

Machen Sie Ihren Computer sicherer!

Eine kurze Anleitung um Ihren Computer vor den alltäglichen Gefahren des Internets zu schützen.

Ich möchte Ihnen aufzeigen, wo Sie die Sicherheit Ihrer EDV verbessern können und was Sie tun können, wenn dann doch etwas passiert ist und Sie sich einen Schädling eingefangen haben und wo Sie weitere Hilfe und Informationen finden können.

Merksatz: Es gibt keine 100%ige Sicherheit!

Aber hier bekommen sie Hilfe, wenn Sie sich

- [schon einen Schädling eingefangen haben](#) oder
- [präventiv etwas für Ihre Sicherheit tun möchten](#).

1. Fall: Wenn es dann doch mal passiert ist.

Das kann manchmal recht einfach passieren, zuweilen - besonders bei den modernern Würmern - aber auch in eine ziemlich anstrengende Arbeit ausarten.

WARNUNG: Die folgende Anleitung ist eher für fortgeschrittenere Benutzer gedacht!

Sie haben versehentlich doch mal in einem aufgehenden Dialogfenster auf „Ja“ geklickt oder etwas herunter geladen und ausgeführt, das nicht sauber war. Als Symptom reagiert der Rechner sehr langsam, oder macht seltsame Dinge, die Sie so nicht gewohnt sind.

Dann heißt es zunächst: Ruhe bewahren!

Trennen Sie den Computer möglichst von Internet, damit Sie nicht als Überträger fungieren.

Im Grunde läuft eine Desinfektion immer gleich ab: im abgesicherten Modus starten und Systemwiederherstellung abschalten, eventuell ein Removal-Tool anwenden, Virensan mit aktuellem Scanner durchführen, fertig.

1. Zunächst gilt es herauszufinden, welcher der vielen verbreiteten Schädlinge sich auf ihrem Computer breit gemacht hat.

Der aktuell am weitesten verbreitete Virus ist meist eine gute Wette, aber wir müssen es genau wissen.

Dazu finden Sie unter <http://vil.nai.com/vil/stinger/> ein kleines kostenloses Programm (Stinger), welches Sie auf ihren Rechner herunterladen und ausführen müssen.

Dieses Programm zeigt Ihnen mögliche Infektionen mit den gängigsten Viren an.

Stinger kann auch eine Desinfektion vornehmen, diese verläuft aber nicht immer erfolgreich, wie Tests gezeigt haben.

2. Wenn Sie den Namen des Schädlinge eruiert haben, können Sie auf

<http://www.symantec.de/avcenter/tools.list.html> nach dem Namen suchen und kommen auf eine Seite, auf der sie sowohl detaillierte Informationen über den Virus als auch leicht verständliche hinweise zu seiner Entfernung finden. Symantec stellt in der Regel auch ein kostenloses Programm zur Entfernung der Viren zur Verfügung, welches im Gegensatz zum Stinger auch immer funktioniert, da es speziell auf den Schädling zugeschnitten wurde.

BITTE BEACHTEN SIE, das für eine erfolgreiche Desinfektion immer im abgesicherten Modus gestartet werden muss und die Systemwiederherstellung ausgeschaltet sein muss!

3. Nach einem Neustart von Windows ist der Desinfektionsprozess hier auch meist schon abgeschlossen.

WICHTIG: Viele der aktuellen Viren und Würmer können einen PC nur befallen wenn nicht regelmäßig die Windowsupdates eingespielt werden! Lesen Sie bitte auch die Hinweise [unten](#)

2. Fall: Sie möchten Ihren PC sicherer machen, damit Viren und Würmer erst gar keine Chance bekommen.

1. Benutzen Sie Ihren Verstand

Ihr gesunder Menschenverstand ist Ihre wichtigste Waffe.

Bewegen Sie sich auf Ihnen unbekanntem Seite nur mit äußerster Vorsicht, klicken Sie auf keinen Fall auf auftauchende Meldungen, die Sie zu einer Installation auffordern. Laden Sie nur Software herunter, wenn Sie einen aktuellen Virenschanner betreiben (siehe unten).

Öffnen Sie keine Emailanhänge, die Sie nicht angefordert haben, ohne sich beim Sender rück zu versichern. Löschen Sie Emails mit Anhängen von Personen, die Sie nicht kennen ungelesen, wenn es wichtig war bekommen Sie sie eh noch einmal.

Niemand, der es gut mit Ihnen meint wird Sie je per Email auffordern ihm Ihre Passwörter oder PINs mitzuteilen. Also tun Sie es auch nicht!

2. Regelmäßiges Windowsupdate

Aktivieren Sie die automatischen Updates von Windows.

Diese prüfen immer wenn Sie sich im Internet bewegen im Hintergrund auf Aktualisierungen und benachrichtigen Sie.

Dazu gehen Sie in das Startmenü, klicken dort auf Systemsteuerung und anschließend auf das Sicherheitscenter. Ganz unten haben Sie den Punkt „Automatische Updates“. Ich würde empfehlen, die Einstellung auf den dritten Punkt „Benachrichtigen, aber nicht automatisch downloaden oder installieren“ zu setzen, So behalten Sie die Kontrolle, wann Sie Ihren Rechner aktualisieren möchten.

Verfügen Sie nicht über Windows XP mit SP2 oder nur über eine Modem/ISDN-Verbindung, dann besuchen sie regelmäßig am zweiten Dienstag jedes Monats die Windowsupdate-Seite von Microsoft. Sie finden diese unter <http://windowsupdate.microsoft.com>. Keine Angst vor diesem Schritt, Sie werden durch die Seite geführt und können nichts falsch machen.

DAS WINDOWSUPDATE IST UNABDINGBAR. OHNE UPDATES KÖNNEN AUCH VIRENSCHANNER NICHT HELFEN!

Wenn sie nicht über einen schnellen Internetzugang verfügen, versendet Microsoft auf Anfrage auch CDs mit den Updates. Sie können mich in diesem Falle auch ansprechen, dann besorge ich diese.

3. Verwenden Sie einen Virenschanner und halten Sie ihn aktuell

Wer kein Geld für einen Virenschanner ausgeben möchte findet unter <http://www.free-av.de> eine kostenlose Alternative. Die Leistung liegt nicht im Topfeld der verschiedenen Anbieter, aber im sehr soliden Mittelfeld. Ich

selbst verwende das Programm auf meinem Privatrechner und bin sehr zufrieden.

Wenn Sie die Ausgaben nicht scheuen können Sie in den nächsten Fachmarkt gehen und dort ein Produkt der großen Anbieter kaufen. als da wären u.a.:

Symantec	http://www.symantec.de
GData	http://www.gdata.de
McAfee	http://www.mcafee.de
Sophos	http://www.sophos.de
Trend Micro	http://www.trendmicro.de

Wichtig ist nur, dass Sie den Virenschanner durch die eingebauten Updatefunktionen stets aktuell halten. Dadurch werden die Fingerabdrücke, der neuesten Schädlinge auf ihren Rechner geladen. Anhand dieser Fingerabdrücke erkennen die Antivirenprogramme die Schädlinge.

In der Regel sollte das update mindesten alle 14 tage erfolgen, besser jede Woche oder immer, wenn Sie sowieso schon online sind. Die meisten Virenschanner erledigen das auf Wunsch auch automatisch.

4a. Verwenden Sie einen alternativen Browser

Der Internet Explorer, der mit Windows mitgeliefert wird ist nicht nur immer wieder von gravierenden Sicherheitslücken betroffen, sondern lässt auch einiges an Funktionalität vermissen.

Meine Empfehlung: Ich verwende seit Jahren den von der Mozilla-Foundation entwickelten Browser [Firefox](#). Er ist ziemlich sicher (es programmieren tausende von Menschen an dem Programm, daher werden Probleme schon in einer sehr frühen Phase entdeckt und ausgemerzt), unterstützt kein ActiveX (eine Microsoft Technologie, die interessante Technologien ermöglicht, aber sehr schnell missbraucht werden kann, um Dialer und Trojaner auf Ihrem Rechner zu installieren) und bietet darüber hinaus noch zusätzliche komfortable Funktionen. Dazu gehören da TabbedBrowsing, bei dem mehrere Seiten in einem Fenster dargestellt werden, hat einen RSS-Reader integriert und lässt sich über sogenannte Extensions leicht mit weiteren Funktionen aufrüsten.

Leider funktioniert die [Microsoft Update Seite](#) mit Firefox nicht, da er wie schon erwähnt kein ActiveX beherrscht.

4b. (streng optional) Verwenden Sie eine Personal-Firewall

Ich persönliche halte nicht viel von Desktop-Firewalls (s. hierzu auch meine [Kurzschritt gegen Personal Firewalls](#)).

Sie benötigen zur Konfiguration eines solchen Programms fundiertes Wissen über die Protokolle des Internets und falsch eingestellt sind Firewalls eher eine Bedrohung als ein Schutz!
Zudem bremsen Sie den Rechner und den Internetzugang unnötig aus. Wenn es jedoch unbedingt sein muss, verwenden Sie am Besten ZoneAlarm.

Dieses leicht zu bedienende kostenlose Programm finden sie unter <http://download.zonelabs.com/bin/free/de/download/znalm.html>
ZoneAlarm konfiguriert sich bei Gebrauch von ganz alleine, es sind nur minimale Arbeiten vom Benutzer notwendig. Eine deutschsprachige Anleitung finden sie unter <http://www.trojaner-info.de/cgi-bin/download.cgi?file=zoneanleitung>.
Die in Windows XP SP2 eingebaute Firewall macht Sie nur im Internet einigermaßen „unsichtbar“, bietet somit nur rudimentäre Schutzwirkung.

Wie immer gilt zum Abschluß:
Bei Fragen stehe ich Ihnen gerne zur Verfügung!

<http://www.agilmer.de/>