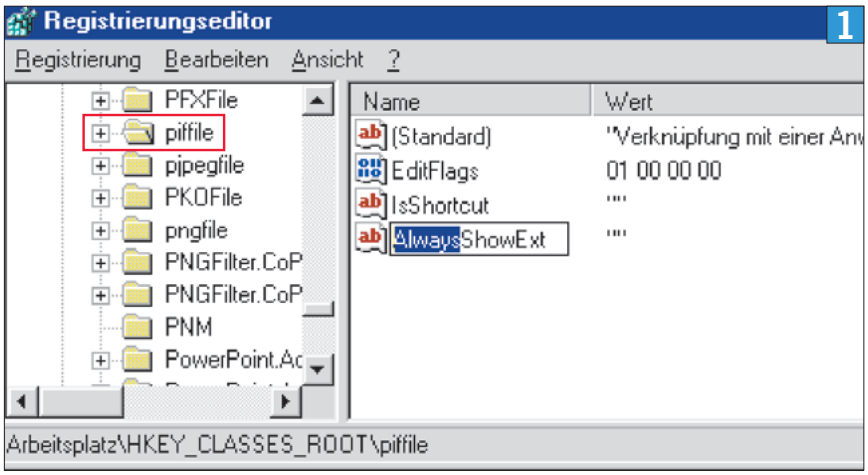
Trügerische Beilagen

Manchmal sind es nicht die Virenschreiber, die einen PC mit einem Wurm infizieren, sondern sogar die Benutzer selbst.



Bei «piffile» und «ShellScrap» soll Windows die Endungen immer anzeigen

von Gaby Salvisberg

Ein per Windows-Update vollständig aktualisiertes Outlook Express blockiert «potenziell gefährliche» Mailbeilagen standardmässig – der Benutzer kann sie weder öffnen noch speichern. Damit versucht Microsoft, die Benutzer vor sich selbst zu schützen. Wem diese Sperre zu viel an Bevormundung ist, kann sie aufheben (siehe «Einfach und sicher », S. 20).

Tun Sie dies nicht, ohne sich anderweitig abzusichern. Bis Sie sich vom Gegenteil überzeugt haben, sind alle Mailbeilagen verdächtig, egal wie vertrauenswürdig Ihnen der Absender vorkommt. Die grösste Gefahr steckt in den Dateiendungen: Nach wie vor zeigt Windows nicht alle an. So wissen Sie nie genau, ob eine Beilage nun wirklich «Familienfoto.jpg» heisst oder ob es sich um «Familienfoto.jpg.shs» handelt – und somit schädlicher SHS-Programmcode und gar kein Bild ist.

Dateiendungen zum Ersten: Öffnen Sie ein Windows-Explorer-Fenster und gehen Sie darin zu EXTRAS/ORDNEROPTIONEN/ANSICHT (Windows 98: ANSICHT/ORDNEROPTIONEN/ANSICHT). Entfernen Sie das Häkchen bei «Dateinamenerweiterung bei bekannten Dateitypen ausblenden» und bei «Geschützte Systemdateien ausblenden». Aktivieren Sie zudem «Alle Dateien und Ordner anzeigen». Unter Windows 98 und 2000 klicken Sie auf ÜBERNEHMEN und auf WIE AKTUELLER ORDNER. Unter Windows XP klicken Sie auf FÜR ALLE ÜBERNEHMEN.

Zwei verdächtige Dateien, einmal mit ausgeblendeten Dateiendungen (oben) und einmal mit allen Dateiendungen (unten)

Dateiendungen zum Zweiten: Um auch die Endungen der von Würmern häufig verwendeten Dateitypen PIF und SHS anzuzeigen, starten Sie den Registry-Editor: *Ctrl+R* eingeben, «regedit» eintippen, *Enter*. Veränderungen in der Registry sind heikel, seien Sie vorsichtig. Navigieren Sie zum Registry-Zweig *HKEY_CLASSES_ROOT/piffile* und klicken Sie ihn an. In der rechten Fensterhälfte klicken Sie mit Rechts auf «NeverShowExt», wählen UMBENENNEN und ändern den Namen des Eintrags auf «AlwaysShowExt», Screen 1. Tun Sie dasselbe auch im Zweig *HKEY_CLASSES_ROOT/ShellScrap*. Künftig sehen Sie die Endungen, Screen 2.

Löschen statt klicken: Mails mit Beilagen von unbekannten Absendern löschen Sie am besten sofort. Seien Sie sich auch stets bewusst, dass Absenderadressen gefälscht sein können. Fallen Sie nicht auf Mails herein, in denen behauptet wird, mit der angehängten Datei lasse sich ein Virus entfernen oder ein System-Update installieren. Dateien mit Endungen wie EXE, COM, BAT, PIF, SHS, VBS, WSH sollten bei Ihnen die Alarmglocke läuten lassen, sogar wenn sie innerhalb einer ZIP-Datei ankommen. Seien Sie auch mit in Mails erwähnten Links vorsichtig: Es gibt Würmer, die sich zu installieren versuchen, sobald Sie den Internetlink im Mailtext anklicken.

Scannen statt öffnen: Solange Sie eine Datei nicht öffnen bzw. ausführen, kann sie Ihrem PC nichts anhaben. Sollten Sie eine Beilage erwartet haben, öffnen Sie diese nicht direkt. Speichern Sie sie stattdessen zuerst via SPEICHERN UNTER oder ANLAGE SPEICHERN aus dem Mailprogramm heraus auf Ihre Festplatte. Über einen Rechtsklick und EIGENSCHAFTEN erfahren Sie mehr über die Datei, etwa deren genaueren Dateityp oder Grösse. Aktualisieren Sie nun Ihren Virenscanner und unterziehen Sie die Datei einer Prüfung: Das geht meist ganz leicht per Rechtsklick, weil die meisten Virenscanner im Kontextmenü einen Eintrag erstellen. Holen Sie im Zweifelsfall eine zweite Meinung über die Datei ein, indem Sie sie beispielsweise vom Kaspersky-Online-Scanner prüfen lassen (www.kaspersky.com/de/scanforvirus.html).

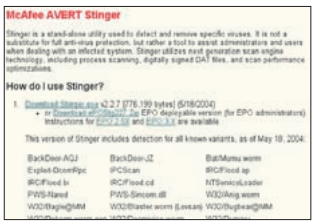
Nur weil zwei verschiedene Virenscanner nichts Ungewöhnliches in der Datei finden, muss sie deswegen noch lange nicht harmlos sein. Warten Sie bei dubiosen Dateien mindestens 24 Stunden, aktualisieren Sie den Virenscanner erneut und prüfen Sie die Datei anschliessend nochmals. Falls es ein neuer Schädling sein sollte, ist die Chance jetzt wesentlich grösser, dass Ihr Virenscanner ihn inzwischen erkennt. ■

MINITIPP VIREN ENTFERNEN

Medizin vom Virendoktor

Manchmal passiert es eben doch, dass ein PC mit einem Virus oder Wurm angesteckt wird. Vielleicht haben Sie eine Datei geöffnet, von der Sie gedacht haben, Sie hätten sie bereits gescannt. Passiert ist passiert! Doch wie werden Sie den Schädling wieder los?

Der Antiviren-Hersteller McAfee stellt ein kostenloses Programm namens Stinger zur Verfügung, das beim Entfernen von rund 40 verschiedenen, weit verbreiteten Würmern hilft. Welche das sind, lesen Sie auf der Stinger-Downloadseite http://vil.nai.com/vil/stinger. *(sal)*



Holen Sie sich das Antiviren-Tool