- Niemals würde das Kriminalamt, oder sonst irgendeine staatliche oder sonstige seriöse Firma eine Privatperson von sich aus **per Email** anschreiben!
- Auch Emailanhänge von Freunden können unter Umständen Schädlinge enthalten: Wenn dieser z.B. von einem Wurm befallen wird, schickt der Wurm ganz automatisch und ohne Wissen des Nutzers, an alle Adressbucheinträge eine Kopie von sich selbst. Wenn von einem Freund also eine merkwürdige Email kommt mit einem merkwürdigen Dateianhang oder einem merkwürdigen Link, sollte sicherheitshalber erst nachgefragt werden!

- Gegen SPAM-Emails kann man leider nichts tun, außer sich eine neue Emailadresse anzulegen und die SPAM-Emails immer direkt ungelesen zu löschen! Weitere Tipps zum Umgang mit SPAM Emails:
  Http://www.vorwahl-nummern.de/fundgr...pam_emails.php
  Http://www.securityinfo.ch/email.html
  Http://www.microsoft.com/germany/ath.../phishing.mspx

Umgang bei der Verwendung von Internet-Tauschbörsen und Chat-Programmen:
Solche Programme sind meistens leider sehr sehr unsicher: Bei Tauschbörsen sind nahezu **die Hälfte aller Dateien** die zum Download angeboten werden mit Viren, Trojanern oder ähnlichen infiziert, und in Chat-Programmen werden die Benutzer regelmässig mit Links auf Interneseiten gelockt die Schädlinge enthalten! Unter den Punkt 4b der Anleitung, findet Ihr ausführlichere Informationen zu diesem Thema, sowie mögliche Alternativen!

Die drei allergefährlichsten Zonen - wo sich am meisten User von einem Wurm, Trojaner, Virus oder Spyware infizieren sind folgende:
1) In SPAM-Emails
2) Beim Besuch oder Download von unseriösen Internetseiten
3) Bei der Benutzung von unsicheren Programmen (Wie z.B. Tauschbörsen und Chatprogrammen)

Einblenden der Datei-Endungen:
Standardmäßig blendet Windows die ihm bekannten Dateiendungen aus - dadurch sieht man dann nicht den Unterschied ob eine Datei, die wie eine Word-Datei aussieht, nun wirklich eine Word-Datei ist (Beispiel.doc) oder doch ein getarnter Schädling ist. (Beispiel.doc.exe)
Auf diese Weise kann man sich die Dateiendung von allen Dateien anzeigen lassen:
Http://www.philognosie.net/index.php/tip/tipview/678/

Folgende Datei-Typen mit diesen Dateiendungen werden am meisten für Schädlinge benutzt:
.exe .com .pif .bat und .scr
Diese Datei-Typen führen nämlich beim Starten eine selbstständige Aktion durch, bei allen anderen Typen hingegen ist es unwahrscheinlich dass ein Schädling darin enthalten ist, da diese nur mit anderen Programmen geöffnet werden können!

Hoaxes:
Und immer öfter gibt es auch Falschmeldungen (so genannte Hoaxes) die versuchen den Nutzer zu verunsichern – wieder mit dem Ziel einen Virus, Trojaner oder ähnliches auszuführen. Auf dieser Internet-Seite wird darüber ausführlich aufgeklärt:
Http://www.tu-berlin.de/www/software/hoax.shtml

Internetnutzung an öffentlichen PCs:
Wenn in z.B. Internet Cafes ins Internet gegangen wird, kann man nie wirkliche Gewissheit haben, wie gut diese PCs geschützt sind! Manche Anbieter sind sehr sicher, da nach jedem Benutzer der ganze PC automatisch wieder in den Ursprungszustand zurückversetzt wird, aber bei vielen sind die Sicherheitsvorkehrungen auch mangelhaft! Und gerade an öffentlichen PCs ist es für Betrüger besonders interessant z.B. Passwörter der vielen verschiedenen Benutzer zu stehlen! Daher sollten folgende Dinge beachtet werden, um dass Risiko so weit es geht zu minimieren:

- Nach jeder Benutzung sollten die temporären Internetdateien gelöscht werden, die Cookies, sowie der Verlauf
- Die Passwörter sollten oft geändert werden, und niemals sollten Passwörter auf fremden PCs abspeichern werden
- Wenn es vom Anbieter erlaubt ist, ist es empfehlenswert ein Programm zu benutzen, welches verhindert das Tastatureingaben protokolliert werden können, um so Passwörter abzulauschen! Das Programm „Anti-Keylogger“ ist nur 40 kb klein, muss nicht installiert werden, und ist dafür gut geeignet:
  Http://myplanetsoft.com/free/antikeylog.php

1. Neueste Sicherheitsupdates von Windows installieren:

[[Hiermit werden Fehler am Auto behoben wie z.B. das beim Treten gegen den Hinterreifen automatisch der Kofferraum aufspringt]]
[[Auch für unerfahrene PC-Nutzer geeignet]]

Dieser Punkt ist der zweitwichtigste für die PC Sicherheit im Internet (und im Netzwerk) und sollte unbedingt regelmäßig durchgeführt werden! Es gibt inzwischen über 100 (!) Updates für Windows XP! Microsoft stellt in der Regel monatlich (jeden zweiten Dienstag) neue Updates gegen die aktuellen Sicherheitslücken zur Verfügung.
Oft werden die Virenprogrammierer gerade durch die neuen Sicherheitsupdates auf Schwachstellen aufmerksam gemacht und richten Ihre Schädlinge genau auf diese aus. Der Wurm Sasser z.B. ist ein klassisches Beispiel für genau diese Situation. Wenn alle Nutzer rechtzeitig ihr Windows geupdatet hätten, hätte dieser Wurm nie Schaden anrichten können!
Die Sicherheitsupdates können übrigens auch jederzeit nachträglich installiert werden, ohne dass der Nutzer befürchten muss dass irgendwelche Treiber gelöscht oder sonstige Einstellungen überschrieben werden!

Es gibt die nun folgenden vier Möglichkeiten, um die Windowsupdates zu installieren:

1. **Es kann die automatische Update-Funktion von Windows aktiviert werden. Dieses ist die einfachste Möglichkeit, denn hierbei braucht sich der Benutzer um nichts zu kümmern:**
   Http://support.microsoft.com/kb/306525/de

2. **Ihr könnt (monatlich) die folgende Internetseite besuchen, wo von dort aus die Updates automatisch installiert werden:**
   Http://windowsupdate.microsoft.com/

3. **Oder Ihr könnt (monatlich) folgenden Patch-Loader verwenden, (Windows 2000 und XP) welcher das System nach fehlenden Sicherheitsupdates scannt und diese dann installiert! Es werden hierbei NUR die reinen Sicherheitsupdates installiert keine anderen Windows-Updates:**
   Http://www.pcwelt.de/downloads/pcwel.../tools/128031/

4. **Oder Ihr könnt aber auch komplett fertige Updatepacks (Windows 98-Me und XP+Vista) downloaden! Bei den Updatepacks werden auch die anderen Windows-Updates, zusätzlich zu den Sicherheitsupdates installiert, mit welchen z.B. Fehler oder Kompatibilitätsprobleme behoben werden:**

   Für Windows 98 SE: Http://www.nandlstadt.com/win98sp/
   Für Windows 98: Http://www.pcwelt.de/downloads/betri...511/index.html
   Für Windows Me: Http://www.zdnet.de/enterprise/os/0,...00257-4,00.htm
   Für Windows XP und Vista: Http://www.winfuture.de/UpdatePack

Anmerkung für Windows XP Benutzer: Da seit einiger Zeit die neuen Sicherheitsupdates nur noch für Windows XP mit installierten Service Pack 2 angeboten werden, ist es nun auch Pflicht das Service Pack 2 zu installieren.
Wenn das System schon länger installiert ist und schon einige Installationen/Deinstallationen hinter sich hat, kann es sein, das das Windows durch die nachträgliche Installation von dem Service Pack instabil wird! In einem solchen Falle lässt es sich dann nicht vermeiden, die Festplatte zu formatieren, neu zu installieren und anschließend dann direkt das neueste Service Pack aufzuspielen, damit das System sicher und stabil läuft!

Anmerkung für Windows 95, 98, und Me Benutzer: Diese Betriebssysteme neigen schnell dazu instabil oder sehr langsam zu werden, wenn neue Updates oder ein neuer Internetexplorer installiert wird. Daher ist es am sinnvollsten dieses direkt nach der Windows Installation durchzuführen! Wenn sich jemand nicht gut genug damit auskennt wie er so etwas selber ausführen kann, dem empfehle ich einen Freund dazuzuholen der Erfahren genug ist, oder solche Installationen in einen PC-Geschäft durchführen zu lassen.

WGA-Prüfung:

Bei den Sicherheitsupdates wird von Microsoft die so genannte WGA-Prüfung (Windows Genuine Advantage) durchgeführt (Nur bei dem Patch-Loader bislang noch nicht) wobei dann geprüft wird, ob man auch ein originales Windows verwendet! Wenn Ihr ein originales Windows habt, welches auch nur ein einziges mal verwendet wird, und die WGA-Prüfung trotzdem scheitert, könnt Ihr dem nachgehen, dass das Windows auch als Original annerkannt wird! Dazu könnt Ihr Euch dann direkt an den Support von Microsoft wenden: Http://www.microsoft.com/germany/sit...k/default.mspx

Falls Ihr aber kein Original habt, oder das Windows auf mehreren PCs verwendet wird, dann besorgt Euch doch eine neue Windowslizenz, 70 EUR (z.B. bei Ebay) für Windows XP sind doch nicht zuviel, oder? Wenn Ihr dann einen neuen Windows-Key habt, kann dieser auch nachträglich, ganz offiziell online geändert werden, ohne Windows neu installieren zu müssen:
Http://www.microsoft.com/genuine/sel...displayLang=de

Microsoft wird immer rigoroser was das Thema „Raubkopien" angeht, sie wollen am liebsten die Sicherheitsupdates nur noch für **die** Nutzer anbieten, die sich dieser WGA-Prüfung unterziehen und diese auch erfolgreich "bestehen"!

2 a. Gilt nur für Windows 2000/XP: unbenötigte Dienste abschalten:

[[Hiermit werden alle standardmäßig offenen Fenster am Auto zugekurbelt]]
[[Nur für fortgeschrittene PC-Nutzer geeignet, alle anderen Hilfe dazuholen]]

Auch dieser Punkt ist zum PC Absichern sehr empfehlenswert! Bei Windows 2000 und XP gibt es die so genannten Dienste, die bestimmte Services zur Verfügung stellen. Diese Dienste sind dazu gedacht im Netzwerk bestimmte Aufgaben zu erfüllen. Nun ist es leider so, dass diese Dienste auch aus dem Internet her ansprechbar sind und damit Ports zum Internet hin öffnen. Diese geöffneten Ports sind ein willkommener Eingang für Angriffe auf Euer System!Dazu kommt noch, dass diese Dienste für "Normalnutzer" eh völlig uninteressant sind!

Mit dem Beenden dieser Dienste werden diese offenen Ports dann endgültig geschlossen (und nicht wie bei einer Firewall nur überwacht)! Dadurch wird den Schädlingen eine viel kleinere Angriffsfläche geboten, welches einer deutlich höheren Sicherheit entspricht!

Es gibt eine Internetseite wo sich einige Leute viele Gedanken genau über dieses "Problem" gemacht haben und die ein kleines Skript (Programm) erstellt haben welches automatisch alle diese überflüssigen (gefährlichen) Dienste auf Knopfdruck abschaltet! Es nennt sich svc2kXp.cmd und hat 4 verschiedene Funktionen inklusive die Möglichkeit alle vorgenommenen Änderungen wieder rückgängig zu machen!

die Funktion „(2) Standard“ benutzen!

Und auf dieser Seite gibt es ein ähnliches wie oben beschriebenes Programm mit grafischer Oberfläche, welches ebenfalls die überflüssigen Dienste abschaltet:
Http://www.dingens.org/

- Und alle Nutzer die einen Router zum Internet verwenden, oder die mit ihrem PC auf ein Netzwerk zugreifen, wählen bei dem Programm von Dingens.org die Funktion „Computer in einem Netzwerk“ - Und alle Anderen, welche über Modem, ISDN-Karte, oder per DSL ohne Router ins Internet gehen, und zudem kein Netzwerk verwenden, können die Funktion „Einzelner Computer“ verwenden!

- Auf der Homepage von dieser Seite, hat der Autor des Programms geschrieben, dass unter Windows XP SP2 die Dienste nicht **unbedingt** abgeschaltet werden müssen, wenn die Windows-Firewall eingeschaltet wird! Es stimmt zwar, dass es auch so geht, **aber sicherer und empfehlenswerter ist es trotzdem,** die Dienste auch unter SP2 abzustellen! Denn jeder Dienst weniger bietet eine kleinere Angriffsfläche, und diese Sicherheit kann keine Firewall ersetzen!

Anmerkung: Beim Ausführen dieser Dateien **kann** es passieren, dass bestimmte Treiber nachher nicht mehr richtig funktionieren oder dass die Netzwerkeinstellungen verändert werden. Dieser Schritt sollte also möglichst vor der Installation der Treiber ausgeführt werden. Es geht natürlich auch gefahrlos nachträglich wenn man sich damit auskennt, wie man einen Treiber drüberinstalliert oder wie das Netzwerk eingestellt war!

Anmerkung zu XP Antispy:
Mit diesem Programm können zwar auch ein paar Dienste von Windows beendet werden, es es sind viel weniger wie bei Ntsvcfg.de und bei Dingens.org, daher kann XP Antispy diese Programme nicht ersetzen!

Natürlich können alle diese Dienste auch ohne ein Zusatzprogramm manuell in der Systemsteuerung abgeschaltet werden:
Http://www.windows-tweaks.info/html/dienste.html

Und zuletzt, gibt es auf dieser Internet-Seite noch eine Beschreibung der einzelnen Dienste zum Nachlesen:
Http://www.different-thinking.de/win...00_dienste.php

Windows Vista:

Speziell für Windows Vista gibt es noch kein automatisches Programm, welches die überflüssigen Dienste abschaltet! Windows Vista ist noch sehr neu, und es gibt daher für dieses Betriebssystem bisher nur sehr wenige Schädlinge die diese Sicherheitslücken ausnutzen! Auf der folgenden Internetseite gibt es aber einen ausführlichen Artikel (für Nutzer mit fortgeschrittenen PC-Erfahrungen) über dieses Thema – wie man die Dienste unter Vista manuell abstellen kann:
Http://www.pcwelt.de/know-how/busine...486/index.html

2 b. Gilt nur für Windows 95, 98, 98SE, Me: unbenötigte Ports schließen:

[[Hiermit werden alle standardmäßig offenen Fenster am Auto zugekurbelt]]
[[Nur für fortgeschrittene PC-Nutzer geeignet, alle anderen Hilfe dazuholen]]

Auch bei diesen älteren Systemen gibt es offene Ports - nicht so viele wie bei Windows XP, aber trotzdem sollten sie geschlossen werden da sonst jeder Beliebige aus dem Internet über diese geöffneten Ports auf den Rechner zugreifen kann! Wie das im Detail geht, steht auf den folgenden Internet-Seiten:

Ports 137-139 schließen:
Http://www.trojaner-info.de/sicherhe...hritt5_neu.htm

NetBIOS und Port 135 beenden:
Http://www.virenschutz.info/virensch...rials-148.html

Nur bei Windows Me gibt es noch einen zusätzlichen Port (5000) den es zu schließen gilt:
Http://www.trojaner-info.de//report_port5000.shtml

3. Gilt nur für Windows 2000/XP/Vista: Nicht mit Administatorrechten im Internet surfen:

[[Alle Autoteile werden hiermit unveränderlich so fixiert, dass nichts mehr daran geändert werden kann!]]
[[[Auch für unerfahrene PC-Nutzer geeignet]]]

Da ein Administrator alles darf, auch wichtige Systemdateien verändern - geht es einem Virus oder Spyware genauso: Wenn der Schädling auf einen PC gelangt auf dem Administrator Rechte vorhanden sind, kann er sich ungehindert ausbreiten und sich installieren.
Wenn Ihr hingegen als eingeschränkter Benutzer surft - hat auch der Schädling auch nur eingeschränkte Rechte - das bedeutet er kann nichts auf C: also nichts an dem Windows verändern und damit geht sein Angriff ins Leere! Dieser Punkt bringt eine sehr gut erhöhte PC-Sicherheit!

Das reine Erstellen eines Benutzerkontos ist sehr einfach und kann auch von jedem unerfahrenen PC-Nutzer vorgenommen

Wenn Ihr ein eingeschränktes Benutzerkonto verwendet, und auf bestimmte Ordner zugreifen möchtet die standardmässig erstmal "gesperrt" sind, könnt Ihr diese mit folgenden Schritten freigeben:

1. Unter Windows XP Professionell klickt im Windows Explorer auf Extras - Ordneroptionen - Ansicht - und entfernt bei "Einfache Dateifreigabe verwenden" das Häkchen, falls es vorhanden ist! - Unter Windows XP HOME startet den PC einfach im abgesicherter Modus als Administrator - Und unter Windows 2000 könnt Ihr direkt mit Schritt 2 anfangen:
2. Danach könnt Ihr im Windows Explorer den entsprechenden Ordner der freigegeben werden soll, rechts anklicken - Eigenschaften - Sicherheit - und klickt dort bei dem Benutzer unter Vollzugriff auf "Zulassen"

Auf den folgenden Internet-Seiten gibt es noch viele weitere Hinweise, Anleitungen und Lösungsmöglichkeiten zum diesem Thema:
Http://www.xpsicherheit.de.nr/
Http://virus-protect.org/administrator.html
Http://www.chip.de/c1_forum/thread.h...hreadid=956782
Https://www.sicher-im-netz.de/partne...iches/fokus/18

Anmerkung: Dieser Schritt kann nur den PC schützen, wenn erstens als Dateisystem NTFS ausgewählt wurde (Nicht bei FAT32) und wenn zweitens auch ein sicheres Passwort für das Administrator UND das eingeschränkte Konto verwendet wurde! (Siehe auch Anhang C) Denn ansonsten kann der Schädling sich nämlich doch noch über "Ausführen als Administrator" aktivieren!
Außerdem ist es wichtig, dass immer ein **neues** Konto erstellt wird, mit den eingeschränkten Rechten! Niemals sollte ein vorhandenes Administrator Konto nachträglich „umgewandelt“ werden, denn wenn nur umgewandelt wird, bleiben nämlich einige Zugriffsrechte auf Windows weiterhin erhalten!

Dann gibt es noch noch ein weiteres Sicherheitskonzept **(Internet Security Suite: Win-SeO)**, welches automatisch alle Dienste abschaltet sowie einen Benutzer erstellt der noch weniger Rechte hat als ein normaler eingeschränkter Nutzer. Dadurch ist eine noch höhere Sicherheit gewährleistet. Allerdings sind für die Verwendung von Win-SeO schon fortgeschrittene PC Kenntnisse empfehlenswert!
(Die Sicherheitsupdates und sichere Internetsoftware müssen hierbei natürlich trotzdem noch installiert werden.)

Hier ist der Download und eine Beschreibung:
Http://www.win-seo.de/winseo.htm

Und hier werden viele Fragen dazu beantwortet:
Http://www.chip.de/c1_forum/thread.h...hreadid=896399

4 a. Sichere Internetsoftware verwenden, aktuelle Versionen, sowie die Sandboxie:

[[Wir benutzen ein Automodell welches unbekannter ist und anders funktioniert]]
[[Auch für unerfahrene PC-Nutzer geeignet]]

Der Internet Explorer und der Outlook Express sind die meist genutzten Programme. Dementsprechend gibt es auch genau für diese die meisten Schädlinge! Wenn dagegen ein Alternativ-Browser verwendet wird kommen viele Schädlinge gar nicht mehr in Frage!
Da unter den Betriebssysteme Windows 95, 98, 98SE und Me allgemein weniger Schutzmöglichkeiten vorhanden sind wie bei Windows 2000 und XP, ist dieser Schritt bei diesen älteren Betriebs-Systemen besonders empfehlenswert. Auch können sich damit Probleme erspart werden, welche sich des Öfteren mit dem Internet Explorer 6 unter Windows 98-Me ergeben.
Ein neuer Internet-Browser kann zur erhöhten PC Sicherheit übrigens völlig gefahrlos installiert werden, da ja an vorhandenen Einstellungen nichts verändert wird! Dieser Punkt ist nicht zwingend erforderlich, wenn die Punkte 0 - 3 schon umgesetzt sind, erhöht die Sicherheit aber trotzdem noch mal um ein gutes Stück!

Hier findet Ihr zwei gute alternative Internet Browser:

- **Firefox: (Sicherer Browser, Sehr schlicht, Weitere Funktionen müssen/können als Addins nachinstalliert werden)**
  Http://firebird-browser.de/
- **Opera: (Sicherer Browser, Großer Funktionsumfang, individuell gut Einstellbar)**
  Http://www.chip.de/downloads/c1_downloads_13000987.html
- **Noch weitere alternativen, und die Unterschiede der verschiedenen Browser sind hier zu finden:**
  Http://www.trojaner-info.de/hijacker/browser.shtml

Und eine empfehlenswerte Alternative für den Outlook Express gibt es hier:
Http://www.thunderbird-mail.de/

Falls Ihr aber doch lieber den Internet-Explorer verwenden wollt (so wie z.B. ich), sollte dieser aber unbedingt noch "sicherer" eingestellt werden! Es gibt nämlich zwei Funktionen, (Visual Basic Script und ActiveX) welche besonders praktische Funktionen auf den Internet-Seiten zur Verfügung stellen sollen. (Wie z.B. das Anschauen von Videos direkt auf einer Internetseite, und vieles mehr) Aber genau diese Funktionen können und werden, leider auch von sehr vielen Schädlingen missbraucht!
Die alternativen Browser (Opera, Firefox, Mozilla, Netzcape) hingegen unterstützen erst gar nicht diese „gefährlichen“ Funktionen!)

Da das Thema für sich komplex ist, empfehle ich für Nutzer mit weniger PC-Kenntnissen daher folgende einfache Vorgehensweise um jederzeit optimalen Schutz zu genießen und trotzdem bei Bedarf alle Funktionen nutzen zu

zurück auf **"Mittel"** (Damit werden die Funktionen dann wieder aktiviert)

Die Sicherheit kann übrigens auch während des Betriebs umgestellt werden, ohne das der Internet Explorer neu gestartet werden muss!

Und so kann die Sicherheit im Internet-Explorer auf Hoch/Mittel umgestellt werden:
Http://www.heise.de/security/dienste...anpassen/ie60/

Oder Ihr stellt die Sicherheit im Internet Explorer grundsätzlich manuell nach dieser Anleitung ein, dabei verzichtet Ihr dann aber grundsätzlich auf ActiveX und Visual Basic Script:
Http://www.datenschutz-bremen.de/sv_internet/ie.php
Http://www.blafusel.de/ie.html

Mit diesen Einstellungen ist der Internet Explorer zwar schon deutlich sicherer, aber noch immer nicht ganz so sicher wie die alternativ Browser!

Anmerkung: Das Windows Update (Falls Ihr es benutzt) benötigt eingeschaltetes ActiveX

Lediglich die Cookies werden mit dieser Einstellung (Hoch/Mittel) noch nicht mit einbezogen! Die Cookies sind kleine "harmlose" Textdateien welche für viele Funktionen (wie z.B. beim Online-Einkaufen den Einkaufswagen) benötigt werden. Allerdings können auch die Cookies missbraucht werden, wenn z.B. unseriöse Seiten mithilfe dieser Cookies das Surf-Verhalten des Nutzers zurückverfolgen um z.B. gezielte Werbung zuzuschicken!
Um Cookies nutzen zu können, aber nicht missbraucht zu werden, sollten die Cookies daher folgendermaßen eingestellt werden:
Http://www.sicherheit-online.net/sic...ger-umgang.php

- **Weitere Infos zum Thema Cookies:**
  Http://www.bsi-fuer-buerger.de/browser/02_04.htm
  Http://www.werle.com/helps/cookies.htm
  Https://www.datenschutzzentrum.de/se...es/cookies.htm
  Http://www.uni-koeln.de/rrzk/www/bro...onfig/cookies/
- **Zum Thema javascript:**
  Http://www.werle.com/helps/javascri.htm
- **Zum Thema Visual Basic Script:**
  Http://www.datenschutz-bremen.de/sv_...t/vbscript.php
- **Tipps zum Virenschutz im Outlook Express:**
  Http://www.jchanke.de/email/article/.../fenster.shtml

Ein weiterer erwähnenswerter Punkt zum Thema Sicherheit im Internet Explorer, betrifft die **Browser Helpers Objekts (BHO's)**, das sind kleine Miniprogramme, welche auf dem PC installiert sind, und ebenfalls bestimmte Funktionen im Internet zur Verfügung stellen! Manche Schädlinge missbrauchen diese BHO's um Viren etc. einzuschleusen, und andere Schädlinge installieren sich selber als BHO in den PC! Daher ist es grundsätzlich empfehlenswert, nur **die** BHO's zu verwenden die auch wirklich benötigt werden!

Hier findet Ihr weitere Informationen über die BHOs, und wie man „schlechte" BHO's wieder loswerden kann:
Http://www.bsi.bund.de/av/hijack/browserhj.htm

Aktuelle Versionen der Programmen verwenden:

Weiterhin ist es empfehlenswert, stets die aktuellen Versionen der Programme zu benutzen. Denn es werden in allen Programmen immer wieder neue Sicherheitslücken entdeckt, die mit neueren Versionen (oder mit Patches die ausgeliefert werden) dann wieder geschlossen werden! (Ähnlich wie bei den Windows-Updates!)

Es sollte also, von Zeit zu Zeit, immer nachgeschaut werden, ob neue Versionen vorliegen und diese dann aktualisiert werden! Bei vielen Programmen wird man automatisch auf neue Versionen aufmerksam gemacht, welches die Arbeit dann natürlich vereinfacht!

Dieses betrifft den Internetbrowser genauso wie Emailprogramme, Office, Musik & Video Abspielprogramme, Java, Chatprogramme usw.
Besonders wichtig ist es, wenn diese Programme mit dem Internet kommunizieren!

Alle bekannten Sicherheitslücken von allen Programmen, und Infos, wie/ob man sie schließen kann, findet Ihr hier:
Http://www.scip.ch/cgi-bin/smss/showadv.pl

Anmerkung: Ähnlich wie bei dem Internet Browser, können übrigens auch die anderen Programme (Office, Musik & Video Abspielprogramme, Java, Chatprogramme usw.) sicherer eingestellt werden! Zum Beispiel kann die Funktion „Codecs automatisch installieren" vom Windows Media Player, dafür missbraucht werden um Schadprogramme zu installieren!

Die Sandboxie:

Dieses ist ein kleines und für Privatanwender kostenloses Programm, mit dem ein „virtueller PC" (Sandkasten) simuliert wird! Wenn mit der Sandboxie im Internet gesurft wird, kann man nicht von Schädlingen von den Internetseiten infiziert werden! Daher kann die Sandboxie die Sicherheit im Internet gut erhöhen! Besonders die PC Nutzer, die mit Administartor-Rechten surfen, sind mit der Sandboxie sehr gut beraten!

- Und, wenn Ihr mit der Sandboxie Dateien herunterladet, landen diese ja erstmal nur innerhalb der Sandbox!
  Um eine Datei aus der Sandbox heraus zu "exportieren" geht im Windows-Explorer in den folgenden Ordner "C:\Dokumente und Einstellungen\Benutzername\Anwendungsdaten\Sandbox\DefaultBox\drive\"
  Von dort kann dann jede benötigte Datei kopiert werden!

Weitere Infos findet Ihr hier:
Http://virus-protect.org/artikel/tools/sandboxie.html

Download der Sandboxie:
Http://www.sandboxie.com/index.php?DownloadSandboxie

4 b. Unsichere Programme vermeiden, sowie: Linux als Betriebssystem?

[[Wir benutzen ein Automodell welches unbekannter ist und anders funktioniert]]
[[Auch für unerfahrene PC-Nutzer geeignet]]

Es gibt viele Programme, die meistens sehr populär und weit verbreitet sind, die aber leider ein erhöhtes Sicherheitsrisiko aufweisen! Denn für solche weit verbreiteten Programme ist es für Virenprogrammierer besonders lukrativ, Schädlinge zu erstellen, da dann umsomehr Nutzer infiziert werden können! Und wenn die Programmierer dieser Programme dann nicht regelmässig neue Versionen ihrer Programme anbieten, die gefundene Sicherheitslücken wieder schliessen, sieht es für den Endnutzer ungünstig aus!

1) Filesharing P2P Programme (Internet-Tauschbörsen) wie z.B. BitTorrent, eMule, KaZaa, Shareaza:

Internet-Tauschbörsen gehören leider zu den unseriösesten Anbietern, und dort werden sehr viele Schädlinge verbreitet, hierbei sollte deshalb, wenn überhaupt, nur ganz besonders vorsichtig umgegangen werden! Laut Studien sind bei den Tauschbörsen bei 45% der zum Download angebotenen Dateien, Viren oder Würmer und sonstige Schädlinge enthalten! Hinzu kommt noch, dass die meisten Downloads von diesen Tauschbörsen eh illegal sind, und damit die Nutzer verleiten werden, „Straftaten“ zu begehen!

Weitere Informationen zum Thema Tauschbörsen findet Ihr hier:
Http://www.internetrecht-rostock.de/filesharing.htm
Http://www.macwelt.de/news/internet/324057/index.html

Die sicherere Alternative: Verwendet zum Downloaden von Musik die offiziellen Musik-Download-Portale, ich finde 1 EUR pro Lied ist wirklich sehr günstig, und meistens gefallen einem eh nur wenige Lieder pro Album:

- **Musicload:** Http://www.musicload.de/start
  (Dieser Anbieter hat eine gute Auswahl an Liedern, es wird kein Zusatzprogramm benötigt, aber etwas teurer wie die anderen Anbieter)

- **iTunes:** Http://www.apple.com/de/itunes/store/music.html
  (Dieser Anbieter hat die allergrösste Auswahl von allen, es muss ein Zusatzprogramm installiert werden, ab Windows 2000, jedes Lied kostet nur 0.99 EUR)

2) Chat-Programme wie z.B. ICQ, MSN, IRC, AIM, Yahoo:

Bei diesen Chat-Programmen sollte man, (wenn man nicht darauf verzichten möchte) immer auf dem Laufenden bleiben, was Sicherheitslücken angeht und wie man sie schließen kann! Ausserdem sollten nie Dateien downgeloadet werden, wenn einem per Chat-Programm ein Link gesendet wird! Auch wenn der Link von einem Bekannten kommt, kann es eine automatisch generierte Nachricht mit Viren sein, daher sollte immer erst nachgefragt werden! (Sehr wichtig, besonders bei ICQ gibt es sehr sehr viele Infektionen wegen dieser Links in Chat-Nachrichten!)

Eine sicherere Alternative:

- **Miranda:** Http://www.chip.de/downloads/c1_downloads_13009297.html
  (Dieses Chatprogrammen ist kompatibel zu ICQ, MSN, Yahoo, AIM, Google Talk, IRC und Jabber, und ist kostenlos)

3) Toolbars wie z.B. die Google-Toolbar:

Solche Toolbars sind zwar meistens sehr praktisch, stellen aber leider ein erhöhtes Sicherheitsrisiko dar, da die Toolbars dazu missbraucht werden können um Schädlinge einzuschleusen! Ausserdem ist es auch immer fragwürdig, was der Anbieter mit den ganzen Informationen anstellt, die er von dem Benutzer der Toolbar zwangsläufig bekommt!

Die sicherere Alternative: Fügt einfach den Link der entsprechenden Homepage in die Favoriten/Lesezeichen ein, wenn Ihr dann z.B. bei Google suchen möchtet, benötigt Ihr nur zwei Mausklicks mehr, wie bei der Verwendung der Toolbar!

Zum Thema „Linux als Betriebssystem“?

Manche PC-Experten empfehlen, wegen der vielen Viren und Schädlinge die es gibt, auf Windows ganz zu verzichten, und

Um Linux zu verwenden sind mehr PC Kenntnisse nötig wie bei Windows, und es ist schwieriger, Problemlösungen zu finden! Ein Teil der „grossen bunten Windows-Welt“ geht bei Linux leider verloren! Meiner Meinung nach ist Linux nur für PC Nutzer geeignet, welche sich gerne und leicht in neue Materie einarbeiten, und denen es leicht fällt auf alle bekannten Programme zu verzichten!

Und da man ja auch unter Windows eine genauso gute Sicherheit erreichen kann, wenn man vorsichtig surft und das System dementsprechend einstellt, empfehle ich es nicht, auf Linux umzusteigen!

5 a. Antivirenprogramme:

[[Wir stellen Wachen um unser Auto auf, die aber teilweise ausgetrickst werden können!]]
[[Auch für unerfahrene PC-Nutzer geeignet]]

Anti-Virensoftware und Anti-Spyware Software stehen an der letzten Stelle der Verteidigung – Denn wenn eines dieser Programme etwas findet zeigt uns das, dass wir uns zuvor nicht "sicher" Verhalten haben! Der optimale Fall wäre, dass diese Programme nie zur Anwendung kommen!

Wichtig ist, diese Software und besonders den Virenscanner regelmäßig (am besten täglich) upzudaten. Und bedenkt auch das der Antivirus nie alle Viren findet und das es Schädlinge gibt die den Virenschutz abstellen können!

Nach meiner bisherigen Erfahrung, können Virenscanner nur bei ca. 50% der Schädlinge, effektiv diese daran hindern, dass das System infiziert wird! Besonders bei aggressiven Würmern und Trojanern sind Virenscanner oft „machtlos“! Deswegen empfehle ich die Punkte 0-4 meiner Anleitung viel mehr, (Da sie wirklich dafür sorgen dass das System erst gar nicht infiziert wird), als wie sich auf einen Virenscanner zu verlassen!

Es sollte übrigens immer nur ein reiner Virenscanner installiert werden, nie diese ganzen „Komplett-Pakete“, die immer mehr in Mode kommen! (siehe auch Anhang A)

Folgende kostenpflichtige Virenscanner sind sehr empfehlenswert:

1. **Kaspersky Anti-Virus Personal 6:** (Sehr gute Erkennungsrate, sehr schnelle Updates, sehr zuverlässig, und benötigt nur wenige Ressourcen)
   Http://www.kaspersky.com/de/kav6
2. **G-Data Antivirenkit 2007:** (Sehr gute Erkennungsrate und sehr schnelle Updates, da er ebenfalls die Kaspersky-Engine benutzt)
   Http://www.gdata.de/trade/DE/productview/705/3
3. **Bitdefender 10:** (Auch sehr gute Erkennungsrate, aber nur befriedigende Updates und höherer Ressourcenverbrauch)
   Http://www.bitdefender.de/PRODUCT-21...-Plus-v10.html

Und folgende kostenlose Virenscanner sind empfehlenswert:

1. **Active Virus Shield:** (Es gibt inzwischen von dem Kaspersky Antivirus diese leicht abgespeckte Version, die kostenlos für alle Nutzer zum Download angeboten wird! Bei dieser Version fehlt im Wesentlichen zum Original Kaspersky Antivirus: 1. Der proaktive Schutz, den meiner Meinung nach eh keiner braucht, 2. Der direkte Live-Scan des Http-Datenstroms, und 3. Die Signaturen für die Rootkit-Erkennung! Er hat sehr gute Erkennungsraten, sehr schnelle Updates und ist nur in Englisch verfügbar)
   Http://www.activevirusshield.com/ant...eav/index.adp?
2. **AntiVir 7:** (Sehr gute Erkennungsrate, befriedigende Updates, benötigt sehr wenige Ressourcen, öfters aber auch Probleme wie z.B. mit dem Update-Server)
   Http://www.free-av.de/

Ich habe mich nun doch entschlossen, noch ein paar weitere Antiviren-Programme hier aufzuführen! Bei allen diesen fünf Produkten handelt es sich um gute Qualität ohne nennenswerte Schwächen, wobei die oberen Produkte eher zu empfehlen sind! Ich empfehle jedem Leser, sich für eins von diesen hier aufgeführten Programmen zu entscheiden! Es sollte darauf geachtet werden, wirklich nur den reinen Virenscanner auszuwählen, keinesfalls die Komplett-Pakete mit integrierten Desktop-Firewalls!

Den Virenscanner von Norton empfehle ich trotz seinen guten Ergebnissen niemanden, da Nortons Programme sehr oft PC-Probleme verursachen!

Da sich die Qualität der Virenscanner stetig ändert (z.B. ist Antivirs Erkennungsrate deutlich besserer geworden) führe ich nun keine Virentest-Links mehr hier auf, wenn sie nicht ganz aktuell und seriös sind! Ich habe mich bei meiner Entscheidung, welche Programme ich hier aufführe, auf den aktuellen Test (2007) von der Stiftung Warentest gestützt sowie auf meine bisherige Erfahrung!

- **Virenscanner im Test:**
  Http://www.hr-online.de/website/spec...561346&seite=1
  Http://www.av-comparatives.org/index...paratives.html

Http://www.zdnet.de/security/praxis/...9141280,00.htm

Anmerkung: Es darf immer nur **ein** Virenscanner aktiviert sein, niemals zwei gleichzeitig, da sich diese gegenseitig behindern würden und im schlimmsten Falle der PC nicht mehr gestartet werden kann!

Falls Ihr Euch mal bei einer Datei nicht sicher seit, ob diese vielleicht einen Virus enthält, könnt Ihr diese Datei auch im Internet überprüfen lassen! Diese nun folgende Internetseite scannt die hochgeladene Datei mit 19 verschiedenen Virenscannern:
Http://virusscan.jotti.org/de/

5 b. Antispywareprogramme und HiJack This:

[[Wir stellen Wachen um unser Auto auf, die aber teilweise ausgetrickst werden können!]]
[[Auch für unerfahrene PC-Nutzer geeignet]]

Anti – Spywareprogramme sind sehr gut dafür geeignet, wenn sich Spyware oder Hijacker installiert haben, diese wieder loszuwerden! Da die meisten Virenscanner auf dem Spyware-Gebiet nicht so gut sind, empfehle ich folgende (kostenlose) Programme zu installieren, und damit, ein Mal pro Woche den PC zu überprüfen:

1. **AD-Aware Personal:** Http://www.lavasoftusa.com/products/...e_personal.php
2. **Spybot:** Http://www.chip.de/downloads/c1_downloads_13001443.html
3. **Spywareblaster:** Http://www.javacoolsoftware.com/downloads.html
4. **A-Squared Free:** Http://www.emsisoft.de/de/software/free/
5. **CWShredder:** Http://www.chip.de/downloads/c1_downloads_13011944.html

Bedienungsanleitung AD-Aware: Http://www.windows-tweaks.info/html/ad-aware.html
Bedienungsanleitung Spybot: Http://www.wintotal.de/Artikel/spybot/spybot.php

Anmerkung: Es können und sollten mehrere dieser Antispywareprogramme parallel genutzt werden, da sie nicht alle das gleiche finden, sondern Ihre unterschiedlichen Stärken haben und sich somit sehr gut ergänzen! Da diese Programme nicht durchgehend mitlaufen, sondern nur auf Abruf scannen, behindern sich die Anti-Spywareprogramme auch nicht gegenseitig!

Beim Scannen ist es hilfreich alle anderen laufenden Programme und Fenster zu schließen da, wenn etwas gefunden wird, dieses dann besser (eher) gelöscht werden kann. Wenn sich etwas trotzdem nicht löschen lassen will könnt Ihr nachschauen ob dieses "Programm" gerade mitläuft und es im Taskmanager beenden, oder es noch mal im Abgesicherten Modus versuchen!

Anti-Spyware Tests:
Http://spywarewarrior.com/asw-test-results-5.htm
Http://www.vnunet.de/tests/security/...051006036.aspx

HiJack This:

Und es gibt noch dieses weitere kostenloses und sehr empfehlenswertes Programm, welches alle aktuellen laufenden Programme und Tasks ausließt und eine Liste erstellt die auch online auf Schädlinge hin geprüft werden kann! Damit kann schnell und einfach herausgefunden werden ob etwas, oder was alles im Hintergrund mitläuft: (siehe auch Anhang B)

- **HiJack This - Download:**
  Http://www.spywareinfo.com/~merijn/programs.php
- **HiJack This - Automatische Online Logauswertung:**
  Http://www.hijackthis.de/index.php
- **HiJack This - Bedienungsanleitungen:**
  Http://www.giza-web.de/html/hijackthis-anleitung.html
  Http://www.hijackthis-forum.de/showthread.php?t=1794
  Http://www.wintotal.de/Tipps/Eintrag.php?TID=873

Wenn Ihr mit Hijack This einen Log-File erstellt habt, und diesen auf der automatischen Online Logauswertung überprüft habt, aber Ihr Euch bei manchen Einträgen nicht sicher seit, ob es sich nun um einen Schädling handelt oder nicht, könnt Ihr Euch auf den folgenden Internetseiten vergewissern:

Hier findet Ihr eine Liste der BHO's, welche gut sind, und welche von Schädlingen stammen:
Http://www.sysinfo.org/bholist.php

- X = Schädling: Spyware, Malware, oder anderer Schädling
  L = Legitime Software
  O = Offener Status (noch keine klare Meinung)
  ? = unbekannter Status

Http://www.sysinfo.org/startuplist.php

Anmerkung: Dieses Programm erstmal **nur für das Log-File** benutzen - Es kann zwar auch Einträge Fixen (löschen), aber wenn mit HiJack This versehentlich etwas falsches gelöscht wird, kommt man eventuell gar nicht mehr ins Internet! **Daher sollten nur erfahrene PC-Nutzer mit diesem Programm Einträge löschen!**

A. Desktop-Firewalls und Hardware-Firewalls:

Desktop-Firewalls:

Desktop-Firewalls sind Programme welche auf dem PC installiert werden. Sie versuchen die Daten zwischen PC und Internet zu kontrollieren und den Benutzer dann immer zu fragen welche von diesen Daten weitergeleitet werden sollen und welche nicht.

- **Beispiel:**
  Ein Schädling aus dem Internet versucht sich selbstständig z.B. über den Port 1234 in dem Ordner C:\Windows zu installieren. Die Desktop-Firewall merkt im Optimalfall dieses auch und meldet dem Benutzer eine Meldung wie „Unbekannte Anwendung versucht eine Verbindung über Port 1234 herzustellen – Zulassen oder Verweigern?“

Im Endeffekt ist eine solche Desktop-Firewall also nur ein Werkzeug, mit dem der Benutzer selber (wenn er sich gut genug auskennt) sein System schützen muss. Aber selbst wenn sich der Benutzer sehr gut auskennt, wird es den Virenprogrammieren immer wieder möglich sein, durch neue Tricks die Desktop-Firewall zu umgehen oder abzuschalten. Denn sie ist nur ein Programm welches zwangsläufig immer beeinflussbar ist!

Hinzu kommt noch, dass wenn die Punkte 0-4 umgesetzt wurden eh schon alle Bedrohungen unterbunden werden und damit einen Einsatz einer Desktop-Firewall überflüssig machen! Wenn z.B. die Dienste abgeschaltet wurden, gibt es eh keine offenen Ports mehr die überwacht werden müssten! Jeglicher Angriff von außen muss dann eh zwangsläufig scheitern! Die Desktop-Firewall wäre damit die ganze Zeit „arbeitslos“ und würde nur noch den Nachteil mit sich bringen, dass das System unnötig komplex und damit fehleranfälliger, sowie langsamer und instabiler wird! Ein gut gesichertes System, wird durch eine Desktop-Firewall etwas unsicherer wie daohne!

Desktop Firewalls - und warum man sie nicht braucht:
Http://www.ntsvcfg.de/#_pfw

Problematik, da Desktop-Firewalls leicht ausgetrickst werden können:
Http://home.arcor.de/nhb/pf-austricksen.html

Problematik, da Desktop-Firewalls nur mit hohen PC-Kenntnissen brauchbar eingestellt werden können:
Http://www.******************/pfw.html

Daher empfehle ich keinem Leser, sich ein Desktop-Firewall Programm zu installieren, welches dem Nutzer nur ein sicheres Gefühl gibt, aber keine wirkliche Sicherheit bietet! Stattdessen setzt lieber einen weiteren von den oben genannten Punkte 0-4 um, denn diese Punkte ersetzen nämlich die Funktion der Desktop-Firewall sehr wirksam und effektiv, haben keinerlei Nachteile, und sind zudem auch noch kostenlos!

Der Grund, warum die Desktop-Firewalls trotzdem so beliebt sind, liegt wohl darin, dass die Menschen vermeiden wollen, **selber** die Verantwortung für ihre PC-Sicherheit zu übernehmen! Viel einfacher ist es doch, den Anderen die Verantwortung zu überlassen, in diesem Falle z.B. der Firewall! Leider ist es aber nur eine Illusion, dass ein PC-Programm uns diese Aufgabe abnehmen könnte ...
In einem Forum bezeichnete ein Benutzer mal eine Desktop-Firewall als „Schnuller“ – und ich finde, dass ist nicht allzuweit hergeholt!

Hardware Firewalls:

Hardware Firewalls (z.B. Router) dagegen werden als eigenes "mechanisches Bauteil" zwischen dem PC und dem Internetanschluss eingebaut und angeschlossen. Sie kontrollieren nichts, sondern funktionieren einfach nur nach folgendem Schema, nämlich dass sie nur die Daten weiterleiteten, die von dem Benutzer auch „bestellt“ wurden! **Daher tragen Hardware-Firewalls zu einer guten erhöhten Sicherheit im Internet bei, und schaden dem Windows oder der Internetgeschwindigkeit in keinster Weise!**

- **Beispiel:**
  Wenn ein Schädling aus dem Internet versucht sich selbstständig z.B. über den Port 1234 in dem Ordner C:\Windows zu installieren landet er ja zuerst in der Hardware-Firewall. In der Hardware-Firewall gibt es aber weder einen Port 1234 noch einen Ordner C:\Windows – daher kann der Schädling dort nichts ausrichten. Und an den PC weiterleiten tut die Hardware-Firewall den Schädling auch nicht, weil der Benutzer nicht eigenständig auf „Downloade mir den Schädling“ geklickt hat. Damit geht der Angriff ins Leere.

Trotzdem sollten natürlich auch bei einer Hardware-Firewall die Punkte 0-5 umgesetzt werden, da es auch Schädlinge gibt die ganz andere Wege gehen und nicht von Ihr aufgehalten werden können!

Funktionsweise von Hardware-Firewalls:
Http://www.netzwelt.de/news/72750-dmz-nat-co-.html

Bei leichten Infektionen kann versucht werden, das System wieder zu bereinigen:

1. Als erstes sollten alle temporären Internetdateien sauber gelöscht werden, dies geht gut mit diesem Programm:
   CCleaner: Http://www.chip.de/downloads/c1_downloads_16317939.html

2. Danach sollte, mit einem guten Virenscanner, das System im abgesicherten Modus gescannt werden, dies geht gut mit diesem Programm:
   Active Virus Shield: Http://www.activevirusshield.com/ant...eav/index.adp?
   (Vor der Installation dieses Virenscanners muss unbedingt der bisherige (alte) Virenscanner komplett abgeschaltet werden, da nie zwei Virenscanner parallel laufen dürfen! Bedenkt auch die Funktion „mit Windows mitstarten“ abzustellen!)

3. Zuletzt sollte, mit guten Anti-Spyware Programmen, das System im abgesicherten Modus gescannt werden, dies geht gut mit diesen Programmen:
   AD-Aware Personal: Http://www.lavasoftusa.com/products/...e_personal.php
   Spybot: Http://www.chip.de/downloads/c1_downloads_13001443.html

4. Wenn dann, nach einem PC-Neustart und erneuten scannen, nichts neues mehr gefunden wird, also alle Scanner ein sauberes System anzeigen, sollte man sich zuletzt noch mit dem Programm HijackThis vergewissern! (siehe Punkt 5b) Wenn aber auch HijackThis keine Schädlinge mehr findet, kann man davon ausgehen das das System erfolgreich bereinigt ist!

Anmerkung: Falls Ihr die Systemwiederherstellung von Windows aktiviert habt, diese unbedingt vorher abstellen, denn sonst kann es sein, dass beim nächsten PC Neustart der Schädling wieder hergestellt wird! Ausserdem sollte zwischen jedem der Schritte der PC neugestartet werden!

- **Anleitungen, wie man im abgesicherten Modus startet, und wie die Systemwiederherstellung abgestellt wird, findet Ihr hier:**
  Http://www.bsi.de/av/texte/wiederher.htm
  Http://www.schieb.de/tipps/result.php?id=564287
  Http://forum.windowspower.de/Systemw...a-w10682-.html
  (Bei Windows Vista muss die Taste F5, für den abgesicherten Modus, beim PC-Start gedrückt werden)

- **Hier gibt es kostenlose Entfernungs-Tools für verschiedene, ganz bestimmte Schädlinge:**
  Http://www.wintotal.de/Tipps/Eintrag.php?TID=1187

- **Und auf den folgenden Seiten gibt es Online-Virenscanner, auf denen Online der PC auf Schädlinge hin geprüft werden kann:**
  Http://www.kaspersky.com/de/virusscanner
  Http://www.bitdefender.com/scan8/ie.html
  Http://www.pandasoftware.com/actives..._principal.htm

- **Und auf diesen Internetseiten gibt es weitere Anleitungen, wie man versuchen kann ein befallenes System zu bereinigen:**
  Http://www.hijackthis-forum.de/showthread.php?t=2912
  Http://www.paules-pc-forum.de/phpBB2/topic.98281.html

Bei schwereren (aggressiven) Infektionen: **[[Nur für fortgeschrittene PC-Nutzer geeignet, alle anderen Hilfe dazuholen]]**
(Beispiele: PC stürzt ab, Programme lassen sich nicht mehr starten, Festplatte ist ausgelastet, Virenscanner findet viele infizierte Dateien, nach PC Neustart findet Virenscanner erneut infizierte Dateien, HijackThis zeigt mehrere Schädlinge an, usw.)[/color]

Wenn das System einmal von einem aggressiven Virus oder Wurm befallen wurde, kann man selbst nach erfolgreichem Entfernen des Virus nicht wirklich sicher sein ob vielleicht schon andere Windows Komponenten manipuliert wurden. Nur, wenn die Festplatte komplett formatiert und Windows ganz neu aufgespielt wurde, kann man zu 100% sicher sein, dass das System wieder sauber und sicher ist!
Bedenkt bitte, dass hierbei sämtliche gespeicherten Dateien vom PC unwiderruflich gelöscht werden!

Auf dieser Seite wird auch noch einmal gut beschrieben, warum ein infiziertes System formatiert werden sollte:
Http://www.mathematik.uni-marburg.de...c-removal.html

Wenn kein Backup vorhanden ist, müssen alle Daten vorher gesichert werden! (z.B. auf CD gebrannt) Bei aggressiven Schädlingen kann es sein, dass Windows sich nicht mehr richtig bedienen lässt, in diesem Falle kann man noch versuchen, den PC im abgesicherten Modus zu starten – dort ist die Chance höher, dass der Schädling nicht aktiv wird!

(Durch den Virenbefall kann es in seltenen Fällen sein, das auch in den gesicherten Daten noch die Schädlinge Mit-Transportiert werden, daher sollten diese gesicherten Daten nicht direkt nach dem Formatieren neu aufgespielt werden, sondern erst 2 Wochen später, wenn mit den allerneuesten Signaturen alle diese Daten noch einmal gründlich gescannt wurden!)

Nach der erfolgreichen Installation von Windows XP müssen aber auch noch alle benötigten Treiber installiert werden, wie z.B. für das Mainboard, die Grafikkarte, Soundkarte, Netzwerk usw.!Ich empfehle daher allen, wenn sie so was noch nicht selber gemacht haben, jemanden dazuzuholen der damit vertraut ist! Wenn es aber niemanden gibt, kann man das Formatieren auch in einem PC-Geschäft durchführen lassen!

Für Windows 2000: Http://www.windows-tweaks.info/html/...tallation.html
Für Windows Me: Http://www.windows-tweaks.info/html/...tallation.html
Für Windows 98: Http://www.windows-tweaks.info/html/...tallation.html

- **Wie partitioniere ich eine Festplatte:**
  Http://www24.brinkster.com/thorsten1...ieren/win2000/

- **Wie installiere ich einen neuen Treiber:**
  Http://www.pcwelt.de/know-how/online/15837/

Die Installation von Windows und den Sicherheitsvorkehrungen sollten, um Software-Fehler und erneute Infektionen zu vermeiden, in folgender Reihenfolge vorgenommen werden:

1. **Windows auf einer leeren, formatierten Festplatte installieren (Nie auf ein vorhandenes System drüberinstallieren!)**
2. **Neuestes Service Pack installieren**
3. **Aktuelle Sicherheitsupdates installieren (Ohne Internetverbindung, also z.B. von CD!)**
4. **VIA 4in1 Mainboard Chipsatz Treiber (Falls vorhanden) installieren**
5. **Dienste abschalten und eingeschränktes Benutzerkonto einrichten**
6. **Restliche Treiber (Grafikkarte, Sound, Netzwerk, Maus usw.) installieren (Natürlich als Administrator)**
7. **Virenscanner, AD-Aware, Spybot und alternativen Browser installieren und einrichten**
8. **Internet Verbindung herstellen!**
9. **Vom Virenscanner, AD-Aware, Spybot und Spywareblaster die neuesten Signaturen/Updates herunterladen**

Zwischen jedem dieser Schritte sollte der PC neu gestartet werden!

Und allgemein ist noch zu empfehlen so wenige Programme wie möglich zu installieren und noch weniger Programme beim Windowsstart mitstarten zu lassen. Denn je weniger Programme mitlaufen, (genauso wie bei den Diensten) desto kleiner ist die Angriffsfläche für Schädlinge!
Im Taskmanager oder z.B. mit dem Programm "HiJack This" könnt Ihr sehen was alles mitgestartet wird. In den meisten Programmen kann man in den Einstellungen die Funktion "Beim Windowsstart mitstarten" abstellen.

Wem das zu kompliziert ist, dem empfehle ich folgendes kostenlose Programm, welches alle Programme die Mitstarten auflistet, und dass Mitstarten auf Wunsch komfortabel abschaltet! Hier gibt es den Download sowie eine Anleitung:
Http://www.toolsandmore.de/Central/P...start-Manager/

C. Sichere Passwörter verwenden:

[[Wir benutzen ein Türschloss, welches aus einer Zehnstelligen Zahlenkombination besteht, anstatt ein Türschloss welches nur aus einer Zweistelligen Zahlenkombination besteht]]
[[Auch für unerfahrene PC-Nutzer geeignet]]

Ein Passwort nützt herzlich wenig wenn es mit einem gängigen Tool aus dem Internet schon in wenigen Minuten geknackt werden kann! Daher sollte es aus möglichst vielen und unterschiedlichen Zeichentypen bestehen, damit ein Knack-Versuch Jahre dauern würde! (Anstatt nur z.B. 30 Sekunden)
Ein Passwort, was nur 8 Zeichen, aber dafür Klein- und Grossbuchstaben, Zahlen und Sonderzeichen enthält ist sicherer als ein Passwort welches 12 Zeichen aber nur aus Kleinbuchstaben besteht. Auch sollten Wörter welche im Duden stehen vermieden werden, da bei Knack-Versuchen solche Wörter als erstes automatisch ausprobiert werden.

Hier könnt Ihr online Testen wie sicher Euer Passwort ist, wenn die Internet-Seite geladen wurde rechts auf "Passwort-Check" klicken:
Https://passwortcheck.datenschutz.ch/

Wirklich sicher ist es erst wenn es Grün angezeigt wird - Dann würde es nämlich Jahre dauern das Passwort zu knacken - Bei Gelb hingegen wenige Tage - und bei Rot nur wenige Minuten! **Besonders die Passwörter fürs Internet sollten sicher sein wenn Ihr z.B. auch online Bezahldienste/Kreditkarten nutzt!**

Am einfachsten kommt Ihr an wirklich sichere Passwörter wenn Ihr Euch einen eigenen Satz ausdenkt und jeweils die Anfangsbuchstaben nehmt - z.B. aus "Morgens trinke ich immer eine Tasse Kaffee mit Milch" wird dann: **Mtii1TK+M** Dieses Passwort z.B. würde über 1000 Jahre zum Knacken brauchen - und ist leicht zu merken!

Eine weitere Möglichkeit ein sicheres Passwort, trotz einem Standard-Wort zu wählen, ist, dieses Wort mit Zahlen und Sonderzeichen zu unterbrechen! Aus „sterne“ wird dann: **ST--erne44** Dieses Passwort braucht über 3000 Jahre um es zu knacken!

Weitere Tipps zum Umgang und zur Auswahl:
Http://www.schieb.de/tipps/result.php?id=322715
Http://aktuell.de.selfhtml.org/artik...nken/passwort/

Und es ist wichtig, die Passwörter auch sicher aufzubewahren! Es gibt tatsächlich Benutzer die auf Ihrem Desktop (!) eine Datei haben, in der alle Ihre Passwörter völlig ungeschützt drin stehen, vom Email Accound bis zum Paypal-Konto! Ich finde, man sollte den anderen ja nicht gerade die Versuchung aufzwingen! Also, wenn Ihr die Passwörter schon auf dem PC speichern wollt, dann wenigstens in einer sicheren, ebenfalls Passwort-geschützten Datei!

Viele nehmen das Thema PC-Sicherheit nicht so wichtig, aber gerade in unserer heutigen Zeit wo die Menschen immer mehr kontrolliert und private Informationen weiterverkauft werden, sollte es solchen Organisationen meiner Meinung nach nicht so einfach gemacht werden. Ich persönlich möchte nicht, dass der ganzen Welt offen bekannt ist, wo ich gerne Einkaufe, welche Produkte ich bevorzuge, wie mein Kontostand ist und wie ich mein Leben führe. Das ist mir zu intim, ich würde ja auch nicht ein Schild an meine Haustüre hängen wo genau alle solche Informationen draufstehen! Unsere Bankdaten, oder unsere Informationen von Ebay werden ja noch so gut es geht geschützt und verschlüsselt, aber unsere eigenen Daten auf der Festplatte sollen für jedermann frei zugänglich sein?!
Noch schlimmer wird es, wenn unser eigener privater PC von dubiosen Organisationen für kriminelle Zwecke missbraucht und fremdgesteuert wird! Ich möchte nicht, dass mein PC ohne mein Wissen Jahrelang für die Verbreitung von SPAM Massen-Emails oder schlimmerem genutzt wird! Dagegen können und sollten wir etwas tun!

Hier ein Beispiel, was geschehen kann, wenn man auf die eigene PC Sicherheit nicht achtet:
Http://www.emsisoft.de/de/kb/articles/tec070503/

Jeder Nutzer der darauf achtet, selber ein sauberes und schädlingsfreies System zu haben, schützt automatisch damit auch alle anderen Nutzer vor Schädlingen! Wenn aber jemand nicht darauf achtet, bringt er damit unfreiwillig auch alle anderen Nutzer des Internets in erhöhte Gefahr!

Allerdings finde ich, muss man nicht zwingend **alle** oben aufgeführten Punkte gleichzeitig umsetzen! (Bis auf die Punkte 0, 1, 2 die sind wirklich Pflicht!) - Aber je mehr Punkte umsetzt werden desto unwahrscheinlicher wird das Risiko einer Infektion:

Jeder muss seinen eigenen Weg wählen wie er sein System absichert, worauf er verzichten kann und worauf er nicht verzichten will. Schließlich soll man ja auch noch Vergnügen am PC haben. Ich denke der goldene Mittelweg ist (wie im wirklichen Leben) auch hier der richtige!
Also: Weder "Desinteresse" noch "Sicherheits-Fanatismus", sondern von beiden Teilen zugleich wäre hier die Mitte - Nämlich gelassene Aufmerksamkeit!

Der Sicherheitsrechner:

Ich werde oft gefragt, wo Nutzer mir Ihre Sicherheits-Vorkehrungen nennen und sie wissen wollen, ob dieses denn nun ausreicht! Daher möchte ich hiermit allen Lesern Gelegenheit geben, einfach selber auszurechnen wie gut Ihre Gesamt-Sicherheit ist!
(Desktop-Firewalls wie z.B. Zonealarm sind hier nicht aufgeführt, da sie nur kaum zur erhöhten Systemsicherheit beitragen!)

In Frage für diesen Sicherheitsrechner, kommen diejenigen, welche die folgenden beiden Sicherheitspunkte schon umgesetzt haben:

- **Sicherheitsupdates regelmäßig installiert** (siehe Inhaltsverzeichnis Punkt 1)
- **Antiviren & Anti-Spyware Programme verwendet** (siehe Inhaltsverzeichnis Punkt 5a und 5b)

Wer nur diese beiden Sicherheitspunkte umgesetzt hat, dessen Sicherheit wird zuerst einmal mit der Schulnote **"ungenügend"** bewertet.

Nun kann aber, mit jedem der nun folgenden Sicherheitspunkte, die Gesamt-Sicherheit um jeweils eine Schulnote weiter verbessert werden:

- **Vorsichtig und Achtsam Surfen** (siehe Inhaltsverzeichnis Punkt 0)
- **Dienste abschalten / Ports schließen** (siehe Inhaltsverzeichnis Punkt 2a und 2b)
- **Keine Administatorrechte verwenden** (siehe Inhaltsverzeichnis Punkt 3)
- **Sichere Internetsoftware benutzen** (siehe Inhaltsverzeichnis Punkt 4)
- **Hardware-Firewall anschließen (z.B. Router)** (siehe Inhaltsverzeichnis Anhang A)

Dieses sind fünf verschiedene Möglichkeiten aus denen jeder ganz frei auswählen kann!
Wer alle auf einmal ausschöpft käme auf die Schulnote: "sehr gut"

Beispiele:
Wenn jemand neben den Sicherheitsupdates und dem Antivirenprogramm, zusätzlich noch vorsichtig surft, die Dienste abschaltet und eine sichere Internet-Software verwendet, dann kann bei diesem die Gesamt-Sicherheit mit **"befriedigend"** bewertet werden!

Wenn jemand hingegen neben den Sicherheitsupdates und dem Antivirenprogramm, nur noch zusätzlich sichere Internetsoftware verwendet, würde er eine Gesamt-Sicherheit von nur **"mangelhaft"** erreichen!

Anderes, mathematisches Beispiel:
Wenn wir vorsichtig und achtsam surfen, kommen z.B. 70 % der Schädlinge nicht mehr in Frage - bleibt also ein Restrisiko von 30%. Wenn dann die Dienste abgeschaltet sind, kommt der PC für weitere 70 % der Schädlinge nicht mehr in Frage - bleibt also ein Restrisiko von 9%. Wenn wir dann noch alle Sicherheitsupdates installieren sind wir wieder um 70% sicherer - bleibt also ein Risiko von nur noch 2,7% - Wenn wir mal annehmen das die sichere Internetsoftware und die Benutzerrechte je 50% Sicherheit bringen bleibt ein Restrisiko von nur noch 0,675% übrig - Damit fangen wir uns statistisch gesehen 148 mal so selten einen Virus/Spyware/Trojaner ein als ohne Sicherheitseinstellungen und ohne vorsichtigem Surfen!

E. Funktionsweise, Erkennungsmerkmale und was am meisten gegen die verschiedenen Schädlinge hilft:

Viren:
Viren sind die älteste Art von PC-Schädlingen. Sie versuchen dem Windows oder den Eigenen Dateien in irgendeiner Art zu

sie sich ganz selbstständig verbreiten. Ein Benutzer braucht nur im Internet eingeloggt sein, und schon kann es sein dass der Wurm den PC infiziert. Würmer kommen hauptsächlich erst ab Windows 2000 und XP in Frage. Gegen Würmer kann man sich nur durch die Punkte 1 und 2 schützen!

Trojaner/Backdoors:
Trojaner/Backdoors versuchen eine neue Tür (offenen Port) zu installieren um dritten Personen den Zugang zu Eueren PC zu gewährleisten. Wenn dies dem Trojaner gelungen ist kann jedermann, sobald die Internet-Verbindung besteht, auf den kompletten PC zugreifen und mit ihm machen was er möchte. Trojaner können sich nicht selbst verbreiten, sondern kommen in SPAM-Emails oder in Dateien von unseriösen Internetseiten vor.

Rootkits:
Rootkits sind meistens in Kombination mit Viren/Trojanern/Backdoors zu finden und haben aber die Besonderheit, dass die Rootkits die Prozesse so gut verstecken, dass sie nur sehr schwer aufgedeckt werden können.

Spyware:
Spyware versucht ein kleines Programm zu installieren welches immer, wenn Ihr online seid, dass Surf-Verhalten und alle möglichen anderen persönlichen Informationen an eine dritte Firma weiterzuleiten. Diese Firma verdient damit, da sie dann gezielt Werbung schicken kann, oder indem sie diese Informationen weiterverkauft. Spyware wird gerne bei unseriösen, kostenlosen Programmen einfach mitinstalliert.

Dailer:
Dailer versuchen eine neue Internet-Verbindung zu erstellen, welche dann z.B. 1,86 EUR/Min kostet oder pro Einwahl 50 EUR! Dieses kann aber aus technischen Gründen nur bei Modem und ISDN funktionieren. Nutzer von DSL sind daher von dieser „Gefahr“ unbetroffen!

Hijacker:
Hijacker sind kleine Programme die erzwingen, dass beim jeden Starten des Web-Browsers eine bestimmte Internet-Seite geöffnet wird, oder dass jede Minute eine bestimmter Werbebanner geladen wird. Dieses kann schnell lästig werden, zumal es sich meistens um unseriöse Internet-Seiten/Werbebanner handelt!

Viele Schädlinge bestehen aus Kombinationen von mehreren verschiedenen Schädlingen und können daher nur schwer einer einzelnen Schädlingsart zugeordnet werden. Auch ähneln sich einige Schädlingsarten sehr - aber im Grundprinzip trifft die Funktionsweise wie oben beschrieben statt.

Wenn ein PC von einem Schädling infiziert wurde, zeigt er oft einige von den folgenden Verhaltensmustern:

- **Die PC-Leistung ist ungewöhnlich verringert**
- **Es erscheinen Popup- oder sonstige unerwartete Meldungen**
- **Das System ist sehr instabil**
- **Die Festplatte ist ständig ausgelastet**
- **Es starten Programme automatisch**
- **Oder es können bestimmte Programme nicht mehr gestartet werden**
- **Die Internetverbindung ist ständig ausgelastet**
- **In der Startleiste oder auf dem Desktop erscheinen unbekannte Symbole**
- **Beim Starten des Internetexplorers wird immer eine unerwünschte Internet-Seite geöffnet und es kann keine andere Startseite mehr eingestellt werden**

Diese Verhaltensmuster müssen nicht immer zwangsläufig auf einen Schädling zurückzuführen sein, aber es sind die typischen Symptome! Es sollte dann mit Antivirensoftware, Anti-Spyware Software und dem Programm „HiJack This“ gescannt, und wenn etwas gefunden wird formatiert werden, [siehe Anhang B] denn diese Symptome weisen meistens auf schwerwiegendere Infektionen hin!

Abhilfe:
Gegen alle diese Bedrohungen (Bis auf die Würmer) hilft an erster Stelle der Schritt 0, nämlich keine unseriösen Internet-Seiten zu besuchen und besonders vorsichtig zu sein wenn es um Installationen von Programmen/Tools aus dem Internet geht! Denn viele Schädlinge (wie schon erwähnt) installiert sich der Benutzer selber, wenn er sich einen kostenlosen Bildschirmschoner installiert, oder auf unseriösen Seiten bei der Frage „Dieser Seite vertrauen“ auf „Ja“ klickt!

Die Punkte 1, 2, 3 und 4 dagegen, schützen davor dass sich irgendeiner dieser Schädlinge automatisch ganz von selber installieren kann! Es nützt also wenig, wenn nur vorsichtig gesurft wird, aber die Sicherheitsupdates nicht installiert werden – oder genauso wenig wenn alle Sicherheitsupdates installiert werden, aber unvorsichtig gesurft wird!

Und die Punkte 5a und 5b sind dafür gut, um zu prüfen ob das System auch noch weiterhin frei von Schädlingen ist! Spyware und Hijacker können in der Regel ganz gut nach einer Infektion erfolgreich mit Anti-Spywareprogrammen wieder entfernt werden, aber bei aggressiven Trojanern und Würmern sollte nach einer Infektion formatiert werden!

F. Geht das ganze auch als Kurzanleitung? – Zusammenfassung: In 7 Schritten zum sicheren PC!

Natürlich, wer nicht viel lesen möchte, und fortgeschrittene PC Kenntnisse hat, kann mit diesen 7 Schritten von dieser Kurzanleitung eine gute bis sehr gute Sicherheit erlangen! Gut ist sie ohne Router, und sehr gut für Nutzer mit Router:

1. Besuche keine unseriösen Internetseiten, betreibe kein Filesharing, lösche alle SPAM-Emails immer ungelesen, und Downloade keine Programme aus unbekannten Quellen!
2. Installiere, falls noch nicht geschehen, das neueste Service Pack, und aktiviere die automatische Windowsupdate-Funktion!
3. Schließe mit dem Programm auf dieser nun folgenden Internet-Seite alle unbenötigten Ports:
   Http://www.ntsvefa.de

Thunderbird!

6. Installiere die kostenlosen Anti Spywareprogramme AD-Aware und Spybot, und scanne mit diesen 1x pro Woche das System!
7. Wenn Du alle diese Punkte durchgeführt hast, kannst Du, falls eine Desktop-Firewall installiert ist, diese deinstallieren, denn von nun an ist sie eh arbeitslos!

G. Tests & Kontrollen zum Abschluss:

Hier gibt es ein kleines Programm mit dem man sehen kann welche Ports gerade verwendet werden:
TCP View: Http://download.pchome.de/download/t...2.80_1811.html

Und hier ein umfangreicheres Programm, welches alle Ports, aktive Prozesse, Autorun-Programme, Dienste und mehr anzeigt, diese mit einer Datenbank vergleicht, und farblich markiert ob es sich um sichere, unbekannte oder Schaedlinge handelt:
A-Squared HiJackFree 3: Http://www.hijackfree.de/de/hijackfree/

Hier findet Ihr eine Liste, welche Ports für was verwendet werden:
Http://www.emsisoft.de/de/kb/portlist/

Und es gibt einige Internet-Seiten auf denen man zur Kontrolle seinen PC nach offenen Ports scannen lassen kann – Damit kann man prüfen wie sicher das System geworden ist und mögliche Schwachstellen herausfinden:
Wichtig: Hierbei werden nur ein Teil der PC-Schwachstellen geprüft, daher sollte man sich nicht alleine auf ein solches Ergebnis verlassen!

Http://security.symantec.com/de
Http://www.security-check.ch/
Http://portscan.winboard.org/
Http://www.securityinfo.ch/firewallcheck.html
Http://www.virenschutz.info/portscanner.html
Http://www.heise.de/security/dienste/

Das Programm HiJack This (siehe Inhaltsverzeichnis Punkt 5b) ist auch sehr gut geeignet, um den PC auf Schädlinge aller Art hin zu prüfen!

H. Weitere Informationen und Links, sowie Verschlüsselung und Anonym surfen, und Kinderschutzprogramme:

Was ist Malware:
Http://de.wikipedia.org/wiki/Malware

Sicherheitstipps für den PC:
Http://www.sewecom.de/pc/
Http://www.wintotal.de/Artikel/pcsic...sicherheit.php
Http://board.protecus.de/t13020.htm
Http://sicher-ins-netz.info/
Http://www.bsi-fuer-buerger.de/brennpunkt/index.htm

Weitere sehr ausführliche Internet-Seiten zum Thema Sicherheit:
Http://virus-protect.org/
Http://www.computerbetrug.de
Http://www.comsafe.de/
Http://www.cidres-security.de/

Erste Hilfe bei Virenbefall:
Http://www.chip-faqs.smv-copgym.de/chip/viren.php

Was ist Spyware - und wie kann ich mich schützen?
Http://www.paules-pc-infothek.de/ppf...opic.php?t=625

FAQ: Spyware und Browser Hijacking:
Http://www.chip.de/c1_forum/thread.h...hreadid=688721

Infektion unvermeidbar? Und was tun wenn es passiert ist?
Http://oschad.de/wiki/index.php/Kompromittierung

Sicherheit, Datenschutz, anonym surfen im Internet:
Http://www.sicherheit-online.net/index.php

Fragen und Antworten:
Http://faq.underflow.de/

Der Link - Block:
Http://www.ntsvcfg.de/linkblock.html

Ports und Dienste im Griff:
Http://www.pcwelt.de/know-how/tipps...417/index.html

Http://www.aptv38.dsl.pipex.com/TheList/index.htm
Http://opensource-cd.de/progliste.htm

Windows XP Reparatur, (Nicht nach Virenbefall durchführen!) und die Reparaturkonsole:
Http://www.chip-link.de.vu/REPARATUR.html

Windows XP Systemwiederherstellung:
Http://www.pqtuning.de/winxp/sichern...tellung/xp.htm

Informationen, Tipps und Anleitungen für Windows:
Windows Vista FAQ: Http://www.winhelpline.info/daten/faqvista.php
Windows XP FAQ: Http://chip-faq.rufisplanet.ch/index.html
Windows 2000 FAQ: Http://www.winhelpline.info/daten/faq2000.php
Windows Me FAQ: Http://www.windows-tweaks.info/html/windowsme.html
Windows 98 FAQ: Http://www.windows-tweaks.info/html/installation3.html

Tipps wenn der PC einfriert:
Http://www.windows-tweaks.info/html/freezstopguide.html

Wie installiere ich einen neuen Treiber:
Http://www.pcwelt.de/know-how/online/15837/

Zum Thema Anonym Surfen:

Viele Nutzer haben sich zu diesem Thema noch eine Ergänzung gewünscht! Es gibt Programme und Möglichkeiten, dass über einen Drittanbieter die eigene Herkunft im Internet verschleiert wird. Das bedeutet, die Internetseite die gerade besucht wird kann nicht sehen wer der Besucher ist. Klingt ganz gut – funktioniert in der Praxis aber meist sehr schlecht – denn die Surf Geschwindigkeit wird damit so extrem verlangsamt als wie wenn man wieder mit einem 33.6 Modem surfen würde! Daher kann ich niemanden empfehlen einen solchen Dienst zu nutzen! Und falls jemand einen solchen Dienst für illegale Zwecke, wie z.B. Raubkopien nutzen wollte, würde ihm das auch nicht weiterhelfen da jeder dieser Anonym-Anbieter alle Informationen speichern, und diese bei Bedarf der Polizei weitergeben muss!

Wer sich trotzdem für dieses Thema interessiert findet auf den folgenden Internet-Seiten viele Informationen:
Http://board.protecus.de/t3305.htm
Http://www.mediauser.de/anleitung-an...urfen-mit-tor/
Http://www.netzwelt.de/news/74366-fi...urfen-mit.html
Http://www.buerschgens.de/Prox/
Http://www.anonym-surfen.com/anonym-...publikationen/

Zum Thema Verschlüsselung von Daten:

Auch zum Thema Verschlüsselung von Daten haben sich viele Nutzer einen Beitrag gewünscht! Da dieses Thema aber nicht direkt zum Thema PC-Sicherheit gehört, und es darüber schon gute Seiten gibt, verweise ich einfach auf diese folgenden Seiten:

Http://www.chip.de/c1_forum/thread.h...hreadid=823607
Http://www.mediauser.de/anleitung-fe...erschluesseln/
Http://uckanleitungen.de/truecrypt/
Http://www.mediauser.de/anleitung-da...erschluesseln/

Zum Thema Kinderschutz im Internet:

Wenn Ihr Euren Kindern einen Zugriff zum Internet einrichtet, aber vermeiden wollt, dass auch unseriöse Internetseiten besucht werden können, da Ihr dem Kind noch nicht zutraut dass es selber Verantwortungsvoll genug damit umgehen kann, gibt es folgende Möglichkeiten den PC dementsprechend einzurichten:

1. Es sollte zuerst, falls Ihr Windows 2000, XP oder Vista verwendet, ein "eingeschränktes Benutzerkonto" für das Kind erstellt werden! Damit kann es keine Programme mehr selber installieren, sondern muss immer ein Elternteil vorher fragen, damit dieses das Kind dann als "Administrator" anmeldet! Das bringt natürlich nur etwas, wenn dann für das Benutzerkonto für das Kind sowie für das Administrator-Konto für die Eltern, jeweils Passwörter vergeben werden!

   Anleitungen, wie das geht, findet Ihr hier:
   Http://virus-protect.org/administrator.html
   Https://www.sicher-im-netz.de/partne...iches/fokus/18

2. Dann, gibt es so genannte Kinderschutz Programme welche bestimmte Web-Inhalte blockieren, die von den Eltern ausgewählt werden können:
   Parents Friend: (kostenlos) Http://www.parents-friend.de/
   Kindersicherung 2007: Http://www.salfeld.de/software/kinde...ung/index.html

   Noch weitere Links zu dem Thema und weitere Möglichkeiten findet Ihr in diesem Artikel:
   Http://www.paules-pc-infothek.de/ppf...opic.php?t=789

3. Allerdings wäre es nicht ratsam, das Kind einfach nur grundsätzlich zu blockieren, sondern dass es zwischendurch trotzdem, (unter der Aufsicht der Eltern) frei surfen kann! Es reicht ja wenn es ein mal pro Woche für zwei Stunden ist! Denn wenn es ab und zu frei surfen kann, wird ihm nicht ganz "der Riegel vorgeschoben" - Das täte dem Kind nämlich auch nicht gut! Es könnte sonst dazu führen, dass es später wenn es älter wird, ein starkes Nachholbedürfnis entwickelt wodurch es dann erst recht "auf die schiefe

I. Backups:

[[Wir kaufen für nur 50 EUR eine komplette Kopie unseres Auto]]
[[Nur für fortgeschrittene PC-Nutzer geeignet, alle anderen Hilfe dazuholen]]

Und zum Schluss kann ich jedem noch als Herz legen, regelmäßig Backups (Images) zu machen wie z.B. mit Norton Ghost oder Drive Image! Denn nicht nur durch Viren können Daten zerstört werden, auch eine Festplatte kann unverhofft den "Geist aufgeben". Teilweise haben die Festplatten auch eine Lebensdauer von nur drei Jahren!
Und wenn mal ein falscher Treiber installiert wurde oder nach einem Update das System nicht mehr startet - und dann nicht wieder neu formatiert werden muss, ist es auch eine erhebliche Erleichterung!
Eine separate Festplatte mit z.B. 80GB ist schon für 50 EUR zu bekommen und auf einer solchen lassen sich sehr komfortabel alle Daten sichern. Im Optimalfall ist eine solche Festplatte nicht permanent angeschlossen, sondern nur für die Zeit während ein neues Backup gespeichert wird. Dadurch wäre dann selbst bei den aggressivsten Viren kein Datenverlust zu befürchten!

Hier gibt es einen ausführlichen Beitrag zum Thema Backup & Images:
Http://www.chip.de/c1_forum/thread.h...hreadid=865714

Für Daten, die viel Speicherplatz benötigen, aber sich meistens nicht groß verändern (wie z.B. eine MP3-Sammlung) können auch mit einer einfachen Batch-Datei die Daten schnell und einfach auf einem Backup-Medium gesichert werden. Mit dem Befehl:

XCOPY E:\Eigene~1\MP3*.* Z:\Backups\Eigene~1\MP3*.* /S /E /R /K /Y /D /H

werden alle Dateien in diesem und allen Unterordnern mit der gesamten Verzeichnis-Struktur gesichert. Das besondere hierbei ist, dass nur solche Dateien kopiert (überschrieben) werden, welche neurer sind, wie die Daten, die auf dem Backup-Medium schon vorhanden sind. Das bedeutet, wenn nur 5 MP3s hinzugekommen sind, aber 1000 Dateien in dem Ordner schon vorhanden sind, wird der Befehl zwar noch 2 Minuten brauchen bis er alle Dateien miteinander verglichen hat, aber trotzdem werden im Endeffekt nur die 5 neuen Dateien kopiert. Das geht viel schneller als wie wenn alle Daten immer komplett neu gesichert werden!
Alle schreibgeschützten, versteckten und Systemdateien werden bei diesem Befehl natürlich auch mitkopiert, und lange Dateinamen werden ebenfalls unterstützt!

Allerdings sollten nur Benutzer mit fortgeschrittenen PC-Kenntnissen solche Batch-Dateien erstellen und verwenden, da ansonsten unter Umständen bei kleinen Fehlern schon große Datenverluste angerichtet werden können!

Jeder darf übrigens diesen ganzen Text (unverändert)
kopieren und weiterverbreiten so wie er möchte!

Vielen Dank auch noch an Tobias28 sowie WhiteKnight/Humdinger, und die vielen anderen, deren Ergänzungsorschläge und deren Fragen bei Unklarheiten, diese Anleitung mit erweitert haben!

Und: Wer Rechtschreibfehler findet darf sie natürlich auch behalten!

Geschrieben von Bernd Homberg, Gandalf_AwA@web.de
-

Zitieren

18.03.2006, 00:20 #2 (permalink)

mr.aldei
Halbes Megabyte

Registriert seit: 04.2005
Ort: Mallorca des Ruhrgebiets (sagt Kachelmann)
Beiträge: 596

@Gandalf_AwA:

Danke!

_____
Da wird man alt wie eine Kuh und lernt immer noch dazu.
Rechner

Zitieren

20.03.2006, 11:53 #3 (permalink)

deoroller
Ganzes Gigabyte
Mein System

Registriert seit: 07.2000
Ort: 2003 UB313
Beiträge: 16.966

Ich schätze solche Beiträge.

Was mir weniger gefällt ist, wie darauf hingewiesen wird, dass das Arbeiten unter eingeschränkten Rechten eher fortgeschrittenen Anwendern zu empfehlen sei.

Tatsache ist, dass erfahrene Anwender aus Fehlern gelernt haben und von sich aus Sicherheitsrisiken meiden, wie Arbeiten unter Adminrechten.

Da wäre es klug, Anfängern vor Schaden zu bewahren und allen diesen Schutz dringend zu empfehlen, damit nicht jeder die selben Fehler macht.

Selbst MS versucht das im kommenden Windows Vista umzusetzen.

Diese Sicherheitsstrategie wird z.B. in jedem Internetforum praktiziert. Auch ein Mod hat nicht alle Rechte.
Es gibt auch immer wieder Mitglieder, die sich wie Schädlinge verhalten. Wenn die alle Rechte hätten, wäre das das Todesurteil eines Forums.

Aus einem Forumsbeitrag "aus Versehen die Festplatte formatiert" könnte dann "aus Versehen das Forum formatiert" werden.

_____
Warnung! Falscher oder fehlender Kaffee - Benutzer angehalten.
Eine NAT-Firewall ist ein schwarzer Schimmel.

Zitieren

27.03.2006, 15:05 #4 (permalink)

Matze88
Byte

Registriert seit: 08.2004
Beiträge: 76

Ein sehr schöner Beitrag... aber vielleicht solltest du noch einen Punkt zu Verschlüsselung von Daten hinzufügen...

mfg
Matze

Zitieren

31.03.2006, 21:13 #5 (permalink)

Gandalf_AwA
Byte

Registriert seit: 04.2005
Beiträge: 27

Hallo deoroller,

Danke für Dein Lob!
Du hast ja Recht, das die Rechte eine Menge Sicherheit bieten die kein Programm ersetzen kann! Aber den unerfahreren Lesern kann ich diesen Schritt trotzdem nicht mit gutem Gewissen empfehlen! Ich möchte nicht dass irgendein Leser durch meinen Text seinen PC "lahmlegt"!

und Hallo Matze88,

Hmm, eine sehr gute Idee, ich habe ja auch schon einige andere Punkte die nicht direkt zum Hauptthema gehören! Allerdings muss ich mich erst selber darüber noch ausgiebig informieren, bevor ich dann anderen Ratschläge geben kann! Kommt aber auf jeden Fall in meine "To-Do" Liste!

Bis Ende des Jahres bin ich nur wenig online, aber danach bin ich wieder voll da!

Es kann also etwas länger dauern!

viele Grüsse,

Bernd

Zitieren

31.03.2006, 22:27 #6 (permalink)

deoroller
Ganzes Gigabyte
Mein System

Registriert seit: 07.2000
Ort: 2003 UB313
Beiträge: 16.966

Zitat:

> Zitat von **Gandalf_AwA**
> *Aber den unerfahreren Lesern kann ich diesen Schritt trotzdem nicht mit gutem Gewissen empfehlen! Ich möchte nicht dass irgendein Leser durch meinen Text seinen PC "lahmlegt"!*

Die Gefahr besteht grundsätzlich nach dem Einschalten des PC.
Kann jedem passieren.
Deshalb ist eine persönliche Sichererungsstrategie zum schnellen Wiederherstellen des Systems unerlässlich. (z.B. Imagesicherung vor einschneidenden Veränderungen)
Wer sich nicht darum kümmert, muss oder will Leergeld zahlen.

Im Übrigen dürfte die Gefahr eines lahmgelegten PC, die von diverser Sicherheitssoftware ausgeht, größer sein, als das Arbeiten unter eingeschränkten Rechten oder Abschalten von Diensten. Ein kaputtes Benuterkonto kann man löschen und neuanlegen und klemmende Dienste über die Wiederherstellungskonsolte abschalten oder fehlende einschalten.
Beides braucht man noch nichtmal zu fürchten, wenn man innerhalb weniger Minuten das Image der Systempartition zurückspielen kann.

_____
Warnung! Falscher oder fehlender Kaffee - Benutzer angehalten.
Eine NAT-Firewall ist ein schwarzer Schimmel.

Zitieren

02.09.2006, 20:45 #7 (permalink)

Wolfgang77
Ganzes Gigabyte

Registriert seit: 10.2002
Beiträge: 16.428

Zitat:

> Euer nicht XP Nutzer hat die Firewall Zone Alarm noch die besten Kritiken

Es gibt keine "Hardware-Firewalls", auch in einem Router läuft ein Stück Software, zum Beispiel in einer FritzBox (Router) ist das Linux
.

_____
|| Wolfgang77
■ the future is now

Zitieren

15.09.2006, 15:07 #8 (permalink)

kanallie
Byte

Registriert seit: 05.2006
Beiträge: 45

@Gandalf_AwA: Vielen Dank an Dich, gute Arbeit und weiter so!
Dir wird hiermit die GOLDENE TASTATUR für Deinen sinnvollen Beitrag verliehen! Gruss Kanallie

_____
Alles verändert sich...nur das Formatchaos ist geblieben.....

Geändert von kanallie (15.09.2006 um 15:43 Uhr). Grund: Ergänzung

Zitieren

24.01.2007, 22:07 #9 (permalink)

zeiss
ROM

Registriert seit: 01.2007
Beiträge: 2

An Aktualität nicht zu überbieten .....

So banal wie manche Aussagen sind, aber solche Beiträge sind für viele Internetnutzer äußerst wichtig - man lese nur das unheimliche Gejammer über die GEZ- und 1§1-Mails.
Wer betroffen ist - warum auch immer - bräuchte nur sein Norton Ghost anschmeißen und die Systempartition wieder herstellen.
Das wars! Oder ist der allerletzte Punkt im Eröffnungsbeitrag etwa nicht richtig?
Gruß zeiss

Zitieren

24.01.2007, 22:49 #10 (permalink)

deoroller
Ganzes Gigabyte
Mein System

Registriert seit: 07.2000
Ort: 2003 UB313
Beiträge: 16.966

So einfach wird es nicht sein. Wer Dateianhänge von Emails sorglos öffnet, wird wohl kaum ein Backup gemacht haben.
Ein Backup nutzt auch nur etwas, wenn es aktuell und frei von Schädlingen ist.

_____
Warnung! Falscher oder fehlender Kaffee - Benutzer angehalten.
Eine NAT-Firewall ist ein schwarzer Schimmel.

Zitieren

Antworten

Seite 1 von 2 **1** 2 >

« Vorheriges Thema | Nächstes Thema »

Forumregeln

Es ist Ihnen **nicht erlaubt**, neue Themen zu verfassen.
Es ist Ihnen **nicht erlaubt**, auf Beiträge zu antworten.
Es ist Ihnen **nicht erlaubt**, Anhänge anzufügen.
Es ist Ihnen **nicht erlaubt**, Ihre Beiträge zu bearbeiten.

vB Code ist **An**.
Smileys sind **An**.
[IMG] Code ist **An**.
HTML-Code ist **Aus**.
Trackbacks are **Aus**
Pingbacks are **Aus**
Refbacks are **Aus**

Ähnliche Themen

Thema	Autor	Forum	Antworten	Letzter Beitrag
Wie kann ich meinen Drucker über meinen DSL Router ins Netzwerk einbinden ?	Timmäh!!!	Drucker	3	02.01.2006 12:53
HW- oder SW-Firewall...wie mache ich mein System sicher?	jomei	Netzwerke	5	03.02.2004 21:51
Wie mache ich Screenshots?	marquardtmartin	Software allgemein	3	23.01.2002 16:07

Alle Zeitangaben in WEZ +2. Es ist jetzt 22:17 Uhr.

PC-WELT online - Archiv - Nach oben