

Schützen Sie Ihren Rechner!

Viele Computer-Viren und Hacker-Angriffen richten nur deshalb Schaden an, weil Internetsurfer einfachste Sicherheitsregeln ignorieren. Lesen Sie unsere Tipps für den Rundum-Schutz.

Viren

Mehr als die Hälfte aller Computernutzer hatte schon mal ein Virus. Wenn sich Ihr PC plötzlich seltsam verhält, sollten Sie vor allem Ruhe bewahren. Voreiliges Löschen von Dateien oder Mail kann mehr Schaden anrichten als das Virus selbst. Am besten ist natürlich gute Vorsorge.

- Benutzen Sie immer ein Virenschutzprogramm. Empfehlenswert sind etwa: Norton AntiVirus, McAfee, GData und Kaspersky, die alle zwischen 40 und 99 Euro kosten. Stellen Sie es so ein, dass es schon beim Start des Rechners geladen wird und stets im Hintergrund aktiv ist.
- Laden Sie sich regelmäßig (mindestens einmal pro Woche) die neuesten Updates für Ihren Virenschutz aus dem Internet. Das geht meist einfach per Mausklick. Die Übertragung der Daten dauert nur wenige Minuten. Manche Hersteller informieren per E-Mail über wichtige Updates, andere Programme erinnern in regelmäßigen Abständen daran, den Virenschutz zu aktualisieren.
- Beachten Sie beim Einlegen alter oder unbekannter Disketten, dass diese Viren enthalten könnten. Gleiches gilt für fremde selbst gebrannte CDs.

Hacker-Angriffe

Nicht nur Firmenrechner, sondern auch Ihr privater PC kann Ziel von Attacken aus dem Internet sein. Kriminelle suchen etwa nach Passwörtern, mit denen sie auf Ihre Kosten surfen oder einkaufen können.

- Wenn Sie oft und lange im Netz unterwegs sind, brauchen Sie eine »Personal Firewall«. Diese Schutzsoftware blockt Angriffe aus dem Internet ab und schlägt bei Gefahr Alarm. Mit der Firewall können Sie auch Trojanische Pferde ausschalten - versteckte Programme, die Daten ausschnüffeln und übers Internet verschicken. In der neuesten Windows-Version »XP« sind Grundfunktionen einer Firewall zwar enthalten, aber nach Meinung von Experten nicht ausreichend. Dennoch: Falls Sie nichts anderes haben, aktivieren Sie den Firewall im Menüpunkt »Eigenschaften«. Besseren Schutz bieten allerdings spezielle Firewall-Programme wie »ZoneAlarm« (für Privatanwender kostenlos im Internet) oder Norton Internet Security. Letzteres verbindet Firewall und Virenschutz in einem - mehrere Hersteller bieten solche Komplett-Pakete.

Internetsurfen

Manchmal genügt ein falscher Mausklick oder eine freizügige Datenangabe im World Wide Web, um den eigenen PC zu gefährden. Einfache Verhaltensregeln machen das Surfen sicherer.

- Grundsätzlich gilt: Vorsicht vor dubiosen Webseiten! Seiten mit schmutzigen oder illegalen Inhalten, etwa Raubkopien, enthalten oft auch schädliche Dateien. Klicken Sie deshalb keine Links an, die Ihnen verdächtig vorkommen. In Schwierigkeiten geraten immer

wieder die »OK-Klicker«, die zu schnell zur nächsten Seite wollen. Lesen Sie, wohin der Link führt, bevor Sie darauf klicken.

- Laden Sie Software nur von vertrauenswürdigen Seiten herunter, zum Beispiel vom offiziellen Server des Herstellers.

- Peer-to-peer-Software wie Kazaa oder Gnutella ist beliebt, weil sie den Zugriff auf die Software- und Musiksammlung von anderen Internetnutzern ermöglicht. Doch oft sind dort virenverseuchte Dateien im Angebot. Checken Sie deshalb jede Datei mit einem Virenschutzprogramm, bevor Sie sie öffnen.

- Installieren Sie ein Dialer-Schutzprogramm. Hinter manchen Links, vor allem auf Erotik-Seiten, verbergen sich Miniprogramme, die nach dem Herunterladen und Ausführen die Internetverbindung trennen und sich über eine teure 0190-Nummer neu einwählen. Das geht schneller, als man denkt, und kann sehr teuer werden. Dialer-Schutz-Programme wie YAW 3.5 warnen, wenn eine andere als die gewohnte Verbindung aufgebaut wird.

- Machen Sie Ihren Browser sicherer. Wer vorsichtig ist, deaktiviert aktive Inhalte wie ActiveX, Java, JavaScript und Skript-Sprachen wie Visual Basic Script - auch wenn das zu Schwierigkeiten bei der Anzeige mancher Web-Seiten führen kann. Ist Ihnen solch eine Seite besonders wichtig, können Sie die Einstellungen kurzfristig wieder lockern. Im Internet-Explorer finden sich die Sicherheitseinstellungen unter »Internetoptionen« im Menü »Extras«. Dort gibt es eine Registerkarte »Sicherheit«, wo man den Button »Stufe anpassen« anklicken und eine Sicherheitsstufe zwischen »sehr niedrig« und »hoch« auswählen kann.

- Melden Sie sich immer ordentlich ab. Wenn Sie Web-Mail nutzen oder Ihre Bankgeschäfte über den Web-Browser abwickeln, sollten Sie nur so lange eingeloggt bleiben wie nötig. Haben Sie Ihre Mail gelesen oder Ihre Überweisung getätigt, klicken Sie auf den »Logout«- oder »Abmelden«-Knopf und schließen am besten noch das Browserfenster.

E-Mail

E-Mail-Würmer werden immer raffinierter und richten immer größere Schäden an - wie »Bugbear«. Gesundes Misstrauen ist die beste Vorsichtsmaßnahme.

- Löschen Sie E-Mails, die Ihnen merkwürdig vorkommen - bevor Sie sie lesen. Klicken Sie niemals angehängte Dateien an, von denen Sie nicht sicher sind, dass sie von einem vertrauenswürdigen Absender stammen. Besonders gefährlich sind ausführbare Programme mit den Endungen .com, .exe, .vbs und .bat und Office-Dateien, die auf .doc, .xls und .ppt enden. Bildschirmschoner sind ebenfalls riskant (.scr).

- Vorsicht auch bei scheinbar bekannten Absendern. Manche Mail-Würmer kapern das Adressbuch des Infizierten und schicken unter seinem Namen Mails an alle gespeicherten Adressen.

- Wählen Sie einen Mail-Anbieter, der eingehende Post nach Viren scannt. Bei Web.de kann man beispielsweise jeden Anhang markieren und die Schaltfläche »Anlage auf Viren prüfen« anklicken.

- Wer ganz sicher sein will, sollte den Versand von Dateianhängen vorher telefonisch abstimmen. Nur dann ist zweifelsfrei gewährleistet, dass die Datei vom angegebenen Absender stammt.

- Schützen Sie sich vor Makroviren, indem Sie Ihr Textverarbeitungsprogramm konfigurieren. Beispiel für Microsoft Word: Klicken Sie im Menü »Extras« auf »Optionen«, dort dann auf die Registerkarte »Sicherheit«. Klicken Sie dann auf »Makro Sicherheit«. Stellen Sie die Sicherheitsstufe auf »hoch«.

Betriebssystem

Viele Computerviren nutzen Sicherheitslücken des PC-Betriebssystems aus - Windows ist das meist verbreitete. Wird so ein Fehler einmal erkannt, dauert es oft nur Stunden, bis es im Internet ein Zusatzprogramm gibt, womit er beseitigt werden kann. Das können Sie nutzen.

- Halten Sie Windows immer auf dem neuesten Stand. Dazu gibt es unter dem »Start«-Knopf» oder im Internet-Explorer unter »Extras« eigens einen Menüpunkt »Windows Update«. Der verbindet Sie mit der Internetadresse <http://windowsupdate.microsoft.com/>. Dort auf »Produktupdates suchen« klicken. Daraufhin fahndet das System selbstständig nach Neuerungen und bieten Ihnen deren Installation an. Installieren Sie auf jeden Fall alle »Service Packs« und »Sicherheitsupdates«. Das Herunterladen kann einige Zeit in Anspruch nehmen, ist aber jede Minute wert.

- Andere Betriebssysteme wie MacOS oder Linux sind für Angriffe deutlich weniger anfällig als Windows. Das liegt zum einen an ihrer geringen Verbreitung: Einen Virus zu schreiben für die wenigen Nutzer dieser Betriebssysteme »lohnt« sich kaum. Zum anderen ist bei Linux/Unix-Systemen schon die Struktur des Systems virenfeindlich: Änderungen von Kernfunktionen des Systems können erst nach der Eingabe eines besonderen Passwortes vorgenommen werden.

Passwörter

Immer wieder berichten Hacker, dass leicht zu knackende Passwörter ihnen den Angriff besonders einfach machen. Wer sein Mailpostfach oder sein Online-Konto schützen will, sollte kreativ sein.

- Behalten Sie Ihr Passwort für sich. Seriöse Anbieter fragen niemals nach dem Passwort - weder per Mail noch am Telefon.

- Ändern Sie Ihre Passwörter regelmäßig. Benutzen Sie für verschiedene Anwendungen auch verschiedene Passwörter, nicht einen »Generalschlüssel«.

- Wählen Sie möglichst außergewöhnliche Passwörter. Oft probieren Passwort-Knack-Programme einfach alles durch, was im Duden steht, und dazu noch Filmtitel, Prominentennamen und Automarken. Suchen Sie also möglichst eine Buchstabenkombination aus, die in der gesprochenen Sprache nicht vorkommt. Buchstabieren Sie zum Beispiel ein leicht zu merkendes Wort rückwärts. Passwörter sollten auf keinen Fall zu kurz sein, denn je kürzer sie sind, desto leichter sind sie zu knacken.

- Besonders schwer zu knacken sind Kombinationen aus Buchstaben und Ziffern, zum Beispiel K3S2T9H7.

- Speichern Sie Passwörter nicht auf Ihrer Festplatte. Dort könnten Sie auch übers Netz ausspioniert werden.

Sicherheitskopien

Für den Fall, dass alle Sicherheitsvorkehrungen doch nicht reichen und Sie Ihre Daten verlieren, sollten Sie immer Backups, also Sicherheitskopien anlegen.

- Speichern Sie wichtige Dateien regelmäßig auf einen separaten Datenträger. Dokumente, Mail und das Adressbuch passen oft schon auf eine Diskette - für Fotos, Musik und Filme eignen sich selbst gebrannte CDs oder DVDs.

- Prüfen Sie, ob Ihre Daten auch wirklich fehlerfrei auf dem Speichermedium angekommen sind.

Freeware, die den Rechner schützt

- > [Anti-Viren-Programm: H+B EDV AntiVir Personal Ed.](#)
- > [Personal Firewall: ZoneAlarm](#)
- > [Schutz vor 0190-Dialern: YAW 3.5](#)
- > [Verschlüsselung: Pretty Good Privacy](#)

Auch Computernutzer mit leerem Geldbeutel müssen ihren PC nicht ungeschützt seinem Schicksal überlassen. Im Internet gibt es leistungsfähige Programme, die nichts kosten. Auch ein Null-Euro-Schutz ist besser als keiner.

Die deutsche Datenschutzfirma H+B EDV stellt für den privaten Einsatz mit **AntiVir** ein kostenloses Anti-Viren-Werkzeug zur Verfügung, das in der Erkennungsrate den kommerziellen Programmen in nichts nachsteht.

[Download beim Hersteller](#)

Dank der einfachen und klar aufgebauten Oberfläche können Einsteiger schon nach wenigen Minuten ihren ersten Scan starten und Viren den Garaus machen. Außerdem bietet das Programm einen »Schutzschild«, der möglicherweise eintreffende Mails bereits auf Disketten oder in E-Mails erkennt.

Eine integrierte Update-Funktion holt sich automatisch die neueste Virendefinition auf den Rechner und stellt so zu jeder Zeit ein Höchstmaß an Sicherheit her – Kosten entstehen dabei nicht. Störend ist lediglich, dass das Programm praktisch jedes Mal, wenn die Definitionsdatei aktualisiert werden soll, auch gleich eine neue Version des Hauptprogramms herunterladen will. Das sind dann jedes Mal 3,5 MB an Daten.

ZoneAlarm ist eine so genannte Firewall – eine Software, mit der Sie ein- und ausgehende Daten kontrollieren und gegebenenfalls sperren können. Die Konfiguration ist sehr einfach, das Programm ist schon direkt nach der Installation einsatzbereit, ohne dass der Nutzer weitere Einstellungen vornehmen muss. ZoneAlarm wird mit dem Windows-Start automatisch geladen.

Versucht ein anderes Programm Verbindung mit dem Internet aufzunehmen, meldet sich Zone-Alarm mit der Frage, ob Sie den Zugriff auf das Web erlauben wollen. Während Sie E-Mail-Programmen und Internet-Browsern den Zugang immer erlauben sollten, sollten Sie zum Beispiel dem Media Player eine Verbindung strikt zu untersagen.

Zugriffe aus dem Web auf Ihren PC blockiert ZoneAlarm zuverlässig ab. Wenn eine Website ein Cookie auf dem Rechner ablegen will, kann der User entscheiden, ob er dies verweigern oder zulassen will.

[Download beim Hersteller](#)

Die Freeware **Yet Another Warner** (YAW) schützt vor 0190-Dialern, die sich automatisch in das DFÜ-Netzwerk installieren.

Wird eine DFÜ-Verbindung aufgenommen, fragt das Programm gesondert nach und löscht automatisch den Eintrag, falls der Nutzer nicht einverstanden ist.

Nach einem einmaligen Scan-Vorgang, bei dem der Rechner nach Dialern durchsucht wird, besteht die Möglichkeit, verdächtige Einträge zu löschen oder zu isolieren.

Das Programm ist im Prinzip kostenlos, bittet aber recht nachdrücklich um Registrierung, die mit Kosten von 1 Euro (oder - wer will - mehr) verbunden ist.

[Download beim Hersteller](#)

E-Mails sind im Grunde genauso unsicher wie Postkarten – wer eine abfängt, kann sie auch lesen. Deshalb ist es wichtig, Mails mit sensiblen Inhalten wirksam zu verschlüsseln. **Pretty Good Privacy** (PGP) hat sich hier als Standard etabliert.

Das Verfahren, mit dem PGP arbeitet, ist nicht ganz einfach: Jeder Anwender generiert zunächst ein so genanntes Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht. Den öffentlichen Schlüssel verschickt er an jeden, von dem er E-Mails empfängt, der private liegt auf seinem PC und darf niemals veröffentlicht werden.

Gleiches macht der Mailpartner: Auch er verschickt an alle seinen öffentlichen Schlüssel. Der Nutzer schreibt seine Mails nun ganz normal in seinem E-Mail-Programm, wählt den öffentlichen Schlüssel des Empfängers aus und klickt dann auf »encrypt«. Geht die Mail beim Empfänger ein, kann nur dieser die Mail mit seinem privaten Schlüssel öffnen und lesen.

[Download beim Hersteller](#)