# VORBEUGEN IST BESSER ALS HEILEN
# Die zehn Gebote des Virenschutzes

## 1. Zwei Anti-Viren-Programme sind besser als eines

Der Einsatz von **Anti-Viren-Software sollte selbstverständlich sein**, wenn der Computer mit dem Internet verbunden ist oder häufig über externe Medien gespeist wird. Anti-Viren-Programme haben eine **Suchfunktion**, mit der sie die gesamte Festplatte nach bekannten Viren durchsuchen. Viele der Programme können gefundene Viren auch eliminieren, ohne die befallene Datei zu zerstören. Eine Übersicht über die **Leistungsfähigkeit der verschiedenen Programme** finden Sie in unserem Test.

Da nicht jede Software alle Viren findet, bietet es sich bei besonders gefährdeten Computern durchaus an, zwei unterschiedliche Programme auf die Jagd zu schicken. Einige Hersteller bieten **auch kostenlose Programme für den privaten Gebrauch** an, so dass diese Sicherheitsmaßnahme Ihren Geldbeutel nicht extra belastet.

## 2. Machen Sie regelmäßig Updates

Das beste Anti-Viren-Programm ist nutzlos, wenn die Virendaten nicht aktuell sind. Täglich tauchen neue Viren auf, gegen die veraltete Software hilflos ist. Die meisten Antiviren-Programme bieten inzwischen die **Möglichkeit automatischer Updates**. Wo Sie die aktuellsten Updates manuell herunterladen können, sehen Sie in unserer Übersicht.

## 3. Verwenden Sie Ihre Anti-Viren-Software

Auf vielen Rechnern ist Antiviren-Software installiert, die aber nicht benutzt wird. Die meisten Programme bieten ein **Wächter-Modul**, das bei jedem Start des Computers geladen wird und automatisch nach Viren Ausschau hält. Wenn Sie diese Funktion nicht aktivieren wollen, sollten Sie **immer einen manuellen Viren-Check durchführen, bevor** Sie fremde Disketten oder CDs öffnen, Dateien aus dem Internet herunterladen oder Attachements von E-Mails öffnen.

## 4. Seien Sie misstrauisch bei Mailanhängen

Moderne Würmer und Viren verbreiten sich per E-Mail. Dabei verwenden sie das Adressbuch und die Absenderadresse des befallenen Computers. So können Sie von einem Bekannten **ohne sein Wissen** einen Virus zugeschickt bekommen. Ein Beispiel dafür war der „I-love-you-Virus“ im Mai 2000, der sich selbst an alle E-Mail-Adressen im Outlook-Adressbuch eines befallenen Rechners verschickte.

**Unangekündigte Attachements in E-Mails sollten Sie nie öffnen**, besonders wenn Ihnen der Titel ungewöhnlich vorkommt. Fragen Sie den Absender vorsichtshalber, ob das Attachement tatsächlich von ihm stammt. Im Zweifelsfalle geht Sicherheit vor Neugierde. Besondere Vorsicht ist angebracht bei **Anhängen, die folgende Extensionen aufweisen**: .exe, .vbs, .js, .hta, .pif, .com, .scr, .bat und .shs.

Wenn Sie Attachements direkt öffnen, sollten Sie einen Virenwächter installiert haben. Die Alternative: Sie speichern den Anhang zunächst auf der Festplatte und lassen ihn dort vor dem Öffnen von einem Viren-Scanner begutachten.

## 5. Seien Sie vorsichtig bei Downloads

Wenn Sie Programme aus dem Internet herunterladen oder aus Newsgroups beziehen, lassen Sie besondere Vorsicht walten. Vergewissern Sie sich vor dem Download, ob die Quelle vertrauenswürdig ist. Bevor sie **neue Software aus dem Internet** ausprobieren, sollten Sie in jedem Fall einen **aktualisierten Virenscanner** einsetzen!

## 6. Erhöhen Sie die Sicherheit mit Desktop-Firewalls

Desktop-Firewalls können zwar nicht vor der Vireninfektion schützen, sie können aber den **Schaden verringern**, den ein Virus oder Trojaner anrichten kann. Eine Firewall verhindert, dass der Virus oder Trojaner selbstständig eine Internetverbindung herstellt, um sich weiter zu verbreiten oder gestohlene Daten an einen Hacker zu übermitteln.

Einige Firewalls bieten auch die Möglichkeit eine so genannte **Sandbox einzurichten**: Wird ein Virus aktiv, kann er diese virtuelle Sandkiste nicht verlassen und so am abgeschotteten Computer keinen Schaden anrichten.

Wie Firewalls genau funktionieren lesen Sie in unserem Hintergrundartikel.

## 7. Schützen Sie Ihren PC mit einem Passwort

Wenn Ihr Computer auch anderen Menschen zugänglich ist, sollten Sie ihn mit einem Passwort versehen. So können Sie verhindern, dass sich in Ihrer Abwesenheit ein Virus in ihr System verirrt, etwa weil Kollegen keine so hohen Anforderungen an die Sicherheit stellen wie Sie. Die meisten Computer bieten die Möglichkeit, **im BIOS ein Passwort einzutragen**, das vor dem Starten des Rechners abgefragt wird.

Dazu müssen Sie beim **Booten des Computers** die Taste F2 oder ENTF drücken (hängt vom Hersteller des BIOS ihres Computers ab). Im Menüpunkt „Security“ oder „Password Setting“ können Sie dann ein Passwort einstellen. Aber Achtung: Verändern Sie im BIOS keine Einstellungen, deren Auswirkung Sie nicht kennen. Falsche Werte können die Systemleistung beeinträchtigen und im schlimmsten Fall dafür sorgen, dass Ihr Computer nicht mehr starten kann!

Wenn Sie Ihren Arbeitsplatz nur kurz verlassen, verwenden Sie einen **Bildschirmschoner mit einem Passwort**. Er lässt sich dann nur mit dem Zauberwort wieder ausschalten und sperrt den Computer so vor fremdem Zugriff.

Die Wirkung bleibt natürlich aus, wenn Sie das Passwort auf einem gelben Zettel auf den Monitor kleben. Aber **auch im Rechner sollten Sie keine Passwörter, Kreditkartennummern und Kontonummern speichern**, da sie von Hackern mit Trojanischen Pferden oder Backdoors leicht gestohlen werden können. Zum **richtigen Umgang mit Passwörtern** lesen Sie auch unseren Hintergrundartikel: Sicherheitslücke Passwort

## 8. Sichern Sie Ihre Daten regelmäßig

Trotz bester Vorsorge kann es zu einer unbemerkten Virenattacke kommen. Um den Schaden dann möglichst gering zu halten, sollten Sie **regelmäßige Backups** Ihrer Festplatte machen. Wichtige Daten sichern Sie möglichst täglich auf externen Speichermedien wie Disketten oder CDs. So ist im Fall des Falles höchstens die Arbeit eines Tages verschwunden.

## 9. Erstellen Sie rechtzeitig eine Startdiskette

Windows bietet die Möglichkeit, eine Startdiskette zu erstellen, die den Computer auch hochfährt, wenn dazu benötigte Dateien auf der Festplatte zerstört oder gelöscht worden sind: Im **Windows-Menü Start** – Einstellungen – Systemsteuerung – Software klicken Sie auf die Registerkarte „Startdiskette“.

Auch manche Virenprogramme können solche Startdisketten erstellen, mit denen es nach einem virenbedingten Absturz möglich ist, **erste Reparaturen am System** vorzunehmen.

## 10. Bei Virenbefall: Keine Panik!

Wenn Ihnen während der Arbeit am PC auffällt, dass er sehr langsam arbeitet oder häufig abstürzt, sollten Sie hellhörig werden und einen Virenscanner einsetzen. Stellt das Programm Viren auf Ihrem Rechner fest, gilt als oberstes Gebot: **Ruhig bleiben** und nicht in Panik verfallen. Sonst könnten Sie selbst größeren Schaden anrichten als der Virus.

# SOFTWAREOPTIONEN NUTZEN
# Die richtigen Einstellungen zum Schutz gegen Viren

**M**it den zehn Geboten des Virenschutzes sind Sie quasi auf der sicheren Seite. Zusätzlich gibt es aber noch **spezielle Software-Einstellungen zum Schutz** gegen Boot-, Skript- und Makroviren.

## 1. Bootviren

Bootviren verbergen sich gerne auf vermeintlich leeren Disketten. Steckt eine **verseuchte Diskette beim Rechnerstart (Booten) im Laufwerk, dann wird der Virus aktiviert**. Mit der richtigen Einstellung des Basic Input-Output-Systems (BIOS) können sie diese Gefahr mindern. Sie ändern die Reihenfolge der Laufwerke, auf denen der Computer ein Betriebssystem beim Starten suchen soll.

Die Standardeinstellung lautet oft „A:, C:". Es wird also zunächst versucht, das Betriebssystem auf einer Diskette zu finden, bevor auf die Festplatte zugegriffen wird. **Ändert man diese Einstellung auf „C:, A:"** können auch versehentlich im Laufwerk befindliche, infizierte Disketten keinen Schaden mehr anrichten.

Leider gibt es **Viren, die diese Funktion austricksen**. Einen hundertprozentigen Schutz bieten somit nur mechanische Einstellungen: Manche Computer-Mainboards ermöglichen es, das BIOS per Schalter in einen schreibgeschützten Zustand zu versetzen.

## 2. Skriptviren

Der „I-love-you"-Virus war der erste berühmte Vertreter der Gattung. Dieser Virus konnte sich erst durch eine neue Funktion im Betriebssystem Windows 98 so rasant verbreiten: den **Windows-Skripting-Host (WSH)** . Er stellt eine Skriptsprache zur Verfügung, mit der **Standardabläufe automatisiert** werden können. Die meisten Benutzer benötigen diese Funktion nicht. Trotzdem gehört der WSH zur Standard-Installation von Windows.

Wenn Sie **keine eigenen Skripts** verwenden, sollten Sie **den WSH deinstallieren**: Klicken Sie im Menü „Start" – „Einstellungen" – „Systemsteuerung" – „Software" auf die Registerkarte „Windows Setup". Wählen Sie „Zubehör" aus und klicken Sie auf den Button „Details". Sollte in dem Auswahlkästchen vor „Windows-Skripting-Host" ein Haken sein, entfernen Sie diesen und klicken auf OK.

Wer sich gegen **unangenehme Überraschungen beim Surfen** absichern möchte, sollte **in seinem Browser** einige Einstellungen vornehmen. Auf Nummer sicher gehen Sie, wenn Sie alle **Skripting-Funktionen** (z. B. Active-X oder Javascript) abschalten. Leider geht das zu Lasten der Funktionalität – besonders bei Webseiten, die solche Skripte für die Navigation nutzen. Hier gilt es, das richtige Gleichgewicht zwischen Sicherheit, Komfort und Funktionalität zu schaffen.

Im **Internet Explorer** finden sich die entsprechenden Einstellungen
unter „Extra" – „Internetoptionen" – auf der Registerkarte „Sicherheit".

Im **Netscape Navigator** (4.73) finden sich die Einstellungen im Menü „Communicator" unter dem Punkt „Extras" – „Sicherheitsinformationen".

**Besser als diese Browser-Einstellungen sind Desktop-Firewalls**: Sie bieten hohe Sicherheit bei uneingeschränkter Funktionalität. Eine Investition, die sich lohnt.

## 3. Makroviren

Makros sollen den Umgang mit Microsoft-Office-Programmen erleichtern. Sie ermöglichen es, häufig ausgeführte Arbeitsschritte aufzuzeichnen und unter einer Tastenkombination abzuspeichern. Diese Funktion kann aber auch zur Entwicklung von Viren genutzt werden. Die Programmiersprache für solche Makros nennt sich Word-Basic und bietet viele Möglichkeiten, auf Systemressourcen zuzugreifen. **Das macht Makroviren so gefährlich**.

Zur Verbreitung brauchen Makroviren **Office-Dokumente oder deren Formatvorlagen**. Diese haben beispielsweise die Dateikürzel .doc, .xls oder .dot. Wenn Sie solche Dateien über das Internet erhalten, sollten Sie immer besonders skeptisch sein: Sie können infiziert sein.

Wenn Sie dennoch **Dokumente mit Makros öffnen, so halten Sie dabei die SHIFT-Taste gedrückt**. Die Ausführung von Auto-Makros wird dadurch unterbunden. Schon **vorhandene Makros** sollten Sie unter dem Menüpunkt „Extras“ – „Makro“ **inhaltlich überprüfen**.

Bei den neueren Microsoft Office Versionen können Sie **Sicherheitseinstellungen für Makros** vornehmen. Sie sollten diese nach Ihren Bedürfnissen konfigurieren. Sie finden sie bei Office 2000 unter dem Menüpunkt „Extras“ – „Makro“ – „Sicherheit“. Office 97 bietet diese Möglichkeit unter „Extras“ – „Optionen“ – „Allgemein“.

Es **gibt allerdings Viren, die in der Lage sind, diese Einstellungen zu umgehen oder zurückzusetzen**. Auch hier gilt also: Nur der **regelmäßige Check** mit einem Anti-Virenprogramm gibt Ihnen echte Sicherheit.

Auch **gegen Virenbefall von Dokumentvorlagen können Sie Vorsichtsmaßnahmen ergreifen**. Dokument- oder Formatvorlagen sind in Microsoft Word eine Art Musterseiten, die Texte und Formatvoreinstellungen enthalten und in Dateien **mit der Erweiterung „.dot“ gespeichert** werden. Diese Dokumentvorlagen, wie zum Beispiel die weiße Musterseite „Normal.dot“, sollten Sie **als schreibgeschützt definieren**. So können sie nicht mehr als Infektionsherd dienen.

Wählen Sie in Word die Menüpunkte „Datei“ und „Neu“. Hier klicken Sie dann mit der **rechten Maustaste** auf die gewünschte Datei (z.B. „Leeres Dokument") und wählen „Eigenschaften“ aus. Setzen Sie ein Häkchen hinter „**schreibgeschützt**“.

**Alternativ** können Sie bei Word eine **Funktion aktivieren**, die Sie **für Änderungen an der Dokumentvorlage um Ihre Zustimmung bittet**. Unter „Extras“ – „Optionen“ – „Speichern“ wählen Sie den Punkt „Automatische Anfrage für Speicherung von Normal.dot“. So behalten Sie Ihre Dokumentvorlage im Auge.

Noch ein Punkt: **Speichern Sie Dokumente unbekannter Herkunft nicht direkt**, sondern kopieren Sie den Inhalt zunächst in ein leeres Dokument und speichern dieses dann. Sie können so die Makros abstreifen. Wenn Sie das Rich-Text-Format (.rtf) für Word-Dokumente verwenden, werden keine Makros mit abgespeichert. So verhindern Sie die Verbreitung.

In Ihrem Internetbrowser gibt es die Möglichkeit, Standardprogramme zur Betrachtung bestimmter Dateiformate zu definieren. **Für das .doc-Format sollte ein Wordviewer, anstelle von Word eingetragen werden**. Für die anderen Produkte der Microsoft-Office-Reihe stehen solche Viewer ebenfalls zur Verfügung. Sie werden unter http://www.microsoft.com/germany/office/Office/viewers.htm zum Download angeboten.

### 4. Gefährliche Ausnahme: Windows 98 und Outlook

Im Normalfall können E-Mail-Viren nur beim Öffnen des Attachements aktiv werden. Von dieser Regel gibt es leider eine Ausnahme. Im Zusammenspiel von Windows 98 und Outlook kann es unter Umständen zu einem **automatischen Öffnen des Attachements** kommen.

**In Outlook** sollten Sie daher unter „Extras“ – „Optionen“ die Registerkarte „Sicherheit“ auswählen und nach einem Klick auf den Button „Anlagensicherheit“ die **Einstellung „hoch„** aktivieren.

Microsoft bietet ein Sicherheitsupdate für Outlook 98 und Outlook 2000 an. Das Update hat im Wesentlichen drei Funktionen:
- Es verhindert den Zugriff auf gefährdete Dateitypen, die per E-Mail eingegangen sind.
- Es informiert den Benutzer mit einer Dialogbox, wenn ein externes Programm auf das Outlook-Adressbuch zugreifen will.
- Es verändert die Standardeinstellung von der Sicherheitsstufe „Internet“ auf „eingeschränkte Sites“.

*Alle Informationen aus:*
*www.focus.de, PC und Multimedia, Thema: Virenschutz*