



| | | | |
|-------------------------|--------------------|----------------------|--------|
| Medientyp: | Fachpresse-Spezial | Auflage: | 360692 |
| Veröffentlichungsdatum: | 01.11.2010 | Verkaufte Auflage: | 228028 |
| Seite : | 174-175 | Verbreitete Auflage: | 231570 |
| AVE: | 16134 | Reichweite: | 490000 |

TIPPS & TRICKS Sicherheits-Tipps

Sicherheits-Tipps

HELIOS LITE 1.005

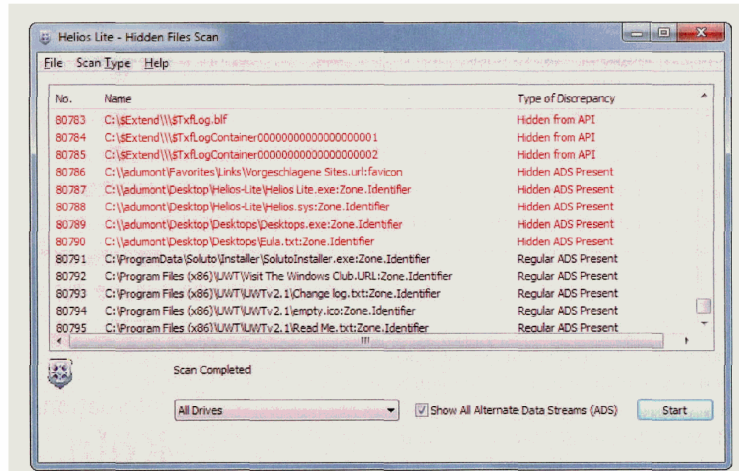
Rootkits jagen

Ein kostenloses Sicherheits-Tool scannt Ihren PC nach Schädlingen, die Rootkit-Techniken verwenden.

Malware mit Rootkit-Technik verbirgt sich tief im System, so dass viele Virens Scanner sie nicht finden. Die spezialisierte Software Helios Lite scannt Ihr System und zeigt alle Dateien, die es für potenziell gefährlich hält (kostenlos, <http://helios.miel-labs.com>).

Starten Sie das Tool mit Administratorrechten. Optional sucht es auch nach Dateien mit alternativen Datenströmen (ADS), in denen sich ebenfalls Malware verbergen kann. In alternativen Datenströmen werden Daten unsichtbar fest an eine Datei gebunden. Der Windows-Explorer zeigt aber weiterhin die ursprüngliche Dateigröße an. Ein Klick auf „Start“ beginnt den Scanvorgang (Bild A).

Viele ADS sind harmlos. Bevor Sie etwas löschen, suchen Sie am besten bei Google nach dem jeweiligen Treffer.



Rootkits aufspüren: Helios Lite 1.005 spürt Malware auf, die sich tief in Ihrem System versteckt (Bild A)

QUICK JAVA 1.7.2

Schalter für Java und Javascript

Java, Javascript und Flash sind Einfallstore für Malware. Setzen Sie diese Techniken nur auf vertrauenswürdigen Webseiten ein.

Um die jeweilige Technik mit einem Mausklick ein- oder auszuschalten, installieren Sie das Firefox-Add-on Quick Java 1.7.2 (kostenlos, <https://addons.mozilla.org/de/firefox/addon/1237> und auf). Es blendet kleine Icons in der Statusleiste ein, die als Schalter dienen und den aktuellen Status anzeigen.

ONLINE-CHECK

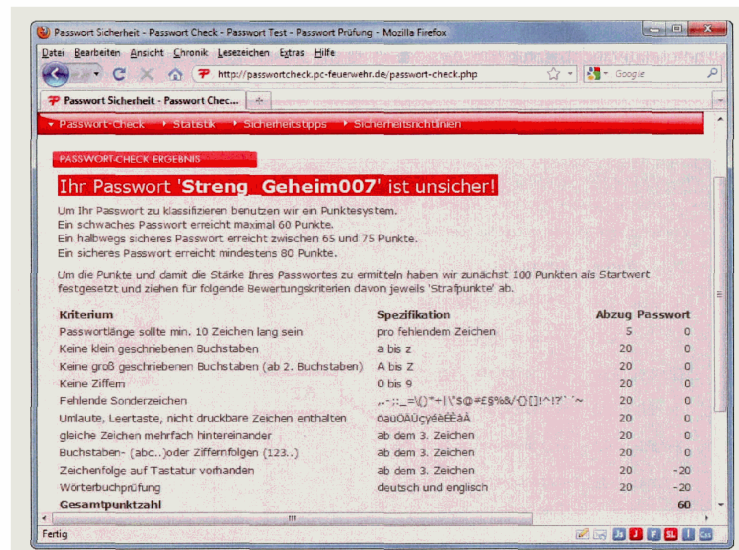
Passwörter prüfen

Wie sicher ein Passwort ist, zeigt Ihnen eine Online-Prüfung.

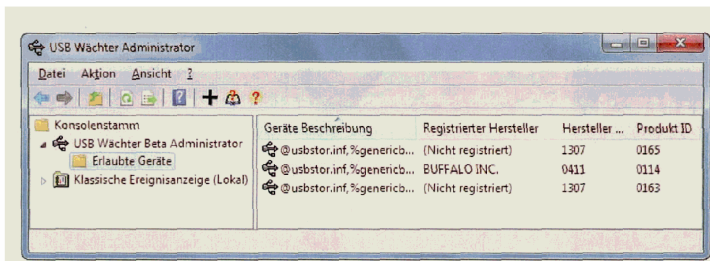
Auf der Webseite <http://passwort-check.pc-feuerwehr.de> lassen Sie ein Passwort nach verschiedenen Kriterien prüfen (Bild A). Maximal sind 100 Punkte zu erreichen. Sichere Passwörter sind mindestens zehn Zeichen lang und verwenden Zahlen, Großbuchstaben und Sonderzeichen.

Auf CD und DVD

Sie finden 7-Zip 9.15 Beta, Adblock Plus 1.2.2, Quick Java 1.7.2 und Restoration 2.5.14 auf in der Rubrik „Tipps & Tricks, Sicherheits-Tipps“.



Passwort-Check: Die Website bewertet, wie sicher ein Passwort ist (Bild B)



Schutz vor fremden USB-Sticks: USB Wächter 0.7.1.130 lässt nur USB-Sticks an Ihrem PC zu, die Sie persönlich freigegeben haben (Bild C)

RESTORATION 2.5.14 Daten retten

Daten, die etwa ein Schädling gelöscht hat, lassen sich mit einem Spezial-Tool wiederherstellen.

Restoration 2.5.14 benötigt keine Installation (kostenlos, www.snapfiles.com/get/restoration.html und auf). Starten Sie das Programm mit Administratorrechten. Anschließend stellen Sie bei „Drives“ das Laufwerk ein, das Sie durchsuchen wollen.

In das Feld darunter lassen sich Teile von Dateinamen angeben. Tragen Sie hier zum Beispiel **EXE** ein, um gezielt nach ausführbaren Programmen zu suchen. Ein Klick auf „Search Deleted Files“ startet die Suche. Sie dauert meist mehrere Minuten.

WINDOWS-STARTMENÜ Verlauf löschen

Im Dialog „Ausführen ...“ im Startmenü speichert Windows alle eingegebenen Befehle und somit auch private Informationen, beispielsweise FTP-Passwörter.

Mit einer kleinen Änderung in der Registry löschen Sie diese Datenspur: Öffnen Sie den Registrierungs-Editor mit der Tastenkombination [Windows R], dem Befehl **regedit** und „OK“. Navigieren Sie zu dem Schlüssel „HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU“. Markieren Sie im rechten Fensterbereich den Befehl, den Sie löschen wollen, und drücken Sie die Eingabetaste.

USB-WÄCHTER 0.7.1.130 PC schützen

Lassen Sie nur solche USB-Sticks an Ihrem PC, die Sie persönlich freigegeben haben.

Malware verbreitet sich häufig über USB-Sticks: Das Tool USB Wächter 0.7.1.130 lässt nur autorisierte USB-Sticks zu (kostenlos, www.trinit-soft.de/usb-waechter).

Um einen USB-Stick in die Liste der vertrauenswürdigen Geräte aufzunehmen (Bild C), klicken Sie auf das Plus-Symbol und danach auf „Weiter“. Stecken Sie jetzt den USB-Stick ein und

setzen Sie ein Häkchen vor dem neuen Eintrag in der Liste. Ein Mausklick auf „Fertig stellen“ schließt den Vorgang ab.

PACKPROGRAMME Archive sicher verschlüsseln

Die meisten Packprogramme bieten die Möglichkeit, Archive mit einem Passwort zu verschlüsseln. Oft ist das nicht sicher.

Je nach Packformat werden die Passwörter mit einem anderen Algorithmus verschlüsselt. Insbesondere ältere Zip-Programme verwenden einen Algorithmus, der verhältnismäßig leicht zu knacken ist.

Sichere Packformate sind beispielsweise RAR und 7z. Letzteres verwendet der Packer 7-Zip 9.15 Beta (kostenlos, www.7-zip.org und auf). Dabei wird das Archiv mit dem Algorithmus AES verschlüsselt, der bis heute als unknackbar gilt. ■

Andreas Dumont

Sicherheits-Tipp des Monats: Adblock Plus 1.2.2

Zwei zusätzliche Filter für den Werbeblocker Adblock Plus 1.2.2 schützen in Firefox vor spionierenden Webseiten (kostenlos, <https://addons.mozilla.org/de/firefox/addon/1865> und auf).

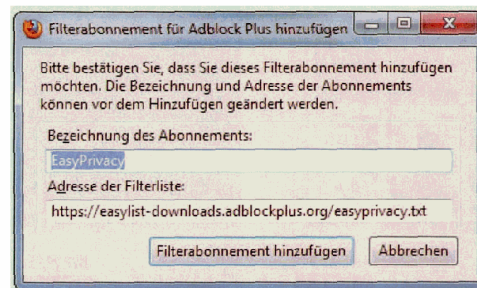
Die beiden Filter Easy List und Easy Privacy schützen Firefox-Nutzer vor Bannerwerbung, Tracking-Cookies und Spionage-Techniken.

Falls Sie Adblock Plus noch nicht verwenden, installieren Sie zunächst diese Erweiterung.

Anschließend abonnieren Sie die beiden zusätzlichen Filter. Dazu surfen Sie zu der Webseite <http://easylist.adblockplus.org>. Klicken

Sie dort bei den zwei Einträgen „Easy List“ und „Easy Privacy“ jeweils auf „Add to ABP“ und bestätigen Sie mit einem Klick auf „Filterabonnement hinzufügen“ (Bild D).

Um Updates brauchen Sie sich nicht zu kümmern: Adblock Plus aktualisiert die Filter automatisch.



Easy Privacy: Der Filter für Adblock Plus schützt vor Tracking-Cookies und anderen Schnüffeltechniken (Bild D)