
ILLUSTRATION TOM HÜBSCHER, TNT-GRAPHICS

# Tipps gegen den Virenkater

**Fallen Sie nicht auf perfide Tricks von Computerschädlingen rein. Wir zeigen, wie Sie Ihren PC schützen können.**

von Gaby Salvisberg

Damit hätten Sie nie gerechnet: Ausgerechnet Onkel Ruedi schickt Ihnen einen Virus. Und warum sich zwei Wochen ohne Update der Viren-Software so schwerwiegend auswirken, ist Ihnen schleierhaft. Schliesslich kamen Sie gerade erst von den Skiferien zurück und wollten das mit den Updates gleich nach dem Lesen der Mails nachholen. Und überhaupt: Sie hätten gar nicht erkennen können, dass ausgerechnet in Onkel Ruedis Mail ein Virus steckt.

Wir sagen: Doch, Sie hätten! Viele Benutzer hadern nach einem Virenbefall mit ihrem Schicksal. Katzenjammer hilft jedoch genauso wenig wie die Wut auf Microsoft oder den Rest der Welt.

Der Schutz vor dem Virenkater ist nicht damit erledigt, einmal Sicherheits-Software zu installieren. In diesem Artikel fassen wir für Sie zusammen, wie Sie den PC absichern und in welchen PCtipp-Ausgaben Sie weiterführende Anleitungen dazu finden. Jeder Artikel steht für Sie in unserem Archiv als PDF-Datei bereit; Sie brauchen auf www.pctipp.ch nur oben rechts den Webcode einzutippen. Ferner erfahren Sie, wie Sie durch cleveres Verhalten fast jedem Schädling zuvorkommen (ab S. 31) und auf welche frechen Lügen Sie in den Wurmmails treffen (ab S. 33). In den Kästchen «Irrtum!» entlarven wir ein paar klassische Fehleinschätzungen, die für Ihren PC fatale Folgen haben können.

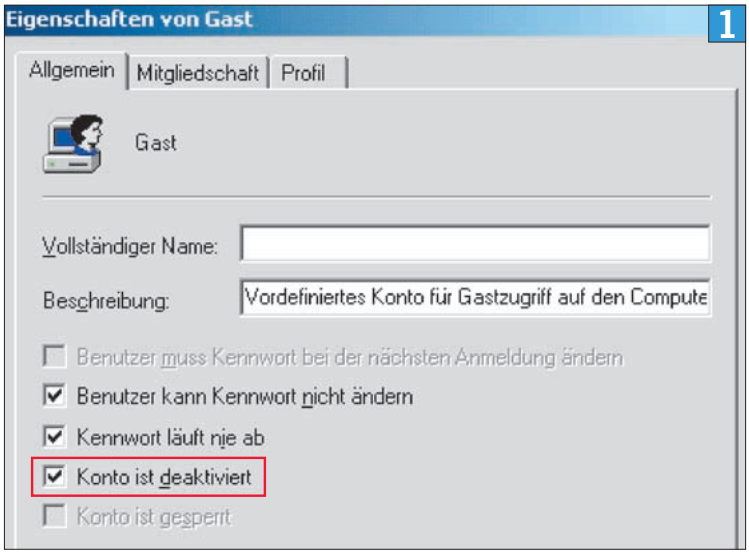
## So sichern Sie den PC ab

**Router für Breitband:** Surfen Sie über einen Breitband-Anschluss wie ADSL oder TV-Kabel? Dann verwenden Sie am besten einen Router. Dieser stellt eine erste Verteidigungslinie gegen Würmer wie z. B. Blaster dar. Eine ausführliche Kaufberatung zu diesem Thema finden Sie im PCtipp 3/2004, S. 68, «Sicherer Kasten», WEBCODE pdf040368.

**Updates von Windows und Virenscanner:** Microsoft veröffentlicht mindestens einmal im Monat Sicherheits-Updates. Diese zu installieren, ist ein Leichtes: Sie finden einen Link zu WINDOWS UPDATE sowohl im STARTMENÜ als auch im Internet Explorer im Menü EXTRAS. Auf der Update-Seite angelangt, verwenden Sie den Link UPDATES SUCHEN. Für die Sicherheit relevant ist alles, was unter «Wichtige Updates» erscheint. Klicken Sie nun zuerst auf UPDATES ÜBERPRÜFEN UND INSTALLIEREN und anschliessend auf JETZT INSTALLIEREN. Wenn Sie dies regelmässig tun, sind die neuen Update-Happen schnell installiert.

Ein Virenscanner hingegen braucht tägliche Updates, um überhaupt seinen Job erfüllen zu können. Wenn Sie nach einer längeren Abwesenheit (z. B. Ferien, Militärdienst etc.) den PC erstmals wieder einschalten, kümmern Sie sich am besten zuerst um die Updates von Windows und Virenscanner – und lesen erst anschliessend die neuen Mails.

Die meisten installierbaren Virenscanner holen sich ihre Updates automatisch. Prüfen Sie auf jeden Fall, ob diese Option bei Ihnen eingeschaltet ist. Wie das geht, erfahren Sie im Handbuch Ihres Virenscanners.




**Solche Gäste wollen Sie nicht: Gastkonto deaktivieren**

**Firewall:** Auch wenn Desktop-Firewalls nicht der Weisheit letzter Schluss sind, können sie Ihnen doch einigen Ärger ersparen. Wie Sie die Internetverbindungsfirewall von Windows XP einschalten, lesen Sie auf Seite 79. Zu diesem Thema erfahren Sie mehr unter WEBCODE **pdf040258**.

Haben Sie eine andere Windows-Version, installieren Sie eine Desktop-Firewall wie z. B. ZoneAlarm von www.zonelabs.com oder nutzen Sie die Firewall-Funktion der Internet-Security-Pakete von F-Secure, Network Associates, Panda Software oder Symantec. Der PCtipp testete diese Software letzten Herbst, siehe WEBCODE **pdf030966**.

**Benutzerkonten und Kennwörter:** Unter Windows 2000 und XP lässt sich mit einer gewissenhaften Verwendung von passwortgeschützten Benutzerkonten einiges an Sicherheit herausholen:

■ **Passwortzwang:** Auch wenn Sie einsam an Ihrem PC arbeiten – so richtig allein sind Sie spätestens dann nicht mehr, wenn eine Internetverbindung besteht. Darum sorgen Sie dafür, dass es auf Ihrem PC kein Benutzerkonto ohne Kennwort gibt, und arbeiten auch Sie selbst nicht dauernd mit Administratorrechten. Wie das geht, lesen Sie unter WEBCODE **pdf031236** und WEBCODE **pdf040258**.

■ **Gastkonto deaktivieren:** Auf PCs mit Windows 2000 und Windows XP gibts ein Konto namens «Gast». Dieses stellt ein Sicherheitsrisiko dar, da sich quasi jeder auf Ihrem PC anmelden kann, um ungeschützte Daten zu lesen. So deaktivieren Sie den Gast: Unter Windows 2000 klicken Sie mit Rechts auf ARBEITSPLATZ und wählen VERWALTEN. Unter «System» klappen Sie «Lokale Benutzer und Gruppen» auf und klicken auf BENUTZER. Falls der Benutzer «Gast» nicht bereits mit einem roten Kreis mit weissem X gekennzeichnet ist, klicken Sie das Konto doppelt an, haken die Option «Konto ist deaktiviert» an und klicken auf OK, Screen 1.

Unter Windows XP gehts zu START/SYSTEMSTEUERUNG/BENUTZERKONTEN. Sofern in der Übersicht der Benutzerkonten bei «Gast» nicht schon «Gastkonto ist nicht aktiv» steht, klicken Sie das Konto einmal an und im nächsten Fenster GASTKONTO DEAKTIVIEREN.

■ **Keine Freigabe ohne Kennwort:** Seien Sie zurückhaltend mit der Freigabe von Ordnern oder Laufwerken. Unter Windows XP und 2000 müssen Sie sowieso einen lokal vorhandenen Benutzer auswählen, wenn Sie etwas per Rechtsklick und FREIGABE mit anderen Usern teilen wollen. Unter Windows 9x und Me sollten Sie hingegen ein mindestens sieben Zeichen langes Kennwort festlegen, wenn Sie einen Ordner freigeben.

**Browser-Sicherheit:** Der Internet Explorer ist eines der häufigsten Einfallstore für unliebsame Programme, wie z. B. Browser-Hijacker, die den Browser auf unerwünschte Seiten umlenken, Spyware, Dialer oder Trojaner. Wer sich nicht dauernd mit solchen Störenfrieden herumschlagen will, steigt am besten auf einen anderen Browser um. Sowohl Mozilla (WEBCODE **20935**) als auch Opera (WEBCODE **16391**) denken nicht im Traum daran, solches ohne ausdrücklichen Wunsch des Benutzers zu installieren. Es gibt nur noch wenige Webseiten, die mit den aktuellen Versionen der beiden Alternativ-Browser Probleme machen.

Den Internet Explorer werden Sie höchstens noch fürs Windows-Update brauchen, für Online-Virenscanner (wie z. B. unter www.pctipp.ch/helpdesk/virenticker) oder für vereinzelte Shopping-Plattformen wie z. B. www.leshop.ch.

Sie wollen nicht umsteigen? Dann bringen Sie dem Internet Explorer wenigstens etwas mehr Sicherheit bei: Gehen Sie zu EXTRAS/INTERNETOPTIONEN und wechseln Sie ins Register SICHERHEIT. Klicken Sie die Zone «Internet» an und gehen zu STUFE ANPASSEN.

**Folgende Einträge setzen Sie auf «Deaktivieren»:**

- «ActiveX-Steuerelemente initialisieren und ausführen, die nicht sicher sind»
- «Download von unsignierten ActiveX-Steuerelementen»
- «Auf Datenquellen über Domänengrenzen hinweg zugreifen»
- «Kein Clientzertifikat auswählen, wenn kein oder nur ein Zertifikat vorhanden ist»

**Setzen Sie Folgendes auf «Eingabeaufforderung»:**

- «ActiveX-Steuerelemente ausführen, die für Scripting sicher sind»
- «ActiveX-Steuerelemente und Plugins ausführen»
- «Download von signierten ActiveX-Steuerelementen»
- «Cookies annehmen, die gespeichert sind»
- «Schriftartdownload»
- «Active Scripting»
- «Einfügeoperationen über ein Script zulassen»
- «Scripting von Java-Applets»
- «Installation von Desktopobjekten»
- «Programme und Dateien in einem IFRAME starten»
- «Subframes zwischen verschiedenen Domänen bewegen»

Das sind relativ sichere Einstellungen, sofern Sie damit richtig umgehen. Sie werden jetzt jedes Mal gefragt, ob sich → Scripts ausführen dürfen. Sie werden merken, dass das Surfen damit zur Qual wird: Der Internet Explorer wird Sie nämlich enorm oft mit Rückfragen belästigen, ob er nun dies oder jenes tun darf. Er kann nicht unterscheiden, ob ein Script einem guten oder bösen Zweck dient. Im Zweifelsfall müssen Sie bei den Rückfragen natürlich NEIN anklicken.

Falls Sie mit dem Internet Explorer weitersurfen wollen, könnten Sie häufig besuchte Sites, ▶

**«Ich brauche keine Updates, weil ich aus Prinzip keine Mailbeilagen öffne.»**

**Irrtum!**

Auf Grund früherer Sicherheitslücken konnten sich Wurmbeilagen automatisch (schon beim Lesen der Mail) ausführen. Ebenso konnte sich zum Beispiel der Blaster-Wurm (mitsamt seinen Nachfolgern) nur dank einer Sicherheitslücke verbreiten. Und das funktionierte sogar völlig unabhängig vom E-Mail-Empfang. Und genau solche Sicherheitslücken stopfen Sie mit den Windows-Updates.

**«Ach, Windows-Updates gehen doch viel zu lang. Und Microsoft will mich ja sowieso nur ausspionieren.»**

**Irrtum!**

Jeder Windows-PC, der sich mit einem Netzwerk oder dem Internet verbindet oder der auf anderem Weg Dateien von anderen PCs erhält, braucht die Service Packs und Patches, die via Windows-Update installiert werden.

**FACHCHINESISCH**

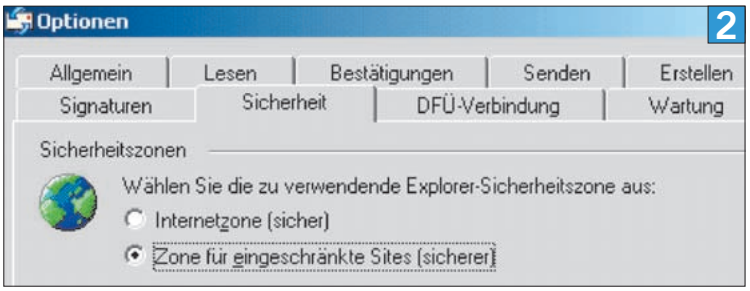
## Scripts

Scriptsprachen wie z. B. JavaScript oder VisualBasic Script werden oft eingesetzt, um Internetseiten interaktiv zu gestalten, zum Beispiel mit sich verändernden Schaltflächen und Menüs. Wie jede Programmiersprache können auch Scriptsprachen für schädliche Zwecke eingesetzt werden.

denen Sie vollumfänglich vertrauen, in die so genannte «Zone der vertrauenswürdigen Sites» aufnehmen. Klicken Sie VERTRAUENSWÜRDIGE SITES an und anschliessend SITES. Fügen Sie dort die Domain-Namen (z. B. www.pctipp.ch) hinzu, denen Sie das Ausführen von Scripts erlauben möchten. Eine detaillierte Anleitung finden Sie auch unter WEBCODE **pdf040271**.

**Outlook und Outlook Express:** Im Prinzip gilt für diese Mailprogramme dasselbe wie für den Internet Explorer, da beide diesen Browser zum Anzeigen von HTML-Inhalten verwenden. Nur lässt sich hier sicherheitstechnisch etwas mehr machen. Scripts jeglicher Gattung haben in einer seriösen E-Mail nichts verloren. Eine Mail, die Scripts enthält, ist schon zum Vornherein höchst verdächtig. Verbieten Sie deshalb Outlook und Outlook Express grundsätzlich alles, was über die Anzeige von normalem Text hinausgeht. Gehen Sie zu EXTRAS/OPTIONEN/SICHERHEIT und wählen Sie dort die ZONE FÜR EINGESCHRÄNKTE SITES aus, Screen 2.

Um diese Zone noch zusätzlich abzudichten, öffnen Sie den Internet Explorer, gehen zu EXTRAS/INTERNETOPTIONEN/SICHERHEIT, klicken EINGESCHRÄNKTE SITES an und wählen STUFE ANPASSEN. Nun setzen Sie rigoros alles, was Ihnen unter die Finger kommt, auf «Deaktivieren» bzw. «höchste Sicherheit».




**Blockieren Sie Scripts in E-Mails mit der Zone für eingeschränkte Sites**

**Alle Dateiendungen anzeigen:** Windows hat die gefährliche Angewohnheit, Ihnen standardmässig die meisten Dateiendungen vorzuenthalten. So können Sie manchmal nur raten, ob es sich bei der fraglichen Datei z. B. um eine potenziell gefährliche EXE-Datei handelt.

Öffnen Sie den Windows-Explorer und gehen Sie darin zu EXTRAS/ORDNEROPTIONEN. Wechseln Sie ins Register ANSICHT. Entfernen Sie die Häkchen bei den folgenden Optionen:

- «Dateinamenerweiterung bei bekannten Dateitypen ausblenden»
- «Geschützte Systemdateien ausblenden»

Bei «Versteckte Dateien und Ordner» setzen Sie hingegen die Option «Alle Dateien und Ordner anzeigen». Klicken Sie nun zuoberst die Schaltfläche WIE AKTUELLER ORDNER an und anschliessend zuunterst die Schaltfläche OK.

**«Wofür denn Windows-Updates? Ich habe doch einen Virenscanner!»**


## Irrtum!

Ein Virenscanner erkennt nur Schädlinge, die ihm bereits bekannt sind und dies auch nur dann, wenn er das Einfallstor des Virus oder Wurms überhaupt scannen kann. Trifft bei Ihnen ein Wurm ein, für den noch keine Virendefinitionen installiert wurden, kann Ihre Antiviren-Software den Schädling nicht blockieren. Der Blaster-Wurm hat sich zum Beispiel durch eine Sicherheitslücke auf unzählige Festplatten geschlichen, obwohl viele dieser PCs mit einem Virenscanner ausgerüstet waren.

**«Ich habe kein Windows, deshalb brauche ich auch keine Updates.»**

**Irrtum!**

Auch andere Betriebssysteme wie zum Beispiel Mac OS oder Linux können Sicherheitslücken aufweisen. Deshalb sind auch da gelegentlich Updates nötig.

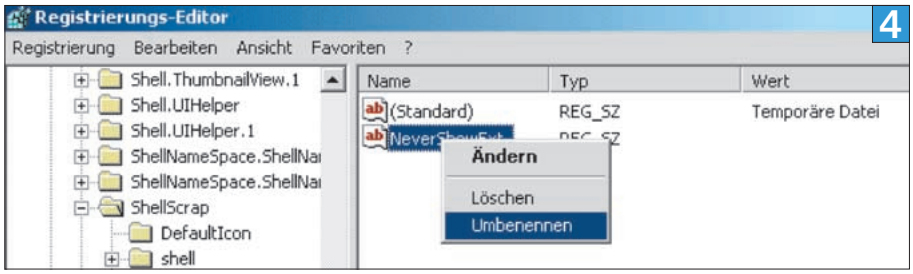
Windows kennt zwei weitere Dateitypen, die häufig in Wurmmails verwendet werden und deren Endungen Ihnen trotzdem unterschlagen werden, nämlich PIF und SHS, Screen 3.

Diesen Missstand beheben Sie durch einen Eingriff in die Windows-Registry. Seien Sie damit bitte enorm vorsichtig. Gehen Sie zu START/AUSFÜHREN (oder *Windowstaste+R*) tippen Sie *regedit* ein und drücken Sie *Enter*. Manövrieren Sie sich zum Registry-Zweig *HKEY_CLASSES_ROOT\ShellScrap* und klicken Sie diesen an. In der rechten Hälfte des Fensters entdecken Sie den Eintrag «NeverShowExt». Mit Rechts klicken Sie auf diesen und wählen UMBENENNEN, Screen 4. Nun ändern Sie den Namen des Eintrags zu «AlwaysShowExt» (ohne Anführungszeichen).

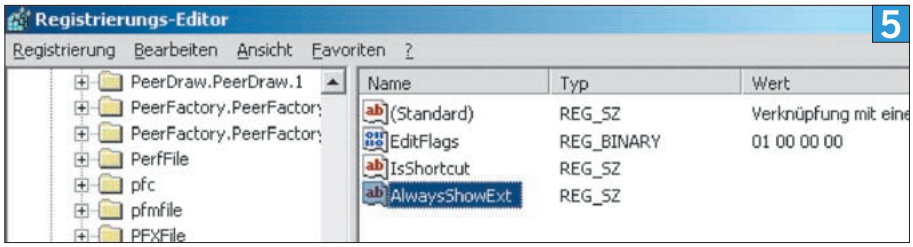
Da Sie schon den Registry-Editor offen haben, scrollen Sie in der linken Fensterhälfte wieder etwas hoch, bis Sie zu «piffile» gelangen. Dort tun Sie dasselbe: «piffile» anklicken und in der rechten Hälfte des Fensters den Eintrag «NeverShow Ext» zu «AlwaysShowExt» umbenennen, Screen 5.

Schliessen Sie den Registry-Editor. Nach dem nächsten PC-Neustart zeigt Ihnen Windows die Endungen wahrheitsgetreu an, Screen 6.


3 **Hätten Sies gemerkt? Links eine SHS- und rechts eine PIF-Datei**




4 **Der Registry-Eintrag vor der Änderung**




5 **Mit AlwaysShowExt zwingen Sie Windows zur Anzeige der Dateiendung PIF**


6 **Na, also! Jetzt ist Schluss mit dem Versteckspiel**

## Cleverer Umgang mit dem PC

Sicherheits-Software und vernünftige PC-Einstellungen nützen wenig, wenn Sie mit dem PC leichtfertig umgehen. Mit einer Portion Wachsamkeit erkennen Sie Bedrohungen womöglich noch vor Ihrem Virenscanner.

**Augen offen halten:** Klicken Sie gerade beim Surfen nicht blindlings auf jeden OK-Knopf. Lesen Sie Windows- oder Browser-Meldungen genau: Will sich da etwas installieren? Wenn ja: Ergibt es einen Sinn, dass sich von dieser Webseite etwas installiert? Zweifelhaftes verweigern Sie mit NEIN oder ABBRECHEN.

**«Mein PC läuft doch gut! Also kann da kein Virus drauf sein.»**

**Irrtum!**

Sehr viele Benutzer arbeiten auf einem infizierten Rechner, ohne es zu wissen. Schliesslich wollen sich ja Computerviren und -würmer – so lange es irgendwie geht – unbemerkt an möglichst viele weitere PCs weiterverbreiten. Würde z. B. der Swen-Wurm die Systeme merklich beeinträchtigen, wäre er schon längst ausgerottet.

**Seriöse und unseriöse Files:** Da Sie vorhin unter «Alle Dateiendungen anzeigen» Windows zu mehr Ehrlichkeit gezwungen haben, müssen Sie jetzt wissen, welche Dateien potenziell unseriös sind. Im Prinzip ist wirklich alles, was als Mailbeilage eintrifft, mit grösster Vorsicht zu geniessen. Beilagen mit diesen Endungen dürfen Sie auf gar keinen Fall öffnen, da es keinen vernünftigen Grund gibt, diese per Mail zu verschicken: .bat, .cmd, .com, .eml, .hta, .js, .jse, .pif, .scr, .shs, .vbe und .vbs.

Auch bei allen anderen Dateitypen sollten Sie misstrauisch sein, sofern sie per Mail eintreffen, insbesondere bei .doc, .exe, .htm, .html, .inf, .lnk, .mdb, .msi, .ppt und .xls. Fragen Sie den Absender zuerst, warum er die Datei geschickt hat. Öffnen Sie Mailbeilagen niemals direkt aus der Mail heraus. Hat der Absender eine plausible Begründung nachgeliefert, speichern Sie die Datei zuerst in einen Ordner oder auf den Desktop. Scannen Sie sie mit einem frisch aktualisierten Virenscanner. Kennen Sie den Absender nicht, löschen Sie die Mail, ohne die Beilage zu öffnen.

Eher unbedenklich sind Bilder (z. B. .bmp, .gif, .jpg, .jpeg, .tif, .png), Sounddateien (z. B. .mp3, .ogg, .wav) und Textdateien (.txt, .pdf). Speichern Sie auch diese zuerst ausserhalb der Mail, starten Sie die Anwendung, mit der Sie die Datei öffnen wollen, und tun Sie das per DATEI/ÖFFNEN. Ein etwas schnellerer Weg ist ein Rechtsklick auf die Datei und der Menüpunkt ÖFFNEN MIT.

**Virenscanner auf Abwegen:** Im Computerbereich ist nichts zu hundert Prozent sicher. Ein Virenscanner kann sich irren – auf die eine oder andere Weise.

■ **Blinder Virenscanner:** Wenn Ihr Virenscanner in einer Datei keinen Schädling findet, bedeutet das nur, dass er keinen sieht, den er schon kennt. Gerade wenn Sie eine veraltete Programmversion verwenden oder die Updates seit längerem versäumt haben, ist ein «Kein Virus gefunden» eine recht unzuverlässige Aussage. Prüfen Sie verdächtige Dateien mit einem zweiten Scanner eines anderen Herstellers – und vergessen Sie das regelmässige Update nicht. ▶

**«Wenn ich den Absender einer Mail kenne, dann ist die Mailbeilage ungefährlich.»**

**Irrtum!**

Viele Viren und Würmer fälschen den Absender; also jenen Namen und jene Mailadresse, die Sie in der «Von»-Zeile lesen. Ausserdem waren auch schon Würmer im Umlauf, die jede Mail, die auf einem infizierten PC eintraf, sofort automatisch beantworteten und eine Wurm-Kopie beilegten. So können Sie also nie sicher sein, dass eine Beilage sauber ist.

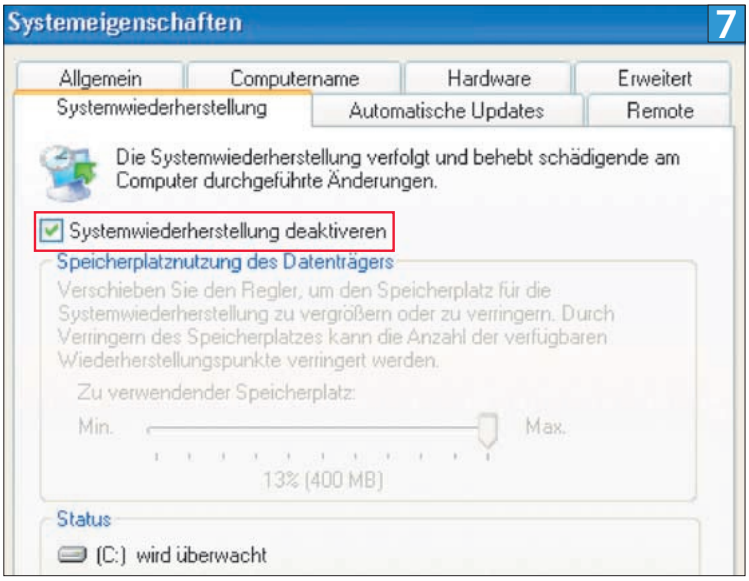
Anstatt zwei Virenscanner zu installieren (was zu Abstürzen führen kann), holen Sie die zweite Meinung bei einem Online-Scanner ein (www.pctipp.ch/helpdesk/virenticker). Einzelne Dateien lassen sich auch übers Webformular von Kaspersky prüfen (www.kaspersky.com/de/remoteviruschk.html).

■ **Keine Panik bei Alarm:** Findet Ihr Virenscanner etwas wie «JS.Exception.Exploit» oder «IFRAME.Exploit», ist das kein Grund zur Panik. Ein «Exploit» bedeutet, dass eine Webseite oder eine E-Mail Programmcode enthält, der *versuchen* könnte, eine bestimmte Sicherheitslücke Ihres Systems zu missbrauchen. Natürlich sind solche Webseiten und Mails höchst unseriös. Wenn aber alle Windows-Updates installiert und die Virendefinitionen auf dem neusten Stand sind, kann Ihnen ein solcher «Exploit» wenig anhaben. Der Virenscanner meldet dieses Vorkommnis natürlich trotzdem, denn dies ist schliesslich seine Aufgabe.

Findet Ihr Virenscanner eine Exploit-Datei in den «Temporary Internet Files», schliessen Sie alle Browser-Fenster bis auf eines. Gehen Sie darin zu EXTRAS/INTERNETOPTIONEN und leeren Sie den Cache. Schliessen Sie den Browser wieder und scannen Sie Ihr System. Oft ist der «Schädling» dann schon Geschichte.

Wird der Scanner in einem Ordner wie «System Volume Information» oder «_RESTORE» fündig? Dateien lassen sich dort nicht einfach löschen. Schalten Sie daher zuerst die Systemwiederherstellung aus: Gehen Sie zu START/SYSTEMSTEUERUNG/LEISTUNG UND WARTUNG/SYSTEM. Wechseln Sie ins Register SYSTEMWIEDERHERSTELLUNG und setzen Sie ein Häkchen bei «Systemwiederherstellung deaktivieren», **Screen 7**. Nach einem Neustart scannen Sie den PC. In der Regel ist zu diesem Zeitpunkt die leidige Sache bereits erledigt, siehe auch WEBCODE **26316**.

Wird als Fundort ein Ordner wie «Recycler» genannt, muss Ihr erster Schritt natürlich ein Rechtsklick auf den PAPIERKORB sein und im Kontextmenü der Befehl PAPIERKORB LEEREN.




**Wird ein Schädling im RESTORE-Ordner gefunden, deaktivieren Sie die Systemwiederherstellung**

**«Und wenn ich mal merken sollte, dass da ein Virus ist, der mich an der Arbeit hindert, installiere ich halt einen Virenscanner, der mir das Vieh beseitigt.»**

### Irrtum!

Ist der Schädling schon da, ist es oft schon zu spät. Virenscanner sind nicht in erster Linie fürs nachträgliche Entfernen von Viren geschaffen, sondern um deren Eindringen ins System zu verhindern. Es gibt Viren und Würmer, die fast nicht mehr aus einem System zu bekommen sind. Zudem gibts darunter einige echte Bösewichte, die Ihre Daten zerstören können. So haben sich zum Beispiel viele Varianten des LoveLetter-Wurms explizit an JPG- und MP3-Dateien vergriffen. In so einem Fall kann Ihnen kein Virenscanner mehr helfen, sondern höchstens noch ein Datenrettungslabor.

## Lug und Trug in Mail und Web

Der Maler Magritte hatte völlig Recht, als er auf eines seiner Bilder schrieb: «Ceci n'est pas une pipe» («Dies ist keine Pfeife»). Schliesslich handelte es sich nur um das *Abbild* einer solchen. Viel weniger ehrlich gehts im Web und in Ihrem elektronischen Posteingang zu und her. Wir zeigen einige Beispiele, denen Sie misstrauen sollten.

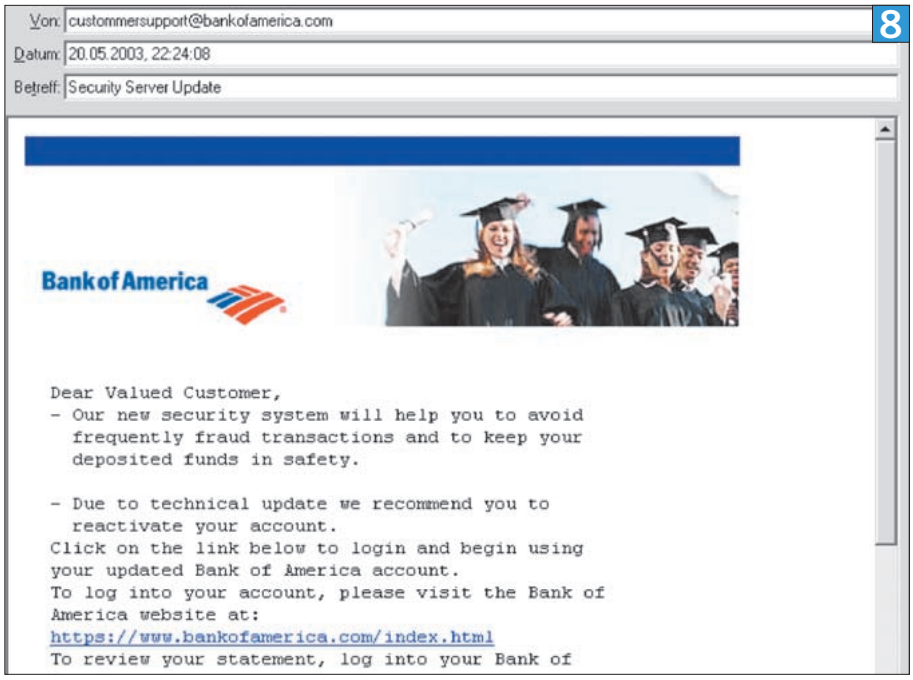
**«100% virenfrei»:** Einige Antiviren-Programme (z. B. Avast) betreiben gerne etwas Gratiswerbung. Sie fügen daher jeder ausgehenden E-Mail eine Zeile hinzu, die besagt, dass die Mail nach Viren gescannt und für gut befunden wurde. Dieses Verhalten ist jedoch völlig unsinnig: Erstens könnte der Virenscanner einen Schädling übersehen haben und zweitens gibt es schon längst Würmer, die genau diese Zeilen in die Mails hineinschreiben. Wenn Sie also in einer Mail etwas lesen wie «No viruses or suspicious files were found in the attached file», «Scanned by McAfee» oder dergleichen, dann handelt es sich schlicht um eine freche Behauptung.

**Lügende Pop-ups:** Beim Surfen auf unbekannten Pfaden erscheinen oft Pop-up-Fenster, die Ihnen etwas von Sicherheitslücken erzählen,

**«Ich weiss zwar, dass mein PC einen Wurm hat, aber was solls? Der PC läuft ja noch gut – und nur das zählt.»**

### Irrtum!

Wenn Sie einen Virus oder Wurm auf dem PC haben, wird sich der Schädling von dort aus weiterverbreiten. Nicht zuletzt gibts Schädlinge, die erst nach einiger Zeit zuschlagen. So zum Beispiel der CIH-Virus: Wurde dieser auf einem PC nicht rechtzeitig eliminiert, löschte er am nächsten 26. Tag eines Monats dessen Festplatte und machte durch ein Überschreiben des Flash-BIOS das Computermainboard unbrauchbar.




**Achtung gefälscht: Auf einen solchen Link sollten Sie keinesfalls klicken**


**Der Beweis im E-Mail-Quelltext: Der Link A führt auf die IP-Adresse B, also nicht zur Bank of America**

die sich nur reparieren lassen, indem Sie eine bestimmte Zugangs-Software oder ein bestimmtes kostenpflichtiges Programm installieren. In den meisten Fällen wollen Ihnen die Verursacher solcher Pop-ups in Wirklichkeit einen Dialer («Zugangs-Software») andrehen. Wenn Sie Sicherheits-Software brauchen, gehen Sie bitte auf die Webseiten von namhaften Herstellern. Und das Patchen Ihres Systems erledigen Sie sowieso via Windows-Update.

**Gefälschte Absender:** Bunt gestaltete und authentisch aussehende Mails, die angeblich von Microsoft stammen, enthalten in der Beilage keine Updates, sondern einen Wurm. Wir können es gar nicht oft genug wiederholen: Microsoft verschickt *keine* Updates per E-Mail. Auf eine ähnliche Weise werden auch Würmer verschickt, die in perfektem eBay- oder PayPal-Layout daherkommen. Übrigens sind die Absenderadressen in praktisch allen Viren- und Wurmmails erstunken und erlogen. Es hat also keinen Sinn, auf eine Wurmmail zu antworten: Es wird den Falschen treffen.

**Datenspione:** Manchmal enthalten gefälschte Mails keine Beilage, sondern nur einen Link, unter dem Sie angeblich Ihre Benutzer- oder Finanzdaten (z. B. Kreditkartennummer) eingeben sollen, Screen 8. Weder Ihr Provider noch eBay noch Ihre Bank oder Kreditkartenfirma würde von Ihnen tatsächlich verlangen, auf einen E-Mail-Link zu klicken, um dort Ihre Daten zu verifizieren. Sollte eine solche Mail eintreffen, klicken Sie nicht auf den Link! Einen Hinweis auf die Fälschung sehen Sie im HTML-Quelltext der E-Mail, Screen 9. Die finden Sie in Outlook Express mit einem Rechtsklick auf die E-Mail und im Kontextmenü über Eigenschaften/Details/Quelltext.

Im Zweifelsfall tippen Sie die offizielle Adresse des Anbieters selbst (von Hand) ins Browser-Fenster und melden sich auf gewohnte Weise bei diesem Dienst an. Sollte mit Ihrem Banking-, eBay, PayPal- oder sonstigen Konto etwas nicht stimmen, würde das bestimmt an Ort und Stelle vermerkt sein. Die verdächtige Mail leiten Sie an den Support des betreffenden Anbieters weiter. Der wird Ihnen sagen können, was es damit auf sich hat. ■