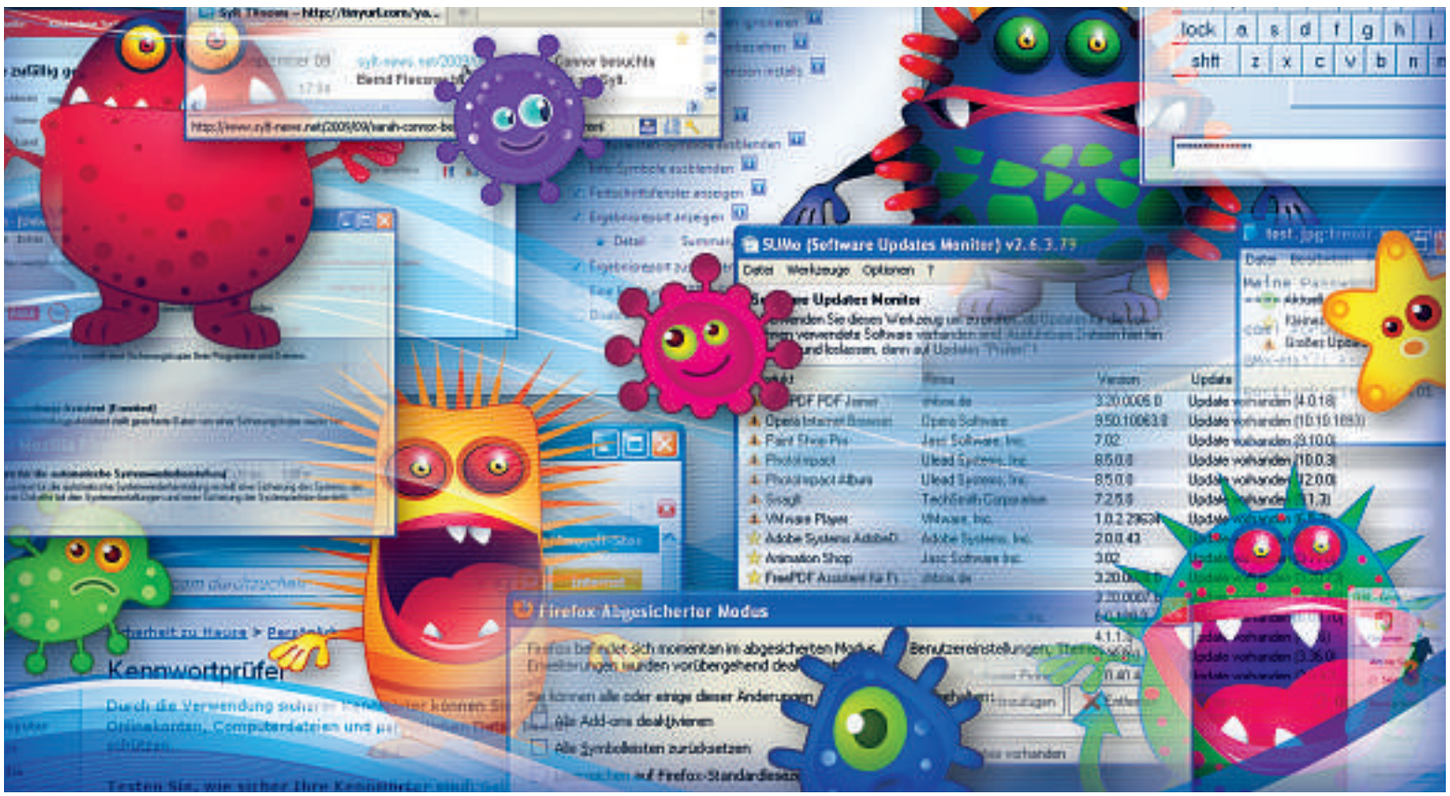


Die besten Sicherheits-Tipps

Nackt im Netz? Das passiert schneller, als Sie denken. Schon ein unbedacht eingestelltes Urlaubsfoto reicht. Online PC macht Sie fit für die Selbstverteidigung im Internet und die Abwehr von Datenspionen.

Kein Aspekt ist so wichtig wie die Sicherheit Ihres PCs. Welches Betriebssystem, welche Tools oder Hardware Sie nutzen – das alles zählt wenig, wenn Angreifer aus dem Internet Ihren PC kapern und Daten stehlen.

Auf den folgenden Seiten finden Sie daher ausgewählte Sicherheits-Tipps, mit denen Sie Ihren PC absichern und vor Eindringlingen schützen.

Kompakt

- ***Der Artikel stellt 30 von der Redaktion geprüfte Sicherheits-Tipps vor.***
- ***Alle benötigten Tools finden Sie auf der Heft-DVD sowie im Internet.***

INTERNET

1. Surfen im Privat-Modus

Moderne Webbrowser verhindern im Privat-Modus, dass Cookies, temporäre Dateien oder der Verlauf gespeichert werden. Diese Daten werden gelöscht, sobald Sie den Browser beenden.

In Firefox 3.6 aktivieren Sie den Privat-Modus mit der Tastenkombination *[Strg Umschalt P]* und einem Klick auf *Privaten Modus starten*. Der Browser wechselt dann in den privaten Modus, den Sie durch erneutes Drücken von *[Strg Umschalt P]* wieder verlassen.

Im Internet Explorer 8 aktivieren Sie den Privat-Modus ebenfalls mit *[Strg Umschalt P]*. Der Internet Explorer öffnet dann ein neues Browserfenster im *InPrivate-Modus*, den Sie am entsprechenden Symbol ganz links in der Adresszeile erkennen. Um den Privat-Modus wieder zu verlassen, schliessen Sie einfach das Browserfenster.

Tastaturspione austricksen: Neo's Safekeys 2008 2.3.2 verhindert das Aufzeichnen Ihrer Tastatureingaben (Bild A).

WINDOWS XP, VISTA UND 7

2. Schutz vor Keyloggern

Keylogger, die jeden Tastendruck aufzeichnen und per Internet versenden, gehören zu den grössten Gefahren. Eine Freeware trickst die Tastaturspione aus.

Neo's Safekeys 2008 2.3.2 (kostenlos, **www.aplin.com.au/?page_id=368** und auf) blendet eine Bildschirmtastatur ein. Ihr Passwort geben Sie durch Klicks auf die Buchstabenfelder ein (Bild A). Anschliessend markieren Sie das Kennwort mit der Maus und ziehen es an die Stelle, an der Sie es eingeben sollen.

BILDBEARBEITUNG

3. Verräterische Fotos

Digitalkameras speichern in EXIF-Daten Infos zu Ihren Schnappschüssen, wie zum Beispiel Blende, Belichtungszeit, Blitzeinstellung, Kameratyp sowie Datum und Uhrzeit. Die EXIF-Daten enthalten aber auch Vorschaubilder der Aufnahmen, und diese zeigen mitunter mehr, als Ihnen lieb ist (siehe auch nebenstehenden Kasten).

Das Vorschaubild und andere EXIF-Informationen entfernen Sie, indem Sie eine Kopie des Bildes ohne EXIF-Daten erzeugen. Dazu öffnen Sie das Bild in einer Bildbearbeitung und markieren mit *[Strg A]* das gesamte Bild oder den Bildbereich, den Sie benötigen. Wählen Sie *Bearbeiten, Kopieren* und erstellen Sie mit *Datei, Neu…* ein neues Bild. Der Befehl *Bearbeiten, Einfügen* fügt die Bilddaten ein. Dabei werden die EXIF-Daten nicht kopiert.

WINDOWS XP

4. Datenklau per USB-Stick

Eine Änderung in der Windows-Registry verhindert, dass jemand Daten von Ihrem PC auf einen USB-Stick kopiert.

Zuerst öffnen Sie den Registrierungs-Editor, indem Sie *[Windows R]* drücken und `regedit` eingeben. Navigieren Sie zum Schlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies*.

Falls dieser Schlüssel fehlt, wählen Sie *Bearbeiten, Neu, Schlüssel* und geben Sie `StorageDevicePolicies` ein.

Wählen Sie *Bearbeiten, Neu, DWORD-Wert* und geben Sie `WriteProtect` ein. Klicken Sie doppelt auf *WriteProtect* und geben Sie als Wert `1` ein. Um die Änderung rückgängig zu machen, setzen Sie den Wert wieder auf `0`.

WINDOWS XP, VISTA UND 7

5. Schnelle PC-Sperre

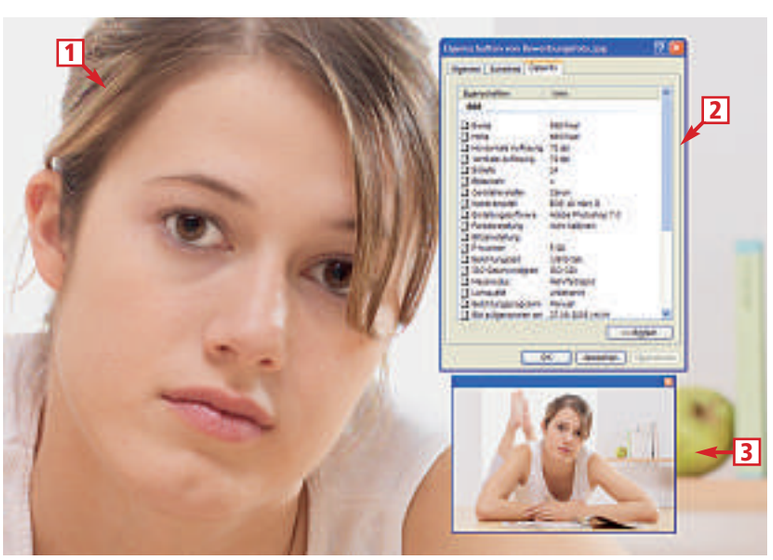
Wenn Sie Ihren PC beim Verlassen des Arbeitsplatzes sperren möchten, dann nutzen Sie die Tastenkombination *[Windows L]* oder ein klickbares Icon.

Das Icon für eine PC-Sperre per Mausklick integrieren Sie beispielsweise in die Schnellstartleiste. Klicken Sie mit der rechten Maustaste auf die Schnellstartleiste und wählen Sie *Ordner öffnen*.

Im Folgedialog nutzen Sie dann *Datei, Neu, Verknüpfung* und tragen `rundll32.exe·user32.dll,LockWorkStation` in das Eingabefeld ein. Abschliessend wählen Sie für die Verknüpfung einen Namen wie zum Beispiel `Computer·sperren` und klicken danach auf *Fertig stellen*. ▶

Verräterische Fotos: Was EXIF-Daten verraten

Die EXIF-Daten eines Bildes enthalten Detailinfos zur Aufnahme. Ein Rechtsklick auf die Bilddatei und die Auswahl "Eigenschaften, Dateiinfo" zeigen diese EXIF-Daten an.



1 Foto
Dieses Foto wurde mit Photoshop auf einen kleinen Ausschnitt reduziert.

2 EXIF-Daten
Sie enthalten Infos zu Blende, Belichtungszeit, Blitzeinstellung, Kameratyp sowie Datum und Uhrzeit.

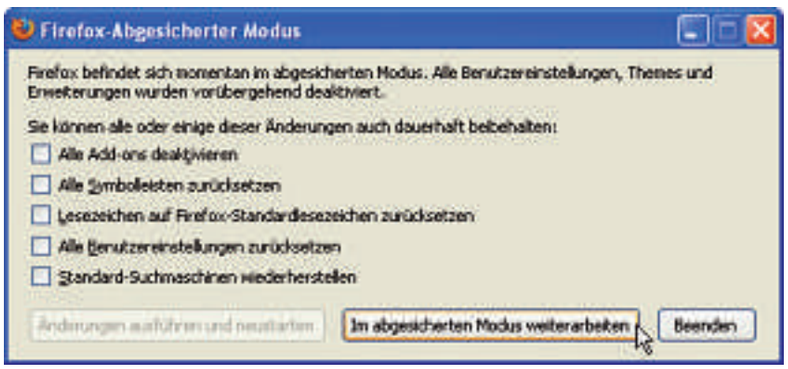
3 Vorschaubild
Die EXIF-Daten enthalten auch das Originalbild in Form einer Miniaturvorschau. Wenn die Bildbearbeitung die Vorschau nicht aktualisiert, dann stellen Sie nicht nur Ihr Gesicht, sondern Ihren ganzen Körper ins Internet.

WINDOWS XP

6. WPA2 für Windows XP

Für Windows XP hält Microsoft ein Update bereit, das Ihr WLAN auf das sichere Protokoll WPA2 umstellt.

Voraussetzung für die sichere Funknetzübertragung ist ein WPA2-fähiger WLAN-Router. Das Update für Windows XP mit Service Pack 2 finden Sie unter **http://support.microsoft.com/kb/917021/de**. Ein Klick auf *Drahtlosnetzwerk-client-Updatepaket jetzt herunterladen* startet den Download.



Firefox-Add-ons deaktivieren: Der abgesicherte Modus schaltet vorübergehend alle Firefox-Erweiterungen ab. Damit verhindern Sie, dass Add-ons Schadecode einschleusen oder Daten ausspähen (Bild B).

INTERNET EXPLORER 8

7. IE 8 ohne Add-ons

Add-ons erweitern den Internet Explorer 8 um neue Funktionen. Schlecht programmierte Add-ons stellen jedoch ein Sicherheitsrisiko dar und können schadhaften Code ins System einschleusen.

Zur Sicherheit lässt sich der Internet Explorer auch ohne Add-ons starten. Dazu drücken Sie *[Windows R]* und geben dann den Befehl `iexplore.exe -extoff` ein.

FIREFOX

8. Firefox ohne Add-ons

Bei Bedarf lässt sich Firefox ebenfalls ohne Add-ons starten. Dazu nutzen Sie den abgesicherten Modus (Safe Mode).

Drücken Sie *[Windows R]* und geben Sie den Befehl `firefox.exe -safe-mode` ein, um Firefox zu starten. Im Dialog *Firefox – Abgesicherter Modus* (Bild B) entfernen Sie alle Häkchen und klicken auf *Im abgesicherten Modus weiterarbeiten*. Nun sind alle Add-ons deaktiviert. Zudem erscheint Firefox jetzt im Standard-Theme und alle Benutzereinstellungen sind auf die Standardwerte zurückgesetzt.

FIREFOX AB VERSION 3

9. Konfigurations-Backup

Febe 6.3.2 (kostenlos, **https://addons.mozilla.org/de/firefox/addon/2109** und auf) exportiert und importiert installierte Firefox-Add-ons ebenso wie Themes, Cookies und Passwörter.

Nach der Installation der Firefox-Erweiterung und einem Neustart des Browsers rufen Sie *Extras, FEBE, FEBE-Einstellungen* auf (siehe auch Kasten auf Seite 33). Legen Sie unter *Ordner* den Zielordner fest und wählen Sie eine der im Register *Optionen* genannten Möglichkeiten. Dann erstellen Sie mit *Extras, FEBE, Sicherungen erstellen* eine Backup-Datei, die Febe im XPI-Format auf der Festplatte ablegt.

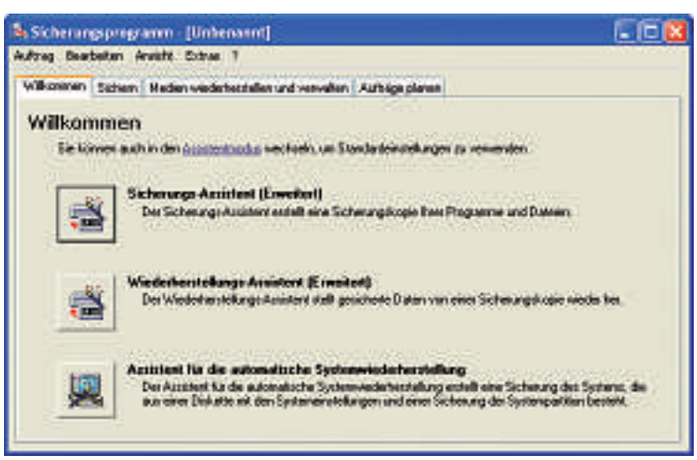
WINDOWS XP

10. Gesperrte Systemsteuerung

Ein Registry-Hack verhindert, dass andere Benutzer Ihres PCs die Systemeinstellungen ungefragt verändern.

Öffnen Sie den Registrierungs-Editor mit *[Windows R]* und `regedit`. Navigieren Sie zu *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer*.

Nun klicken Sie doppelt auf *NoControlPanel* und ändern den Wert auf `1`. Ist der Eintrag noch nicht vorhanden, legen Sie ihn mit *Bearbeiten, Neu, Zeichenfolge* an. Nach der Änderung lässt sich die Systemsteuerung vom aktuellen Benutzer nicht mehr starten und sie wird für ihn auch nicht mehr im Startmenü angezeigt. Der Wert `0` nimmt die Änderung zurück.



Microsoft NTBackup: Unter Windows XP Home müssen Sie das kostenlose Sicherungsprogramm selbst nachinstallieren (Bild C).

WINDOWS XP

11. Gesperrte Programme

Dieser Trick schützt Sie davor, dass andere Benutzer bestimmte Programme Ihres PCs aufrufen.

Öffnen Sie mit *[Windows R]* und `regedit` den Registrierungs-Editor. Navigieren Sie zu *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer*.

Wählen Sie *Bearbeiten, Neu, DWORD-Wert* und nennen Sie den Wert `DisallowRun`. Mit einem Doppelklick weisen Sie dem Eintrag den Wert `1` zu. Dann legen Sie mit *Bearbeiten, Neu, Schlüssel* einen neuen Schlüssel an und nennen ihn ebenfalls `DisallowRun`. Klicken Sie auf den neuen Schlüssel, wählen Sie *Bearbeiten, Neu, Zeichenfolge* und vergeben Sie als Name `1`. Klicken Sie den Eintrag doppelt an und tragen Sie bei *Wert* den Pfad zu dem Programm ein, etwa `C:\Programm.exe`. Setzen Sie den Pfad in Anführungszeichen, wenn er Leerzeichen enthält.

Der aktuelle Benutzer kann nach einem Neustart des PCs das Programm mit dem Dateinamen *Programm.exe* nicht mehr starten. Falls Sie weitere Programme sperren wollen, dann fügen Sie entsprechend weitere Parameter `2`, `3` und so fort hinzu.

Hinweis: Wenn die Systempartition Ihres PCs mit NTFS formatiert ist, dann lässt sich statt des hier beschriebenen Tricks die Rechtevergabe von Windows zum Sperren des Programms nutzen.

WINDOWS XP HOME

12. Verstecktes Backup-Tool

NTBackup ist eine kostenlose Backup-Lösung für Windows XP (Bild C). Nutzer mit Windows XP Home müssen das Microsoft-Tool allerdings selbst nachinstallieren.

Dazu legen Sie die Setup-CD von Windows XP Home in das Laufwerk ein und wechseln von dort in das Verzeichnis *VALUEADD\MSFT\NTBACKUP*. Die Installation starten Sie nun per Doppelklick auf *NTBACKUP.MSI*. Nach Abschluss der Installation finden Sie den neuen Eintrag *NTBackup* im Startmenü unter *Start, Alle Programme, Zubehör, Systemprogramme, Sicherung*. Starten Sie das Programm NTBackup von dort.

SUMO 2.6.3.79

13. Software-Updates

Veraltete Software enthält häufig Sicherheitslücken. Der Software Updates Monitor (Sumo) 2.6.3.79 (kostenlos, **www.kcsoftwares.com/?sumo** und auf DVD) deckt die Schwachstellen auf.

Beim ersten Start von Sumo öffnet sich ein Assistent. Klicken Sie auf *Installierte Software automatisch erkennen*. Sumo versucht nun, alle auf Ihrem PC installierten Anwendungen zu lokalisieren. Anschliessend klicken Sie auf *Auf Updates Ihrer installierten Software prüfen*. Beenden Sie den Assistenten danach mit *Schliessen*.

Sumo zeigt Ihnen nun zuerst die mit einem roten Warnzeichen markierten Programme, die schon länger nicht mehr aktualisiert wurden (Bild D). Darunter markieren gelbe Sterne Tools, für die kleinere Updates bereitstehen.

Wenn Sie einen Eintrag mit der rechten Maustaste anklicken und *Update holen* wählen, öffnet sich ein Browserfenster mit Links zu verschiedenen Download-Portalen. Meist geht es jedoch schneller, wenn Sie den Namen des Tools bei Google eintippen und das Update direkt vom Hersteller holen.

WINDOWS

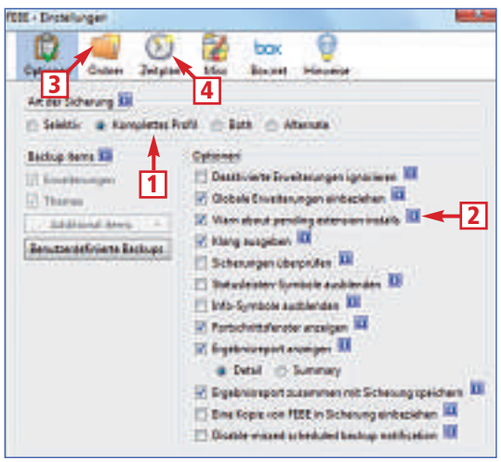
14. Update-DVD

Sicherheitsrelevante Patches für Windows lassen sich auch als DVD-Abbild laden.

Das DVD-Abbild der monatlichen Sicherheits-Patches von Microsoft erhalten Sie über **www.microsoft.com/downloads/results.aspx?DisplayLang=de&nr=20&freetext=-ISO-Abbild+Sicherheit.**

So geht's: Firefox-Profil sichern mit Febe 6.3.2

Febe 6.3.2 (kostenlos, https://addons.mozilla.org/de/firefox/addon/2109 und auf DVD) ist ein Backup-System für Ihr Firefox-Profil. Das Tool sichert alle installierten Firefox-Erweiterungen sowie Ihre Themes, Cookies und Passwörter.



1 Optionen
Wählen Sie als *Art der Sicherung* die Option *Komplettes Profil*.

2 Hilfe
Ein Klick auf das blaue Info-Symbol öffnet ein Fenster mit kurzen Hilfetexten.

3 Ordner
Dieses Symbol führt Sie zur Definition des Backup-Zielordners.

4 Zeitplan
Klicken Sie hier, um festzulegen, wann und wie oft Febe ein Backup erstellt.

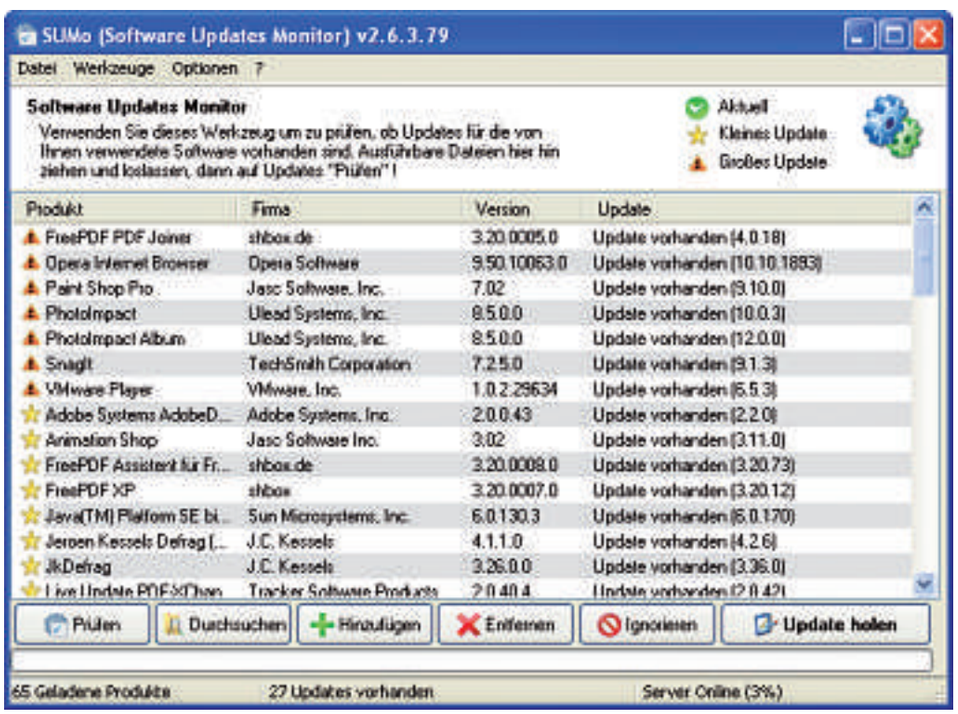
E-MAIL

15. Wegwerf-Adressen

Zahllose Webseiten wie Foren und Shops verlangen zur Anmeldung eine E-Mail-Adresse. Wegwerf-Adressen schützen Ihre Privatsphäre und verhindern Spam.

Die Firefox-Erweiterung Trashmail.net 2.0.2 (kostenlos, **https://addons.mozilla.org/de/firefox/addon/1813** und auf DVD) richtet Wegwerf-Adressen ein und verwaltet sie. Nach der Installation konfigurieren Sie die Firefox-Erweiterung mit *Extras, Trashmail, TrashMail Optionen*. Im Folgedialog tragen Sie bei *Ihre echte E-Mail-Adresse* Ihre Adresse ein und speichern diese mit einem Klick auf *Save*.

Wenn Sie sich künftig im Web registrieren, müssen Sie nicht mehr Ihre private E-Mail-Adresse preisgeben. Stattdessen klicken Sie mit der rechten Maustaste auf das entsprechende Eingabefeld der Webseite und wählen *Wegwerfbare Adresse einfügen*. Ein Klick auf *Erstellen* trägt die Wegwerf-Adresse ein. E-Mails werden an Ihre echte Adresse weitergeleitet. Nach Ablauf der Gültigkeitsdauer oder einer maximalen Anzahl von Weiterleitungen erlischt die Wegwerf-Adresse.



Update-Manager: Sumo 2.6.3.79 zeigt an, welche Software auf Ihrem PC veraltet ist (Bild D).

WINDOWS XP, VISTA UND 7

16. PC ohne Datenspuren

So entfernen Sie Spuren vom PC und machen mit einer aufgeräumten Windows-Registry Ihr System sicherer.

Das kostenlose Tool Ccleaner 2.26 (kostenlos, **www.ccleaner.com/download/builds** und auf DVD) schützt Ihre Privatsphäre, befreit Ihre Festplatte von Ballast und verschlankt das Betriebssystem. Am besten laden Sie aus dem Internet die portable Version des Tools. Diese muss nicht installiert werden und enthält auch keine Werbe-Toolbar.

Entpacken Sie das Tool und starten Sie es mit einem Doppelklick auf die Datei *CClea-* ▶

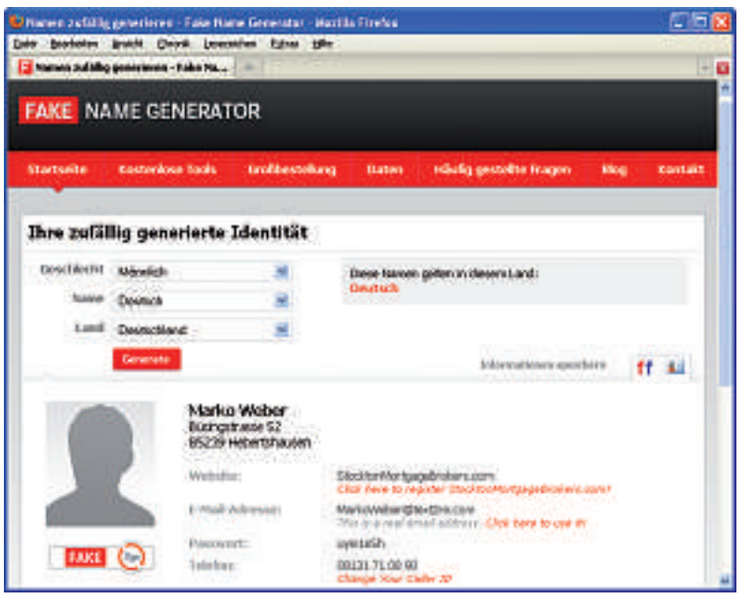
ner.exe. Nun legen Sie fest, welche Operationen Ccleaner ausführen soll. Ein Klick auf *Analysieren* startet den Vorgang. Prüfen Sie die Löschliste sorgfältig, bevor Sie die überflüssigen Daten mit *Starte CCleaner* endgültig beseitigen.

FAKE NAME GENERATOR

17. Gefälschte Identitäten

Der Fake Name Generator (**www.fakenamegenerator.com**) erstellt gefälschte, aber echt wirkende Identitäten, die sich beispielsweise für die Anmeldung in Online-Foren eignen.

Der Dienst schützt Ihre persönlichen Informationen vor Datensammlern im Internet. Wenn Sie sich einen schweizerischen Datensatz erzeugen lassen, passen sogar die Postleitzahl und die Vorwahl zum generierten Wohnort (Bild E).



Fake Name Generator: Der kostenlose Online-Dienst erzeugt gefälschte, aber plausible Identitäten für 19 Länder, darunter auch die Schweiz (Bild E).

BETTER PRIVACY 1.45

18. Supercookies in Flash

Der Flash-Player legt heimlich Cookies auf Ihrem PC ab, in denen Website-Betreiber Ihr Surfverhalten speichern. Diese Supercookies lassen sich nicht im Browser löschen.

Die Firefox-Erweiterung Better Privacy 1.45 (kostenlos, **https://addons.mozilla.org/de/firefox/addon/6623** und auf DVD) macht kurzen Prozess mit Flash-Cookies. Nach der Installation des Add-ons öffnen Sie die Optionen der Erweiterung mit *Extras, Better Privacy*. In der *Liste gespeicherter Flash-Cookies (LSOs)* sehen Sie alle auf Ihrem PC abgelegten Flash-Cookies. Ein Klick auf *Entferne alle LSOs* löscht die Spionage-Kekse.

BIOS-ZUGRIFFSSCHUTZ

19. Risiko Ophcrack

Mit der kostenlosen Ophcrack Live-CD ist das Knacken von allen Windows-Passwörtern für Hacker ein Kinderspiel.

Vergeben Sie deshalb zusätzlich ein Benutzer-Passwort im BIOS Ihres Rechners. Dazu rufen Sie beim PC-Start mit der Taste *[Entf]* das BIOS auf. Die entsprechende Option finden Sie dann meist unter dem Namen *User Password* oder *Change User Password*.

WINDOWS XP

20. Risiko Auslagerungsdatei

Unverschlüsselte Daten und Passwörter sind mitunter auch nach Herunterfahren des PCs im Klartext auf der Festplatte vorhanden. Windows speichert sie in der Auslagerungsdatei.

Konfigurieren Sie Windows so, dass es die Auslagerungsdatei automatisch löscht: Öffnen Sie den Registrierungs-Editor, indem Sie *[Windows R]* drücken und `regedit` eingeben. Markieren Sie den Schlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\MemoryManagement*. Klicken Sie im rechten Fensterbereich doppelt auf *ClearPageFileAtShutdown* und geben Sie unter *Wert* `1` ein. Falls der Eintrag *ClearPageFileAtShutdown* noch nicht existiert, legen Sie ihn mit *Bearbeiten, Neu, DWORD-Wert* neu an. Fortan wird die Auslagerungsdatei beim Herunterfahren des PCs automatisch gelöscht.

HIJACK FREE 3.1.0.22

21. Schädlinge im Autostart

Trojaner nisten sich in den Autostart ein, um sicherzustellen, dass sie bei jedem Systemstart aktiviert werden. Verhindern lässt sich das nur durch eine regelmässige Systemanalyse.

Hijack Free 3.1.0.22 (kostenlos, **www.hijackfree.de/de** und auf DVD) ist darauf spezialisiert, die verschiedenen Autostart-Bereiche von Windows nach Schädlingen zu durchsuchen und diese zu entfernen. Die integrierte Online-Analyse dieses Tools zeigt sofort, welche Autorun-Einträge, Prozesse oder Add-ons eine Gefahr darstellen (Bild F).

Hijack Free analysiert mehr als 30 Positionen Ihres PCs, an denen sich Autostart-Einträge einnisten. Anschliessend übermittelt das Tool die Daten Ihrer Windows-Installation zur Online-Analyse an einen Webserver. Dieser liefert Ihnen dann eine Liste aller Autostart-Einträge, Prozesse und Add-ons Ihres PCs. Ist einer der Einträge gelb oder rot gefärbt, dann sollten Sie ihn mit *View Details* genauer unter die Lupe nehmen und gegebenenfalls deaktivieren.

Für eine derartige Online-Analyse starten Sie Hijack Free und klicken dann rechts oben auf die Schaltfläche *Online-Analyse*. Wenig später erscheint im Webbrowser die detaillierte Gefahrenliste aller Software-Einträge Ihres PCs.

DISABLE STARTUP 1.2

22. Wächter für Autostart

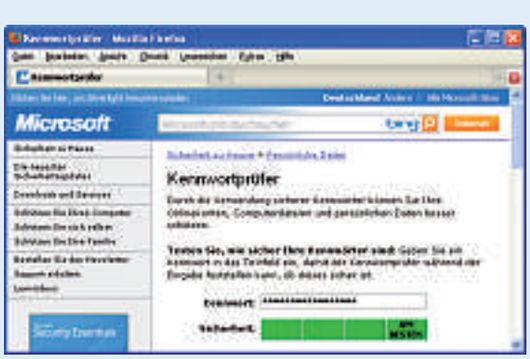
Die Freeware Disable Startup 1.2 (kostenlos, **www.disablestartup.com**) überwacht die Autostart-Bereiche von Windows.

Wählen Sie beim ersten Aufruf im Reiter *Disable Startup Settings* die Option *Show one warning message when new startup added*.

Online-Check: Microsoft Kennwortprüfer

Ein sicheres Passwort muss bestimmte Kriterien erfüllen, die Sie am einfachsten mit einem Online-Tool überprüfen (Bild G).

Ein sicheres Kennwort sollte als zufällige Folge von 14 oder mehr Zeichen erscheinen und eine Kombination aus Gross- und Kleinbuchstaben, Zahlen und Symbolen enthalten. All diese Kriterien testet der Microsoft Kennwortprüfer (kostenlos, **www.microsoft.com/germany/protect/yourself/password/checker.mspx**). Wenn Sie Ihr Passwort im Kennwortprüfer eintragen, dann zeigt der farbige Balken sogleich dessen Sicherheitsstufe.



Microsoft Kennwortprüfer: Das Online-Tool zeigt, wie sicher ein Passwort ist (Bild G).

Info: USB-Autorun

Ein Tastendruck verhindert automatische Programmstarts beim Anschliessen von USB-Sticks.

PC-Schädlinge verbreiten sich auch über die Autorun-Funktion für automatische Programmstarts vom USB-Stick. Um die Autorun-Funktion zu deaktivieren, halten Sie einfach die Umschalttaste gedrückt, während Sie den USB-Stick einstecken. Dieser Trick funktioniert auch beim Einlegen von CDs und DVDs.

Das Tool warnt Sie künftig bei jedem Programm, das ungefragt einen neuen Autostart einträgt. Markieren Sie *Show one warning message when Internet Explorer Start Pages be changed*. Dann warnt das Tool Sie, wenn die Startseite des IE geändert wird. Auch wenn Sie mit Firefox surfen, ist dies nützlich, um Infektionen mit Adware zu erkennen.

Setzen Sie zuletzt noch ein Häkchen vor *Start this program with Windows Startup*, damit das Tool automatisch startet und Ihren PC vor neuen Startup-Einträgen schützt.

ONLINE-SCANNER

23. Virensuche online

Wenn Sie einen Schädling auf Ihrem PC vermuten, Ihr Virenscanner aber nichts findet, dann verwenden Sie einen oder mehrere Online-Virenscanner.

Eine kommentierte Übersicht kostenloser Online-Scanner finden Sie im Web unter **http://forum.hijackthis.de/showthread.php?t=25893**.

LONG URL PLEASE 0.4.1

24. Gefährliche Kurz-URLs

Über Kurz-URLs ist es für Angreifer ein Leichtes, manipulierte Webseiten zu verschleiern. Eine Firefox-Erweiterung schafft Abhilfe.

Long URL Please 0.4.1 (kostenlos, **www.longurlplease.com** und auf) reduziert die Gefahr, unversehens auf dubiosen oder gefährlichen Websites zu landen. Das Add-on ersetzt Kurz-Adressen durch die wahre Zieladresse und unterstützt 75 Online-Dienste, mit denen sich Kurz-URLs generieren lassen.

NTFS-DATEISYSTEM

25. Unsichtbarer Daten-Safe

Das Dateisystem NTFS unterstützt Alternate Data Streams (ADS). Sie ermöglichen es, Daten unsichtbar an eine Datei anzuhängen.

Hängen Sie zum Beispiel an ein Bild namens *test.jpg* im Ordner *C:* einen geheimen Text an. Dazu öffnen Sie Notepad mit *[Windows R]* und dem Befehl `notepad·C:\test.jpg:tresor`. Die folgende Nachfrage bestätigen Sie mit *Ja*, um den geheimen Datenspeicher an die Bilddatei anzuhängen.

In Notepad tragen Sie nun beliebige Daten ein und sichern diese mit *[Strg S]*, bevor Sie den Editor schliessen. Die angehängten Daten erscheinen nun weder im Windows-Explorer noch auf der Kommandozeile, wenn Sie mit dem Befehl `dir` den Inhalt des Ordners *C:* ausgeben.

Um auf die versteckten Daten zuzugreifen, öffnen Sie Notepad erneut mit *[Windows R]* und dem Befehl `notepad·C:\test.jpg:tresor`. Wenn Sie die geheimen Daten beseitigen möchten, dann löschen Sie diese in Notepad, oder speichern Sie die Datei *test.jpg* auf einem Datenträger mit FAT32-Format.

INTERNET

26. Sichere Passwörter

Mit einem Trick erstellen Sie sichere Passwörter, die Sie sich leicht merken.

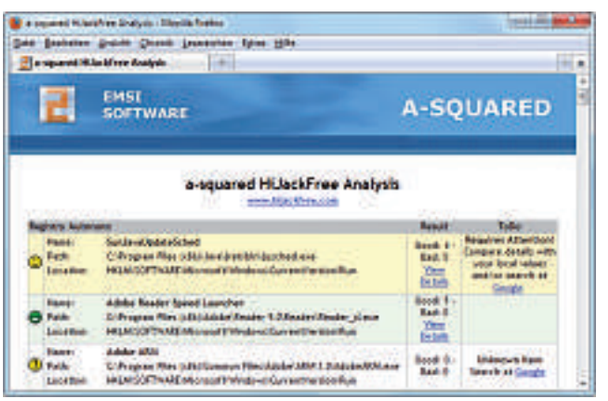
Nehmen Sie zunächst die Anfangszeile eines Liedes oder Gedichts, etwa "Bolle reiste jüngst zu Pfingsten, nach Pankow war sein Ziel", und notieren Sie sich die Anfangsbuchstaben der Wörter, also `BrjzPnPwsZ`. Suchen Sie sich dann eine Zahl aus, die mit einem bestimmten Ereignis verknüpft ist. `1980` etwa ist das Todesjahr von John Lennon. Nun benötigen Sie nur noch ein zufälliges Sonderzeichen wie den Klammeraffen sowie ein Trennzeichen wie das Komma. Fügen Sie alle Elemente zusammen, und Sie erhalten Ihr neues Passwort: `BrjzPnPwsZ,1980,@`.

FILE VERIFIER++ 0.6.2.5822

27. Unsichere Downloads

Prüfen Sie fragwürdige Downloads nicht nur auf Viren. Testen Sie zusätzlich, ob die Datei manipuliert wurde.

Viele Softwarehersteller liefern Ihnen dazu Prüfsummen oder Hash-Werte der angebotenen Downloads. Mit einem Tool wie File Verifier++ 0.6.2.5822 (kostenlos, **www.programmingunlimited.net/siteexec/content.cgi?page=fv** und auf) berechnen Sie die Prüfsumme Ihres Downloads und vergleichen diese mit der des Herstellers. Wenn die beiden Werte voneinander abweichen, dann sollten Sie die Download-Datei umgehend löschen. ■



Hijack Free 3.1.0.22: Das kostenlose Tool erstellt eine Liste gefährlicher Software, die sich in den Autostart-Bereichen Ihres PCs versteckt (Bild F).

Stefan Kuhn/jb