

PC-SICHERHEIT

AK
PC-Berater



**Wie Sie
Ihren
Computer
sicherer
machen!**

Herausgeber, Medieninhaber und Verleger: Kammer für Arbeiter und Angestellte für Salzburg. - Für d. Inhalt verantwortlich: Mag. Heimo Typplt und Georg Bogojevic - Produktion: Michael Koch, alle A-5020 Salzburg, Markus-Sittikus-Straße 10. - Druck: Koller-Druck, Lamprechtshausen

PC-Sicherheit

**Wie Sie Ihren Computer
sicherer machen!**



Vorwort

**Sehr geehrte
KonsumentInnen und
InternetbenutzerInnen!**

Einsteiger in die Welt des Internet tun sich oft schwer, die Sicherheit ihres privaten PCs einzuschätzen, aber auch erfahrene User sind oft erstaunlich sorglos.

Diese Broschüre soll Ihnen Tipps geben, wie Sie Ihren PC sicherer machen können – und zwar ohne große Kosten und viel Aufwand. Oft genügen schon ein paar Klicks, um Ihre Daten zu sichern und Ihre Privatsphäre zu wahren.

Informationen über PC-Sicherheit füllen Bände der Fachliteratur. Hier geben wir Anleitungen und Anregungen für den Durchschnitts-PC-Anwender, ohne besonders auf die Technik einzugehen, die dahinter steht.

Ich wünsche Ihnen sicheres Surfen!

Ihr

Siegfried Pichler
AK-Präsident

Oft gestellte Fragen (FAQ's)

Gibt es eine rechtlich garantierte Sicherheit?

Natürlich gibt es eine Reihe von gesetzlichen Bestimmungen, welche bei einem Angriff von außen auf Ihren PC zum Tragen kommen. Das sind in erster Linie zivilrechtliche Unterlassungs- und Schadenersatzansprüche oder datenschutzrechtliche Bestimmungen. Allerdings ist eine – nachträgliche – rechtliche Verfolgung meist langwierig und auch mit Kosten verbunden. Häufig ist eine solche Verfolgung nicht oder nur schwer möglich, da der Schadensverursacher unbekannt ist oder irgendwo im Ausland sitzt. Aus diesem Grund sollen hier nur einfache technische Ratschläge angeführt werden, bei deren Einhaltung Probleme erst gar nicht entstehen sollten.

Was verstehen wir in diesem Folder unter »Sicherheit«?

Es soll einerseits Eindringlingen so schwer wie möglich gemacht werden, an Ihre Daten zu gelangen und diese zu verändern (löschen,

kopieren, etc), oder Ihre Gewohnheiten auszuspiionieren. Andererseits sollen Sie auf gewisse Sicherheitslücken hingewiesen werden, welche im schlimmsten Fall zu einem finanziellen Schaden führen können.

Viren – Würmer – Trojaner

Traurig, aber wahr: sehr viele User arbeiten heute noch ohne einen vernünftigen Virenschutz. Dabei ist das heutzutage schon fast grob fahrlässig.

Wir raten dringend, ein Antiviren-Programm zu installieren!

Jeder braucht heute ein Antivirenprogramm – auch wenn Sie kein Internet haben (Es kommt z.B. nicht selten vor, dass der Nachwuchs virenverseuchte „Schulhofkopien“ von Spielen installiert und damit das System lahm legt).

Aber Achtung: Auch ein Antiviren-Programm ist praktisch nutzlos, wenn man es nicht regelmäßig per Internet selbst auf den neuesten Stand bringt!

Die neuesten Versionen von Antivirenprogrammen haben dies berücksichtigt und übernehmen das automatisch für Sie. Dies ist nicht nur komfortabel und einfach für den Anwender, sondern

bietet auch den bestmöglichen Schutz. Das Programm ist immer aktiv, sodass es Sie vor Viren schützen kann. Es erkennt aber auch, wenn eine Internetverbindung aktiv wird und updatet sich dann automatisch sozusagen „im Hintergrund“ und informiert Sie danach über das erfolgte Update.

Mittlerweile kommen schon fast täglich neue Viren in Umlauf. Schon deswegen sollte man täglich kurz ins Internet, damit das Antiviren-Programm sich automatisch updaten kann.

Sind zwei Virenprogramme besser als eines?

Nein, eines genügt vollauf! Zwei Antiviren-Programme gleichzeitig laufen zu lassen kann sogar zu Komplikationen führen, nämlich dann, wenn beide Programme gleichzeitig Zugriff auf eine Datei verlangen.

Die beiden bekanntesten Antiviren Programme „McAfee“ und „Norton“ sind beide sehr gute Programme, die man vorbehaltlos empfehlen kann. Für welches der beiden man sich letztendlich entscheidet, kommt schon fast einer „Glaubensfrage“ gleich, da nicht selten auch „Computerexperten“ im Streit darüber liegen, welches der beiden Programme nun das bessere sei. Die Kosten liegen für beide bei ca. 40 Euro.

Viren per E-Mail

Viele Viren verbreiten sich per E-Mail. Wenn Sie ein übervolles Postfach haben (siehe auch AK-Folder „Spam“), werden mit Sicherheit auch einige virenbefallene Mails darunter sein. Der Absender ist meist gefälscht, sodass es den Anschein hat, die Mail würde von einer seriösen Quelle kommen.

Eine weitere Falle, die Sie zum Öffnen der Viren verleiten soll (diese werden als Anhänge mitgeschickt): Der Virus schreibt einen kleinen Text in der Mail dazu, dass diese Mail virengeprüft wurde und es sich hierbei um keinen solchen handeln würde.

Kurz gesagt:

Öffnen Sie NIE Anhänge von Ihnen unbekanntem Quellen! Dies gilt auch dann, wenn Sie den Absender zwar kennen, das Mail von der Aufmachung her jedoch irritierend ist.

Beispiel: Ihnen ist der Absender namentlich bekannt, jedoch schickt er Ihnen nur kurz etwas „zur Info“, einen Anhang ohne persönliche Anrede. Oder der Freund schickt Ihnen Ihre „Anmeldedaten“ zu. In diesem Fall gilt: *Nicht öffnen und sofort löschen.*

Gut haben es hier Besitzer von Antivirensoftware, die Sie bereits beim Eingang der Mail über den Virus benachrichtigt und diesen außer Gefecht setzt.

Mehr zu Thema Spam erfahren Sie im AK-Folder „SPAM“

„Malware“, „Spyware“ und Browsersicherheit

Den Begriff „Internetbrowser“ wird jeder schon einmal gehört haben. Er steht für das Programm, das Sie zum Surfen verwenden. In den meisten Haushalten wird dazu der Internet-Explorer der Fa. Microsoft verwendet, da es ja schon mit dem Betriebssystem ausgeliefert worden ist.

Leider häuften sich die Meldungen über Sicherheitslücken in diesem Programm, sodass man gezwungen war, dieses Programm durch Sicherheits-Updates und neuere Versionen ständig zu verbessern.

So war es auch „Dialer“-Programmen möglich, sich unbemerkt auf dem PC einzunisten. Aber nicht nur Dialerprogramme können von unseriösen Adressen heruntergeladen werden, sondern beispielsweise auch ganze „Fernwartungs-Programme“, die einen Vollzugriff auf Ihren PC

ermöglichen. Hierzu wird ein kleiner Programmteil unbemerkt heruntergeladen (ein sogenannter „Loader“), der wiederum den Rest des Programmes herunterlädt und installiert.

Diese kleinen Programme sind allerdings nicht als Viren eingestuft (Viren verbreiten sich ja selbständig, diese Programme nicht). Ein neuer Begriff musste für diese neuen Schädlinge gefunden werden: Malware.

Unter Malware versteht man alle Programme, die Sie ausspionieren wollen (z.B. Ihre Surfgewohnheiten) oder das System verändern (z.B. Weiterleitung an eine andere Homepage). Nicht zu verwechseln mit „Spyware“. Unter diesen versteht man Software, die durchaus einen Nutzen hat, allerdings gerne über das Internet Informationen über Sie an den Hersteller schickt (z.B. welche Filme, Musik, etc. am PC konsumiert wurden, wie oft und wann).

Browser-Hijacking

Darunter versteht man die „Entführung“ Ihres Browsers. Ihre Startseite ist plötzlich weg, und Sie befinden sich auf einer Ihnen gänzlich unbekanntem Seite. Oder Sie tippen die Adresse einer Ihnen bekannten Internetseite ein und landen stattdessen auf einer englischsprachigen Suchmaschine oder Sexseite.

Dies rückgängig zu machen kann sich als äußerst schwierig erweisen, da diese Programme sich sogar in die Registrierungs-Datei von Ihrem System einschreiben und bei jedem Systemstart aktiv werden!

Wie wird man solche Programme los?

Mit kostenlosen Programmen aus dem Internet. Eines der bekanntesten ist zum Beispiel „Ad-Aware“ der Firma Lavasoft, das wir an dieser Stelle empfehlen können.

Die „PersonalEdition“ ist kostenlos von der Seite

<http://www.lavasoftusa.com/software/adaware/>
zu beziehen.

Anders als Antiviren-Software arbeitet das Programm nicht automatisch im Hintergrund, sondern muss Schritt für Schritt nach dem Surfen angewendet werden, um alle eventuellen Veränderungen an Ihrem System zu reparieren. Das gleiche gilt für die Aktualisierungen, diese sind ebenfalls manuell einzuleiten.

Doch wenn Sie es sich angewöhnen, nach dem Surfen jedesmal eine Überprüfung des Systems durch dieses Programm durchzuführen (die Zeitdauer ist hierbei je nach System mit nur einigen Minuten nicht wirklich hoch), kann man dies leicht verschmerzen und ist noch immer sehr gut geschützt. Weiters „repariert“ es

auch die sogenannte „Registry“ des Betriebssystems, sodass das System beim nächsten Neustart wieder „sauber“ ist.

Es gibt eine komfortablere Version des Programmes, die Sie auch während des Surfens schützt, diese ist allerdings **nicht** kostenlos.

Auch hier gilt: regelmäßig updaten! Nach Möglichkeit circa zwei Mal die Woche überprüfen, ob eine neue Version erhältlich ist.

Zurück zum Browser:

Sie werden sich vielleicht fragen, warum das Produkt „Browser“ nicht sicherer gemacht wird, anstatt mit anderen Programmen die Schäden zu flicken.

Nun: es wird verbessert! Und auch regelmäßig. Doch Hand aufs Herz: Wann haben Sie zuletzt ein Sicherheitsupdate von Microsoft heruntergeladen?

Presseberichten zufolge soll das Sicherheitsupdate, das den Befall eines Computersystems durch den Sasser-Virus verhindert hätte, 14 Tage vor Ausbruch des Virus online erhältlich gewesen sein!

Unter *www.microsoft.de* finden Sie in der Rubrik Sicherheit viele Downloads, die Ihr System sicherer machen werden.

AK-Tipp

Alternativbrowser Firefox

Dieser äusserst empfehlenswerte Browser ist unter www.mozilla.org zu beziehen und in 25 Sprachen für Windows, Macintosh wie auch Linux erhältlich. Absolut kostenlos, „nur“ 4,7 Megabyte in der deutschen Version groß, bietet der Browser alles was man sich als Surfer erwartet: ein schönes Design, einen sehr guten „Popup-Blocker“ (der aufspringende Fenster und damit auch unerwünschte Downloads verhindert) und weitere sinnvolle Optionen.

Ein sehr sicherer Browser, der bereits mehrere unabhängige Tests gegen den Microsoft Internet-Explorer gewann.

Auch hier gilt: in Zukunft die Augen aufhalten nach Updates! Der Firefox hat bereits erfolgreich am Marktanteil des Internet-Explorers geknabbert. Und je mehr Personen ihn benutzen, desto interessanter wird es auch für Malware-Verbreiter, eventuelle Sicherheitslücken des „Feuerfuchses“ aufzuspüren und gegen Sie zu verwenden.

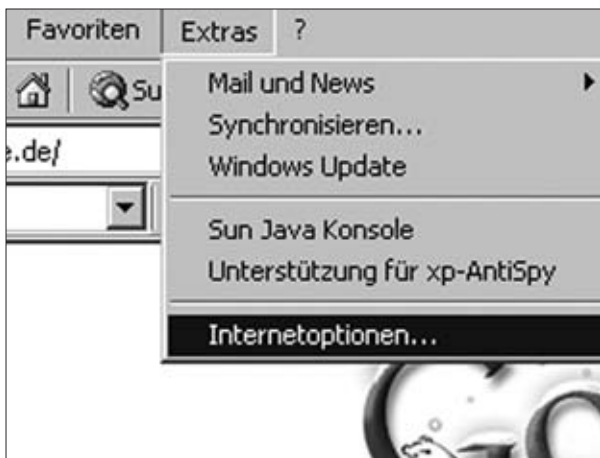
Doch derzeit gilt: Empfehlenswert!

Java und ActiveX:

Auf der einen Seite ermöglichen diese „Bestandteile“ des Browsers das Ausfüllen von Internet-Formularen oder das automatische Abspielen von Musik beim Besuch einer Website, andererseits stellen sie auch ein Sicherheitsrisiko dar. Durch Java-Befehle wäre es z.B. auch möglich, virenverseuchte Dateien auf den PC zu installieren (wie Trojaner, die eventuell einen Vollzugriff auf Ihren PC ermöglichen könnten).

Wenn Sie „auf Nummer Sicher gehen“ wollen, sind diese beiden Optionen folgendermaßen auszuschalten:

Schritt1: Öffnen Sie Ihr Browserprogramm (In diesem Fall Microsoft Internet Explorer)



Im Microsoft Internet Explorer finden Sie den Menüpunkt „Internetoptionen“ unter „Extras“

Schritt 2: Klicken Sie auf die Schaltfläche „Sicherheit“ und „Stufe anpassen“



Schritt 3: Hier können Sie alle relevanten ActiveX-Einstellungen und Java deaktivieren, bzw. so einstellen, dass Sie darüber informiert werden, wenn eine Internetseite diese Bestandteile nutzen will.



Nachteil: Ihnen bekannte und vertrauenswürdige Internetseiten können eventuell nicht mehr richtig funktionieren (z.B. das Anmelden an bekannten Seiten, wie es bei kostenlosen Email-Internetseiten benötigt wird). Wenn ein Formular oder eine Anmeldung plötzlich nicht mehr funktioniert, ist Java wieder zu aktivieren.

Falls Sie den Browser Firefox verwenden, sind diese Einstellungen unter „Extras“ und „Einstellungen“ zu finden (siehe Bilder unten)



Hier finden Sie zahlreiche Einstellungsmöglichkeiten. Wir empfehlen, Websites das Installieren von Software nicht zu erlauben, sowie Java dann zu deaktivieren, wenn Sie auf Ihnen unbekanntem Seiten surfen. Benötigen Sie Java wieder für eine vertrauenswürdige Seite, ist Java mit ein paar Mausklicks schnell wieder aktiviert.

Firewalls

Den Begriff haben Sie sicher schon oft gehört, allerdings vielleicht weniger über den konkreten Nutzen oder die Funktionsweise (das Sperren von „Ports“).

Stellen Sie sich Ihre Internetverbindung als ein Seil vor. Ein Seil besteht aus mehreren Fasern. Während Sie surfen, wird eine bestimmte Faser dafür verwendet, wenn Sie eine E-Mail schicken, ebenso beim Hochladen von Dateien in das Internet, usw.

Eine Firewall sperrt unbenötigte „Fasern“ bzw. stellt sicher, dass nur von Ihnen erwünschte Programme diese verwenden. Diese „Fasern“ aus unserem Sinnbild entsprechen den „Ports“ im Fachjargon.

Mit Hilfe dieser Ports können sich Hacker Zugriff zu Ihrem Computer verschaffen und so Ihre Daten manipulieren oder mithören.

Bestimmte Programme wären in der Lage, Ihre Tastatureingaben auszulesen und so an Ihre Bankverbindungsdaten bei an sich „sicheren“ Verbindungen zu gelangen.

Das Installieren einer kostenlosen Firewall ist leicht. Das Konfigurieren einer solchen wird für nicht so Geübte eher kompliziert, da man einen Überblick haben sollte, welche Programme zulässig sind und welche nicht.

Windows-XP

Das gebräuchlichste Betriebssystem für neue PCs und somit schon weit verbreitet, da es bereits vorinstalliert ist. Dieses Betriebssystem verfügt über eine schon eingebaute Firewall, die jedoch in Einzelfällen zu deaktivieren ist (einige Provider in Österreich raten dazu, damit die Internetverbindung funktioniert).

Wenn Sie Windows XP verwenden und keine Probleme mit der Internetverbindung haben, können Sie diesen Punkt der Broschüre überspringen.

Wenn Sie kein Windows XP verwenden bzw. die eingebaute Firewall deaktivieren mussten, versuchen Sie es mit der Installation von kostenloser Software, die Sie vor Übergriffen aus dem Netz schützt.

Hier wieder nur ein Beispiel an empfehlenswerter Software:

ZoneAlarm

ist unter www.zonelabs.com auch als deutsche Version erhältlich. Eine kostenlose Firewall, die zuverlässig über Zugriffe auf Ihren PC informiert, mit einer übersichtlichen und einfach zu bedienenden Oberfläche, die jedem Benutzer ohne Firewall empfohlen werden kann.

Bei der Installation ist darauf zu achten, dass Sie dem Programm die richtige Verbindung (Modem oder ADSL) angeben, sowie das Programm im Zweifelsfall selbst entscheiden lassen, was gesperrt wird oder nicht. Weiters sollten Sie Benachrichtigungen über die Aktivität der Firewall deaktivieren, da Sie ansonsten bereits nach wenigen Minuten genervt wären. Dann würde sich nämlich alle paar Minuten ein Info-Fenster öffnen, das Sie darüber informiert, dass etwas abgewehrt wurde. Damit wird das Surfen im Netz zur Qual.

Abschließend eine Checkliste

Ist Anti-Virensoftware installiert bzw. auf dem neuesten Stand?

Ist mein Betriebssystem auf dem neuesten Stand?

Ist mein Browser auf dem neusten Stand?

Habe ich eine aktive Firewall?

Habe ich ein Anti-Malware Programm installiert bzw. auf dem neusten Stand?

Nachwort

Ist es möglich, einen PC anhand dieses Folders ganz sicher zu machen?

Leider nein. Eine hundertprozentige Sicherheit im Netz gibt es nicht!

Wenn Sie allerdings diesen kurzen Leitfaden befolgen, werden Sie zumindest ein gutes und relativ sicheres System konfiguriert haben und es Angreifern nicht so leicht machen, an Ihre Daten zu gelangen.

Bedenken Sie: auch Hacker sind nur Menschen. Ist ein System einigermaßen gesichert, ist es einem Hacker meist zu mühselig, diese Sicherungen zu umgehen. Es befinden sich ja noch tausende andere Personen im Netz, die sich nicht geschützt haben, warum sich also die Mühe mit Ihrem System machen?

Unter diesem Gesichtspunkt haben Sie bereits einen großen Schritt zur Sicherheit Ihres PCs gemacht.

Sie benötigen weitere Hilfe oder Informationen?

Haben Sie noch Fragen zu dieser Broschüre oder
rund um den PC, Hardware, Software oder
Internet?

Wenn ja, dann wenden Sie sich an:

Computerfachberatung der Konsumentenberatung der Arbeiterkammer Salzburg

Markus-Sittikusstraße 10
5020 Salzburg

Jeden Dienstag 16.00 bis 18.00 Uhr

Tel.: 0662-8687-103

Fax: 0662-8687-150

E-Mail: g.bogojevic@ak-sbg.at

Wir helfen Ihnen gerne weiter
Ihre AK





5020 Salzburg · Markus-Sittikus-Straße 10
© (0662) 86 87-0 · Fax: (0662) 87 62 58

Im Internet:

E-Mail: kontakt@ak-sbg.at

Homepage: www.ak-sbg.at