WINMEND FOLDER HIDDEN 1.4.2

Ordner verstecken

Vertrauliche und private Daten lassen sich auf dem PC zuverlässig verbergen. Sie werden sogar unsichtbar.

Winmend Folder Hidden 1.4.2 versteckt einzelne Dateien oder ganze Ordner (kostenlos, www.winmend.com/folder-hidden). Diese lassen sich anschliessend nur noch von Ihnen nutzen oder überhaupt wahrnehmen. Und nur mit einem Passwort lassen sich die versteckten Daten wieder anzeigen (Bild A).

Auch auf Winmend Folder Hidden selbst hat lediglich Zugriff, wer das nach der Installation festgelegte Passwort kennt.

Versteckte Daten: Diese Ordner und Dateien lassen sich nur mit Winmend Folder Hidden 1.4.2 und einem Passwort wieder sichtbar machen (Bild A).

WINDOWS ACTIVITY MONITOR 1.1

Windows überwachen

Ein kleines Tool überwacht im Hintergrund, welche Programme auf Ihrem PC genutzt werden, und erstellt daraus eine Statistik.

Wenn mehrere Personen an Ihrem Rechner arbeiten, ist es interessant zu erfahren, welche Programme wie lange genutzt wurden. Windows Activity Monitor 1.1 startet als Dienst und protokolliert, welches Programm gerade aktiv ist (kostenlos, http://code.google.com/p/wamon und auf). Um die Statistik zu sehen, rufen Sie im Browser die Adresse http://127.0.0.1:57824/stats auf (Bild C).

XP ANTISPY 3.97-10

Windows mundtot machen

Ein Programm verhindert, dass Windows Daten an Microsoft überträgt.

Viele Windows-Komponenten wie der Internet Explorer übertragen – etwa nach einem Absturz – Informationen an Microsoft. Dies läuft meist im Hintergrund ab und niemand ausser Microsoft weiss, welche Daten genau übertragen werden.

Das Tool XP Antispy 3.97-10 sucht nach entsprechenden verräterischen Registry-Einträgen (kostenlos, www.xp-antispy.org/index.php/de/download?func=sellang&iso=de).

Damit lässt sich die Datenübertragung mehrerer gesprächiger Windows-Komponenten wirksam unterbinden, und Ihr Betriebssystem wird dadurch nicht nur sicherer, sondern meistens auch schneller.

NEO'S SAFEKEYS 3

Keylogger austricksen

Keylogger zeichnen Tastatureingaben auf, etwa um Passwörter auszuspähen, und versenden sie über das Internet. Ein Spezial-Tool hebelt die Malware wirksam aus.

Das neue Neo's Safekeys 3 bringt jetzt gleich mehrere Schutzmechanismen mit, um Keylogger aller Art unwirksam zu machen (kostenlos, www.aplin.com.au/neos-safekeys-v3).

Auf DVD

Sie finden Windows Activity Monitor 1.1 auf in der Rubrik "Computer, Sicherheits-Tipps".

Beim Start blendet das Tool eine virtuelle Tastatur ein, über die Sie dann vertrauliche Daten wie Passwörter, PINs und TANs eingeben (Bild B).

Um auch solche Keylogger auszutricksen, die die Zwischenablage auslesen, wird diese zu keinem Zeitpunkt verwendet. Noch ausgefeiltere Keylogger, die Screenshots aufnehmen, haben ebenfalls keine Chance: Neo's Safekeys legt eine unsichtbare Schicht über den gesamten Bildschirm, während es aktiv ist. Der Keylogger erhält bei einem Screenshot dann nur diese Schutzschicht.

Auch die Position des Mauszeigers verrät nichts, da Safekeys jedes Mal an einer anderen Position und in einer anderen Grösse startet.

CAIN & ABEL 4.9.36

Vergessene Passwörter finden

Das universelle Passwort-Recovery-Programm Cain & Abel 4.9.36 liest alle Arten von Passwörtern aus (kostenlos, www.oxid.it/cain.html).

Ganz gleich ob Login-Passwörter oder Zugangsdaten für das E-Mail-Konto: Cain & Abel findet alle Passwörter, die unter Windows oder in Ihrem Netzwerk gespeichert sind. Das Tool verfügt auch über eine Funktion zum Knacken von Passwörtern mittels Brute-Force-, Wörterbuch- oder Kryptografieangriffen.

Hinweis: Einige Antivirenprogramme melden Cain & Abel fälschlicherweise als Schädling.

WINDOWS XP, VISTA UND 7

Kennwortabfrage deaktivieren

Mit der Funktion Ruhezustand wird der aktuelle Systemstatus auf Festplatte gespeichert und der Rechner in einen Akku schonenden Schlafzustand versetzt. Um ein Notebook aus dem Ruhezustand aufzuwecken, ist ein Passwort nötig. Zu Hause ist diese Schutzfunktion aber überflüssig und lässt sich abschalten.

Unter XP wählen Sie dazu "Start, Systemsteuerung, Leistung und Wartung, Energieoptionen". Dort klicken Sie auf "Erweitert" und deaktivieren darin die Option "Kennwort bei Reaktivierung des Computers anfordern".

Bei Windows 7 wählen Sie "Start, Systemsteuerung, System und Sicherheit". Vista hat die entsprechende Einstellung unter "Start, Systemsteuerung, System und Wartung".

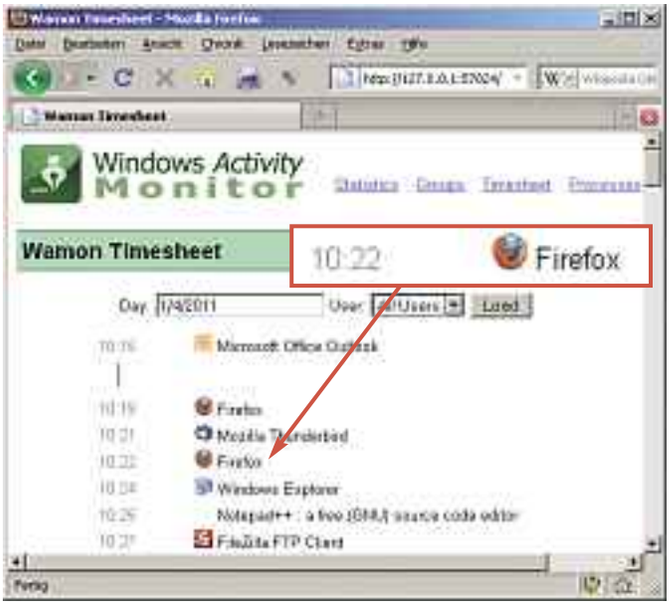
Neo's Safekeys 3: Eine virtuelle Tastatur und weitere Schutzmechanismen lassen Keyloggern keine Chance (Bild B).

Klicken Sie dann auf "Kennwort bei Reaktivierung des Computers anfordern" und wählen Sie die Option "Kennwort ist nicht erforderlich".

WINDOWS XP, VISTA UND 7

Kritische Lücke im Internet Explorer

Eine kritische Sicherheitslücke im Internet Explorer 6 bis 8 ermöglicht es Hackern, Schadcode einzuschleusen, wenn Anwender eine manipulierte Webseite besuchen. Auch Anwendungen wie Mail-Clients, die den IE zur Anzeige von HTML-Code nutzen, können betroffen sein. Ein Exploit nutzt die Schwachstelle bei der Verarbeitung von Cascading Stylesheets (CSS), um die Schutzmechanismen Address Space Layout Randomization (ASLR) und Data Execution Prevention (DEP) zu umgehen. Als Ad-hoc-Hilfe empfiehlt Microsoft diese Fix-it-Lösung: **http://support.microsoft.com/kb/2488013**



Windows Activity Monitor 1.1: Statistiken zeigen, welche Programme wann und wie häufig genutzt wurden (Bild C).

E-MAIL MIT TROJANER

Gefälschtes Microsoft-Update

Deutschsprachige Spam-Mails versprechen Windows-Anwendern ein Update, das "ein Sicherheitsproblem bzgl. Internet Explorer 9 und Firefox 3" beheben will. Die Mails tragen einen Betreff wie "Microsoft Update-Service" und enthalten Links zu gefälschten Seiten wie etwa Microsoft-downloads.de oder Microsoft-patches.de. Die angebliche Update-Datei "WindowsXP-7-Vis-v3-x86-DEU.exe" ist in Wahrheit ein Trojaner. Er wird von aktuellen Virenscannern als Pefsire oder Pilleuz erkannt. **www.phishing-abc.de**

FEHLER IN XP UND VISTA

Vorschau-Bug in Windows

Microsoft warnt vor einem Sicherheitsleck in Windows XP und Vista, das sich dazu missbrauchen lässt, Schadcode auf dem Rechner des Opfers auszuführen. Wenn das Opfer eine manipulierte Webseite oder eine Word- beziehungsweise Powerpoint-Datei öffnet, führt die Darstellung von Vorschaubildern zu einem Pufferüberlauf. Bis zum Erscheinen eines Patches empfiehlt Microsoft, ein bereitgestelltes Fix-it-Tool zu nutzen. Es schliesst die Lücke nicht, verhindert aber, dass sie ausgenutzt wird.
http://support.microsoft.com/kb/2490606 ■

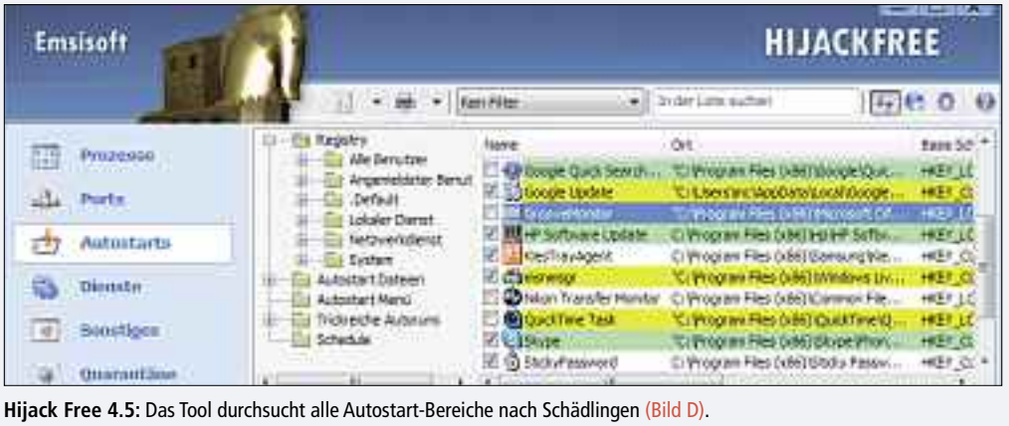
Andreas Dumont

Sicherheits-Tipp des Monats: Schädlinge aufspüren und entfernen

Malware nistet sich oft im Autostart von Windows ein. Ein spezialisiertes Tool spürt sie dort auf.

Hijack Free 4.5 (kostenlos, www.hijackfree.de/de) durchsucht die Autostart-Bereiche von Windows nach Trojanern und entfernt diese.

Über das Icon rechts oben in der Systemleiste starten Sie die Online-Analyse. Wenig später erscheint im Browser eine Liste aller Autostart-Einträge Ihres PCs. Sie gibt detailliert Auskunft, welche Autorun-Einträge, Prozesse oder Add-ons potenziell gefährlich sind. Gelbe oder rote Einträge erfordern Ihre Aufmerksamkeit (Bild D). Diese sollten Sie über "View Details" genauer unter die Lupe nehmen und gegebenenfalls löschen oder deaktivieren.



Hijack Free 4.5: Das Tool durchsucht alle Autostart-Bereiche nach Schädlingen (Bild D).