung ins Internet bestehen.

Hier ein Beispiel, welche Meldung Netstat ausgeben könnte:

Active Connections

```
Proto Local Address Foreign Address State
```

```
TCP _:27374 0.0.0.0:45178 LISTENING
```

```
UDP _:27374 *.*
```

Wie man hier sehen kann, wird der Port 27374 "belegt". Anhand der Portliste (<http://www.trojaner-info.de/port.shtml>) könnte man daraus schließen, dass ein System mit dem SubSeven Trojaner neuerer Version infiziert ist.

Zumindest ist es ein recht sicheres Anzeichen dafür. Jedoch möchte ich noch erwähnen, dass man anhand des belegten Ports und der Portliste nie zu 100 % bestimmen kann, um welchen Trojaner es sich genau handelt. Sehr viele Trojaner bieten die Möglichkeit einen Port selber festzulegen.

Die Überprüfung mittels einer einzigen hier genannten Methode ist nicht unbedingt empfehlenswert. Geht der Anwender jedoch alle hier genannten Methoden nacheinander durch, wird man dem Trojaner sicherlich auf die Schliche kommen können.

Weniger erfahrene Anwender sollten in jedem Fall einen Fachmann zu Rate ziehen, bevor in Panik irgendwelche Dinge entfernt werden. Falsche Handhabungen können unter Umständen das gesamte Betriebssystem des Computers außer Gefecht setzen !