Online PC EXTRA

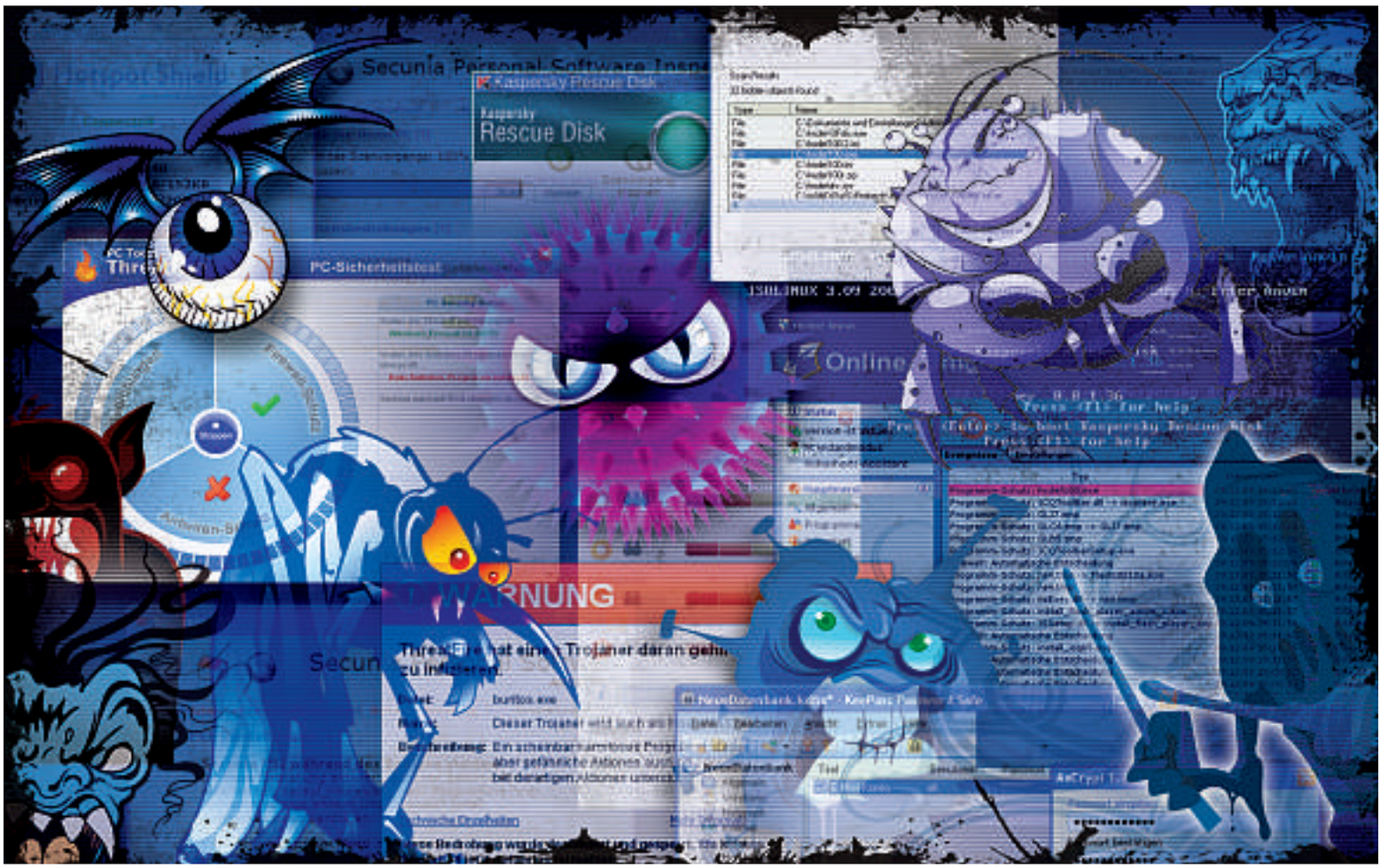
- Die besten Security-Tools S. 28
- eBook Sicherheit S. 35
- Datenspuren vom PC beseitigen S. 36

FÜR XP, VISTA, WINDOWS 7

Ratgeber Sicherheit

- Zehn häufige Sicherheitsprobleme und was man dagegen tun kann S. 28
- Cobian Backup sichert Ihre Daten S. 33
- Wie Ihr PC Sie verrät und wie Sie die Spionage verhindern können S. 34

NEU: PERSONAL SOFTWARE INSPECTOR S. 33



Grosser Ratgeber: Computer-Sicherheit

Was ist das beste Tool gegen Rootkits? Was macht man gegen Trojaner? Und wie bekämpft man eigentlich brandneue Schädlinge, zu denen es noch keine Signatur gibt?

Windows-Nutzer sind zahlreichen Gefahren im Internet ausgesetzt. Die grösste Bedrohung sind Schädlinge, die unbemerkt den PC infizieren und anschliessend den Benutzer ausspionieren sowie private Dokumente oder gar Bankdaten klauen.

Ist ein Trojaner, ein Rootkit oder ein Wurm erst einmal eingedrungen, ist es oft schwer, den Übeltäter wieder loszuwerden. Dieser Artikel beschreibt zehn häufige Sicherheitsprobleme und zeigt, wie Sie sie lösen.

Die verwendeten Sicherheits-Tools stellt jeweils ein dazugehöriger Kasten vor. So finden Sie das Tool zu Problem 1 im Kasten "Tool 1", das beste Programm zu Problem 2 im Kasten "Tool 2" und so weiter.

Kompakt

- *Der Artikel beschreibt zehn häufige Sicherheitsprobleme und zeigt, was man dagegen unternehmen kann.*
- *Alle vorgestellten Sicherheits-Tools finden Sie auf der Heft-DVD oder kostenlos zum Download im Internet.*

Ein spezieller Tipp ist Tool Nr 10. Cobian Backup ist weniger ein klassisches Backup-Tool als ein Dienst, der sich vollautomatisch um das Sichern Ihrer Daten kümmert.

Ein Assistent hilft bei der Planung der gewünschten Datensicherung. Cobian Backup unterstützt auch inkrementelle Backups, bei denen nicht die gesamten Daten, sondern nur veränderte Dateien übertragen werden.

Problem 1: Rootkits

Wie kann ich mir sicher sein, dass sich kein Rootkit auf meinem PC versteckt?

Lösung: Das Mittel der Wahl gegen Rootkits ist das Tool Rootkit Buster 2.80 Beta von Trend Micro. Den Rootkit Buster brauchen Sie nicht zu installieren. Das Programm ist nach einem Doppelklick sofort einsatzbereit. Ein Klick auf *Scan Now* startet die Suche nach Rootkits.

Die Option *File Streams* sollten Sie nicht anhaken. Das Tool würde dann auch verborgene ADS-Daten (Alternate Data Streams) aufspüren. Diese Technik wird zwar gelegentlich auch von Schädlingen verwendet. Allerdings versieht Windows heruntergeladene Dateien mit einem ADS-Hinweis. Diese machen die Scan-Ergebnisse teils sehr unübersichtlich.

Wenn Rootkit Buster ein Rootkit entdeckt, füllt sich das Fenster *Scan Results* meist mit mehreren Einträgen. Das liegt daran, dass ein Rootkit oft mehr als nur seine ausführbare Datei versteckt. Markieren Sie jeden Eintrag in der Liste, den Sie löschen wollen, mit der Maus und klicken Sie auf *Delete Selected Items*. Mehrere Einträge markieren Sie, indem Sie die Taste *[Strg]* gedrückt halten. Zur Bereinigung ist am Ende ein Neustart Ihres Rechners nötig.

Problem 2: Trojaner

Wie gehe ich vor, wenn ich den Verdacht habe, dass ein oder mehrere Trojaner meinen PC verseucht haben?

Lösung: Meist findet sich auf einem infizierten Rechner mehr als nur ein einziger Trojaner oder Virus. Sehr effektiv gegen diese Plage ist Anti-Malware 1.44 von Malwarebytes.

Die Installation des Reinigungs-Tools ist schnell erledigt. Belassen Sie im letzten Dialog die beiden Häkchen vor *Aktualisiere Malwarebytes' Anti-Malware* sowie *Malwarebytes' Anti-Malware starten* und klicken Sie dann auf *Fertig stellen*. Nun lädt das Programm die aktuellen Signaturen über das Internet.

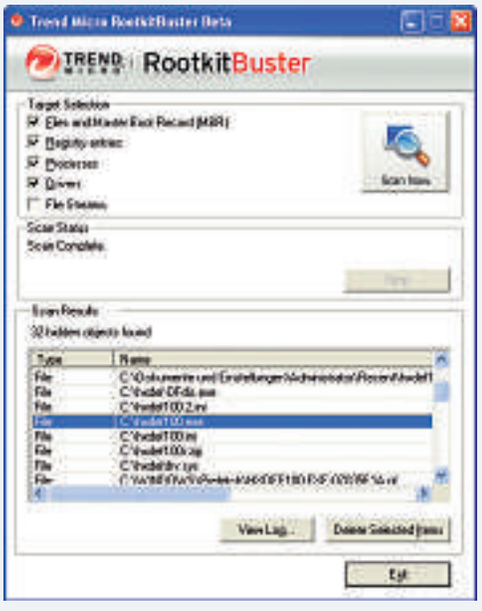
Sobald die Oberfläche von Anti-Malware gestartet ist, markieren Sie unter *Scanner* die Option *Vollständigen Suchlauf durchführen* und klicken auf *Scan*. Markieren Sie in dem kleinen Fenster, das sich automatisch ▶

Tool 1: Rootkit Buster 2.80 Beta

Rootkit Buster sucht in noch so verborgenen Dateien Ihrer Festplatte blitzschnell nach aktiven Rootkits und entfernt diese zuverlässig.

Rootkit Buster 2.80 Beta (kostenlos, **www.trendmicro.com/download/rbuster.asp** und auf ⊙) sucht in verborgenen Dateien, in Registry-Einträgen, Prozessen und sogar in Treibern sowie dem Master Boot Record (MBR) der Festplatte nach Rootkits (Bild A). Spürt das Tool einen dieser besonders heimtückischen Schädlinge auf, bietet er eine Desinfizierung an.

Die aktuelle Beta-Version unterstützt Windows 2000, XP, Vista und 7, aber noch keine 64-Bit-Systeme. Rootkit Buster muss nicht installiert werden und funktioniert deswegen auch als Sofort-Tool von einem USB-Stick.



Rootkit Buster 2.80 Beta: Der Rootkit-Jäger prüft in der neuesten Version sogar den MBR der Festplatte auf Rootkits (Bild A).

Tool 2: Anti-Malware 1.44

Das Sicherheits-Tool ist wegen seiner besonders schnellen und gründlichen Suche das beste Werkzeug gegen Trojaner.

Anti-Malware 1.44 (kostenlos, **www.malwarebytes.org/mbam.php** und auf ⊙) scannt einen möglicherweise verseuchten PC nach Trojanern, Rootkits, Dialern, Spyware und sonstiger Malware. Oft findet das Tool mehr als einen Schädling (Bild B).

Der Hersteller bietet neben der kostenlosen Variante auch eine kostenpflichtige Version für 25 Dollar an, die automatische Updates, zeitgesteuerte Scans und einen Hintergrundwächter enthält. Zur Bereinigung eines verseuchten Rechners genügt jedoch in der Regel die kostenlose Version. Anti-Malware belastet die Systemressourcen nur unwesentlich. Das Tool funktioniert unter Windows 2000, XP, Vista und 7, sowohl in 32 Bit als auch in 64 Bit.

Anti-Malware 1.44: Findet oft mehr als nur einen Schädling (Bild B).

öffnet, alle zu prüfenden Laufwerke und bestätigen Sie mit *Scan starten*.

Nachdem der Scan durchgelaufen ist, klicken Sie auf die Schaltflächen *OK* sowie *Ergebnisse anzeigen*. Schliessen Sie dann alle geöffneten Anwendungen, bevor Sie mit *Entferne Auswahl* alle gefundenen Schädlinge in Quarantäne verschieben.

Problem 3: Schädlinge mit Selbstschutz

Was mache ich gegen Schädlinge, die für meinen Virenscanner unsichtbar sind und die er deswegen nicht entfernen kann?

Lösung: Die beste Methode, den PC einer gründlichen Tiefenreinigung zu unterziehen, ist der Einsatz einer bootfähigen Antiviren-CD wie der Rescue Disk 8.8.1.36 von Kaspersky. Brennen Sie die ISO-Datei der Rescue Disk mit einem Programm wie Imgburn 2.5 (kostenlos, **www.imgburn.com** und auf) auf eine CD. Sie finden die ISO-Datei auf der Heft-DVD oder zum Download unter **http://devbuilds.kaspersky-labs.com/devbuilds/RescueDisk**. Die Datei heisst *kav_rescue_2008.iso*. Starten Sie Ihren PC von dieser Scheibe.

Drücken Sie die Eingabetaste, wenn das Boot-Menü der Rescue Disk erscheint. Sobald die grafische Oberfläche des Kaspersky-Virenscanners geladen ist, beginnt die Software mit der Aktualisierung der Signaturen über das Internet. Das funktioniert jedoch nur, wenn Ihr Router mit DHCP (Dynamic Host Control Protocol) arbeitet.

Setzen Sie nun je ein Häkchen vor die Partitionen, die das Programm durchsuchen soll. Den eigentlichen Suchvorgang starten Sie mit *Start Scan*.

Zusätzliche Optionen finden Sie oben rechts unter *Settings*. Standardmässig sucht der

Tool 3: Kaspersky Rescue Disk 8.8.1.36

Die bootfähige Live-CD bekämpft auch Schädlinge, die sich erfolgreich vor dem bereits installierten Virenscanner verstecken.

Die Rescue Disk 8.8.1.36 (kostenlos, **www.kaspersky.de** und auf) ist eine bootfähige Live-CD, auf der sich neben einem Linux-System auch der Virenscanner von Kaspersky befindet.

Wenn Sie Ihren PC von dieser Live-CD starten, können sich Windows-Schädlinge nicht aktivieren und vor dem Scanner verbergen. Auf diese Weise lassen sich auch besonders hartnäckige Schädlinge einfach entfernen (Bild C).

Im Gegensatz zu anderen Antiviren-CDs ist die Variante von Kaspersky besonders leicht zu bedienen und erfordert vom Anwender keinerlei Linux-Kenntnisse.

Rescue Disk ist mehrsprachig. Zurzeit werden in der Version 8.8.1.36 18 Sprachen unterstützt.

Rescue Disk 8.8.1.36: Die Live-CD startet Linux als Betriebssystem und bereinigt Windows (Bild C).

Virenscanner nicht innerhalb von Archiven nach Schädlingen. So spart er Zeit. Sicherer ist es jedoch, die Suche in Archiven ebenfalls zu aktivieren. Klicken Sie dazu auf *Settings* und dann bei *Scan* noch einmal auf *Settings*. Setzen Sie das Häkchen vor *Scan archives* und bestätigen Sie zwei Mal mit *OK*.

Problem 4: Brandneue Schädlinge

Kein Virenscanner erkennt 100 Prozent aller Schädlinge, besonders neue, unbekannte Viren werden oft übersehen. Was kann man dagegen unternehmen?

Lösung: Selbst laufend aktualisierte Virenscanner haben nur Erkennungsquoten im Bereich zwischen 95 und 99 Prozent. Optimal ist deswegen ein zusätzlicher Schutz mit Threatfire 4.7.0.11. Diese Zusatzsoftware zu einem herkömmlichen Virenscanner erkennt auch unbekannte Schädlinge an verdächtigem Verhalten.

Die Installation lässt sich schnell durchführen. Entfernen Sie jedoch während des Setups das Häkchen vor *Installieren Sie die kostenlose Google Toolbar mit Threatfire*, wenn Sie diese Toolbar nicht wollen.

Nach dem Setup schlägt das Tool einen Sicherheits-Check vor, den Sie mit *Start Scan* starten sollen. Die Ergebnisse dieses Scans können Sie aber ignorieren, da ein Klick auf *Fix Now* Sie nur auf die Webseite des Herstellers leitet, der Ihnen dort ein Tool verkaufen will.

Prinzipiell können Sie Threatfire nach der Installation sich selbst überlassen. Das Programm überwacht Ihren PC unauffällig im Hintergrund und meldet sich nur, wenn es eine Bedrohung erkannt hat.

Zusätzlich bietet das Schutz-Tool einen Scan an, bei dem die Festplatte gezielt nach Rootkits und anderen Bedrohungen durchsucht wird.

Problem 5: Gefährliche Webseiten

Wie kann ich mich vor Webseiten schützen, die versuchen, meine Bankdaten zu klauen oder meinen PC zu verseuchen?

Lösung: Einen optimalen Schutz bietet die Browser-Erweiterung Web of Trust 20091028 – kurz WOT –, die jede besuchte Webseite mit einer internationalen Datenbank bekannter gefährlicher Adressen vergleicht. Die Einträge in dieser Datenbank werden von allen Nutzern gepflegt.

Nach der Installation im Browser blendet die Erweiterung links neben dem Adressfeld einen neuen Button ein. Je nachdem, ob die besuchte Seite seriös oder gefährlich ist, ändert sich die Farbe dieser Schaltfläche. Grün bedeutet keine Gefahr, während Rot auf eine riskante Seite hinweist. Von dieser Seite sollten Sie weder Dateien herunterladen noch sollten dort persönliche Daten eingegeben werden.

Tool 4: Threatfire 4.7.0.11

Das Tool schützt, wenn der Virenscanner wegen einer fehlenden Signatur versagt.

Eigentlich soll man ja nicht zwei Hintergrundwächter verwenden. Threatfire 4.7.0.11 (kostenlos, **www.threatfire.com/de** und auf CD) ist mit seiner verhaltensbasierten Erkennung jedoch die ideale Ergänzung zu einem normalen Virenscanner und läuft in den meisten Fällen problemlos nebenher. Threatfire muss nur installiert werden. Anschliessend passt das Tool unauffällig auf.

Eine verhaltensbasierte Suche schützt auch bei neuen, bislang unbekannten Gefahren. Threatfire erkennt einen Schädling etwa daran, dass er mehrere Kopien von sich an verschiedenen Orten auf der Festplatte ablegt oder dass er Tastatureingaben mitschneidet und über das Internet versendet. Treffen mehrere verdächtige Eigenschaften zusammen, schlägt das Tool Alarm (Bild D). Findet Threatfire einen Schädling, haben Sie anschliessend die Möglichkeit, ihn zu löschen.

Threatfire 4.7.0.11: Das Tool erkennt Schädlinge an ihrem Verhalten (Bild D).

Problem 6: Würmer und Hacker

Wie verhindere ich, dass sich Würmer oder Hacker heimlich und unbemerkt auf meinem PC einschleichen?

Lösung: Würmer und Hacker greifen meist von aussen auf einen PC zu. Dagegen schützt am besten eine zuverlässige Firewall, wie sie in den meisten DSL-Routern enthalten ist, oder eine Desktop-Firewall wie Online Armor Free 4.0.0.15.

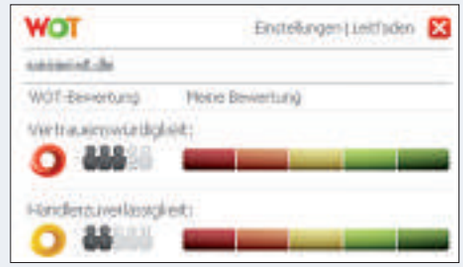
Führen Sie nach der Installation zuerst den Einrichtungsassistenten aus. Die markierte Option, alle aktuell vorhandenen Programme als sicher einzustufen, birgt jedoch das Risiko, dass ein bereits eingedrungener Schädling in Zukunft ungehindert mit dem Internet kommuniziert. Das Häkchen an dieser Stelle sollte deswegen entfernt werden. Der Einrichtungsassistent unterzieht Ihren PC anschliessend einer mehrstufigen Überprüfung.

Nach einem Neustart des Computers beendet die Firewall die Einrichtung. Das dauert etwa zwei Minuten. Danach kann der PC normal genutzt werden. Online Armor Free nervt relativ selten mit Warnmeldungen. Trotzdem sollten Sie gelegentlich die Ereignisanzeige des Programms überprüfen. Sie finden sie nach einem Doppelklick unten rechts auf das Schild-Icon unter *Ereignisse*.

Tool 5: WOT

Die Erweiterung für Firefox und Internet Explorer zeigt mit Ampelfarben, ob eine Webseite harmlos oder gefährlich ist.

Der beste Schutz gegen Internetbetrüger ist ein Tool, das gefährliche Webseiten bereits beim Besuch erkennt und vor ihnen warnt: Web of Trust 20091028 (kostenlos, **www.mywot.com/de** und auf CD) ist ein kostenloses Add-on für Firefox und den Internet Explorer, das jede besuchte Seite mit einer Datenbank vergleicht (Bild E). Diese Datenbank wird von allen Nutzern von Web of Trust gepflegt.



Web of Trust 20091028: Die Browser-Erweiterung warnt vor gefährlichen Webseiten (Bild E).

Problem 7: Dateien verschlüsseln

Ich benutze Truecrypt, um verschlüsselte Container anzulegen. Aber wie verschlüssele ich eigentlich einzelne Dateien oder Ordner?

Lösung: Einzelne Dateien verschlüsseln Sie am besten mit einem Spezial-Tool wie Axcrypt 1.7.1878 Beta. Direkt nach der Installation ist das Tool sofort einsatzbereit. Klicken Sie mit der rechten Maustaste auf eine Datei, die Sie sichern wollen, und wählen Sie *AxCrypt, Verschlüsseln* aus. Es öffnet sich ein Axcrypt-Fenster, in dem Sie ein Passwort vergeben. Axcrypt ersetzt die Datei anschliessend durch eine verschlüsselte Version.

Wenn Sie stattdessen ein unverschlüsseltes Original behalten wollen, wählen Sie *Axcrypt, Kopie verschlüsseln* aus. Der dritte Menüpunkt *Kopie als .EXE verschlüsseln* erstellt eine portable Datei, die auch auf einem Rechner entschlüsselt werden kann, auf dem das Programm Axcrypt nicht installiert ist. Das ist beispielsweise dann praktisch, wenn Sie eine geheime Datei per E-Mail an einen Bekannten versenden wollen. ▶

Mehrere Dateien, die Sie verschlüsseln wollen, packen Sie am besten zuerst in ein ZIP-Archiv. Ebenso wie bei einem Ordner, den Sie mit der Maus markieren, erstellt Axcrypt sonst lauter einzelne verschlüsselte Dateien.

Zum Entschlüsseln genügt ein Doppelklick oder ein Rechtsklick auf eine mit Axcrypt behandelte Datei. Nach der Eingabe des Passworts ersetzt das Tool die verschlüsselte Version durch das unverschlüsselte Original.

Problem 8: Unsichere Passwörter

Passwörter sollen lang sein, sollen Sonderzeichen und Ziffern enthalten und am besten noch regelmässig geändert werden. Wie kann man da noch den Überblick behalten?

Lösung: Das perfekte Programm, um die Kontrolle über die eigenen Passwörter zu behalten, ist Keepass 2.09. Entpacken Sie nach der Installation zuerst die deutsche Sprachdatei (kostenlos, **www.keepass.info/translations.html** und auf) in den Installationsordner von Keepass. Starten Sie dann das Programm und wählen Sie *View, Change Language…* aus, markieren Sie *German* und bestätigen Sie abschliessend mit *Ja*.

Legen Sie nun eine neue Datenbank für Ihre Passwörter mit *[Strg N]* an und vergeben Sie einen Namen für diese Datei im KDBX-Format. Im folgenden Fenster legen Sie das Master-Passwort fest, das den Zugriff auf alle in Keepass hinterlegten Zugangsdaten und Passwörter sichert. Bestätigen Sie anschliessend zwei Mal mit *OK*.

Jetzt sehen Sie im linken Bereich mehrere Beispielkategorien, die Sie beibehalten oder mit einem Klick der rechten Maustaste verändern können. Markieren Sie eine Kategorie und drücken Sie *[Einfg]*, um einen neuen Eintrag anzulegen. Vergeben Sie einen *Titel* wie `E-Mail-Konto` und füllen Sie danach die zusätzlichen Felder aus.

Die beiden Passwortfelder hat Keepass bereits mit einem zufällig erstellten Passwort gefüllt. Wie es lautet, sehen Sie, wenn Sie rechts daneben auf den kleinen Button mit den drei schwarzen Kreisen klicken.

Verwenden Sie das vorgeschlagene Passwort oder tragen Sie Ihr bisher verwendetes Kennwort in die beiden Felder ein. Ein neues Passwort erstellen Sie mit einem Klick auf das Schlüssel-Icon unter dem Button mit den drei schwarzen Kreisen. Es öffnet sich das Fenster des Passwort-Generators. Sobald Sie alle benötigten Informationen eingetragen haben, schliessen Sie den Eintrag mit *OK*. Wenn Sie jetzt Keepass beenden, fragt Sie das Programm, ob Sie die Änderungen in der Datenbank speichern wollen. Bestätigen Sie mit *Ja*.

Beim nächsten Start von Keepass geben Sie das Master-Passwort ein, um auf die hinterlegten Passwörter zuzugreifen. Markieren Sie anschliessend einen Eintrag und drücken Sie *[Strg C]*, um das Kennwort direkt in die Zwischenablage zu kopieren.

Die verschlüsselte Passwortdatei sollten Sie gelegentlich auf einem anderen Datenträger sichern, damit sie nicht verloren geht.

Problem 9: Veraltete Software

Auf einem PC finden sich schnell ein Dutzend oder mehr Programme, die wegen Sicherheitslücken laufend aktualisiert werden müssen. Wie lässt sich dieser Vorgang erleichtern?

Lösung: Der Personal Software Inspector 1.5.0.1 prüft installierte Software und zeigt Updates an. Beachten Sie bei der Installation, dass Sie die Option *Privater Gebrauch* auswählen.

Nachdem das Tool gestartet ist, beginnt es sofort mit der Suche nach veralteten Programmen. Im Feld *Sicherheitsbedrohungen* listet Software Inspector anschliessend alle Anwendungen auf, die dringend aktualisiert werden sollten. Am einfachsten geht dies, indem Sie in der Spalte *Lösung* auf die blaue Kugel mit dem weissen Pfeil klicken. Teils verbirgt sich dahinter ein direkter Download-Link, teils eine Webseite mit einer Download-Möglichkeit. Gelegentlich sind nur englischsprachige Updates verlinkt. In diesem Fall empfiehlt es sich, die Webseite des Anbieters aufzurufen und von dort die neueste deutsche Version herunterzuladen.

Klicken Sie oben rechts auf *ERWEITERT*, um die Profi-Ansicht von Personal Software Inspector zu aktivieren. Hier finden Sie unter

Tool 6: Online Armor Free 4.0.0.15

Die Desktop-Firewall nervt nicht jeden Augenblick mit Nachfragen, bietet aber trotzdem einen hohen Schutz vor Angriffen aus dem Internet.

Online Armor Free 4.0.0.15 (kostenlos, **www.tallemu.de/products-online-armor-free.php** und auf) schützt den PC vor Angriffen aus dem Internet und aus dem lokalen Netz. Im Vergleich zur in Windows integrierten Firewall bietet Online Armor Free weit mehr Einstellmöglichkeiten, Zusatzoptionen und Protokollfunktionen (Bild F). Im laufenden Betrieb macht sich Online Armor Free lediglich anhand eines Icons im Systemtray bemerkbar. Will ein unbekanntes Programm auf das Internet zugreifen, warnt die Software.

Der Hersteller bietet auch zwei kostenpflichtige Varianten an, die Zusatzfunktionen enthalten. Wer nur eine Firewall benötigt, kann bedenkenlos zur kostenlosen Version greifen.

Online Armor Free 4.0.0.15: Die Firewall blockiert Würmer und Hacker (Bild F).

Tool 7: Axcrypt 1.7.1878 Beta

Axcrypt ermöglicht die blitzschnelle Verschlüsselung einzelner Dateien mittels AES-Algorithmus und einer Schlüssellänge von 128 Bit.

Der Klassiker zum Verschlüsseln von Daten ist Truecrypt 6.3a (kostenlos, **www.truecrypt.org** und auf). Das Open-Source-Programm ist aber ungeeignet, wenn man nur schnell eine einzelne Datei verschlüsseln will (Bild G).

Ideal für diesen Zweck ist Axcrypt 1.7.1878 Beta (kostenlos, **www.axantum.com/axCrypt** und auf), das sogar verschlüsselte, selbstextrahierende Archive erstellt, die Sie per Mail versenden können. Auf dem Zielrechner muss Axcrypt dann nicht installiert sein. Nur das Passwort müssen Sie über einen anderen Weg übertragen, zum Beispiel per Telefon.

Das in sieben Sprachen erhältliche Programm verfügt auch über einen integrierten Dateishredder.

Axcrypt 1.7.1787: Anders als Truecrypt erstellt Axcrypt keine verschlüsselten Container, sondern es verschlüsselt einzelne Dateien (Bild G).

Unsicher alle dringend zu aktualisierenden Programme und unter *Veraltet* die Anwendungen, bei denen ein Update nicht so eilig ist.

Problem 10: Schutz vor Datenverlust

Wie verhindere ich – möglichst automatisiert –, dass meine privaten Daten bei einem Angriff durch einen Schädling verloren gehen?

Lösung: Zum Schutz vor Gefahren aus dem Internet gehört auch die Sicherung Ihrer wichtigsten Daten. Sowohl bei einem Virenbefall als auch bei einem Systemfehler sind Ihre Daten dann vor Verlust geschützt. Cobian Backup 9.5.1.212 bietet Funktionen wie automatische Backups und sichert Dateien auf Wunsch sogar in einen FTP-Ordner. Installieren Sie Cobian Backup und belassen Sie bei der Frage nach dem *Installationstyp* die Auswahl auf *Windows-Dienst*. Das Programm startet in Zukunft automatisch im Hintergrund als Windows-Dienst. Dieser Dienst kümmert sich dann ressourcenschonend um die von Ihnen eingerichteten Backup-Aufträge.

Klicken Sie nach dem Setup doppelt auf das Fliegenpilz-Icon unten rechts im System-Tray, um die Bedienoberfläche zu öffnen. Legen Sie zuerst einen Backup-Auftrag mit *Sicherung, Neue Sicherung* an. Setzen Sie dann in dem neuen Fenster ein Häkchen vor *Volumenschattenkopie verwenden*. Das Programm sichert damit auch gerade geöffnete Dateien. Stellen Sie dann den *Sicherungstyp* auf *Inkrementell* um, damit Cobian Backup nicht immer alle Dateien erneut komplett sichert. Bei einer inkrementellen Sicherung überträgt das Tool nur veränderte Daten. Das spart Bandbreite und Zeit.

Markieren Sie danach oben links *Dateien* und klicken Sie unter *Quelle* auf *Hinzufügen*. Wählen Sie *Verzeichnis* aus, um Ordner zur Sicherung hinzuzufügen, und *Dateien*, um einzelne Dateien zu sichern. Sobald Sie dies erledigt haben, legen Sie mit *Hinzufügen* bei *Ziel* fest, wohin Ihre Daten gesichert werden sollen. Das Hinzufügen zu sichernder Dateien lässt sich auch per Drag and Drop aus dem Windows-Explorer erledigen.

Bei *Zeitplaner* stellen Sie ein, wann und wie oft das Backup durchgeführt werden soll. Bei *Komprimierung* legen Sie fest, ob die Dateien gepackt werden sollen. Sobald Sie mit allen Einstellungen zufrieden sind, schliessen Sie die Konfiguration mit *OK* ab.

Der Backup-Auftrag taucht nun im Hauptfenster auf. Wählen Sie ihn aus und klicken Sie auf das Diskettensymbol. Bestätigen Sie das Info-Fenster mit *OK*, um das erste Backup zu starten. Sicherungsaufträge mit Zeitplan führt das Programm selbstständig zum angegebenen Zeitpunkt aus. Prüfen Sie bei jedem neu erstellten Sicherheitsauftrag, ob auch alle Dateien wie vorgesehen gespeichert wurden. Nichts ist so fatal wie sich auf ein fehlerhaftes Daten-Backup zu verlassen. ■

Andreas Th. Fischer/jb

Tool 9: Personal Software Inspector 1.5.0.1

Das Tool findet alte Programme auf Ihrem PC. Der Hersteller Secunia hat sich auf Sicherheitslücken in Software spezialisiert.

Der Personal Software Inspector 1.5.0.1 (kostenlos für Privatanwender, **www. secunia.com/vulnerability_scanning/personal** und auf DVD) prüft, welche Software auf einem PC installiert ist und in welcher Version (Bild I).

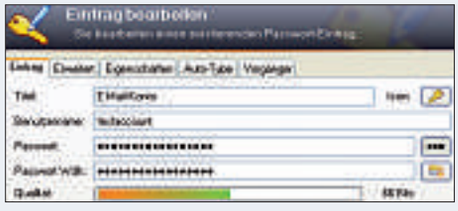
Die Ergebnisse vergleicht das Tool mit einer gigantischen Datenbank, in der Secunia alle bekannten Sicherheitslücken gespeichert hat. Anschliessend präsentiert das Programm dem Anwender Listen mit Programmen, die umgehend aktualisiert werden sollten, und solchen, bei denen ein Update nicht sicherheitsrelevant ist.

Software Inspector 1.5.0.1: Der Update-Wächter zeigt an, welche installierten Programme dringend aktualisiert werden sollten (Bild I).

Tool 8: Keepass

Keepass ist der beste kostenlose Passwortmanager, der Passwörter in einer verschlüsselten Datenbank sichert.

Keepass 2.09 (kostenlos, **www.keepass.info** und auf DVD) schützt Zugangsdaten und Passwörter vor fremdem Zugriff. Das Tool speichert alle Daten in einer verschlüsselten Datei, die mit einem Master-Passwort gesichert ist (Bild H). Alle relevanten Daten verbirgt das Tool zudem hinter Sternchen, so dass selbst ein Keylogger, der heimlich Screenshots anfertigt, keinen Zugriff auf die Passwörter erhält.



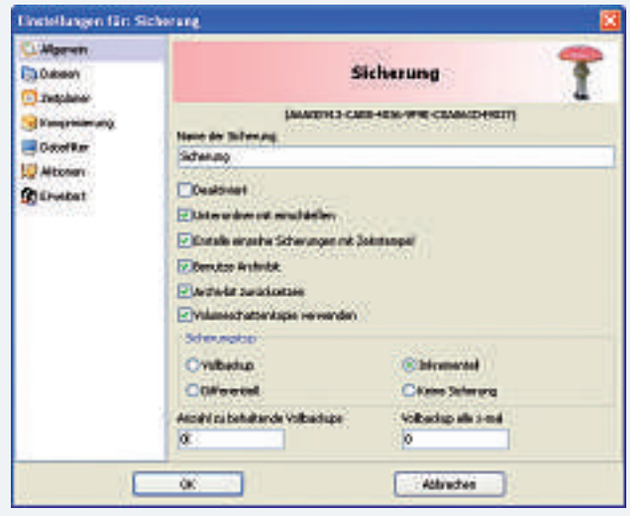
Keepass 2.09: Für jedes zu sichernde Passwort legen Sie einen Eintrag an. Alle Kennwörter sind mit einem Master-Passwort gesichert (Bild H).

Tool 10: Cobian Backup 9.5.1.212

Cobian Backup ist weniger ein klassisches Backup-Tool als ein Dienst, der sich vollautomatisch um das Sichern Ihrer Daten kümmert.

Cobian Backup 9.5.1.212 (kostenlos, **www.educ.umu.se/~cobian/cobianbackup.htm** und auf DVD) sichert beliebige Dateien und Verzeichnisse auf Ihrem PC. Als Speicherort eignet sich eine andere Partition auf dem PC, eine externe Festplatte und sogar ein nur über das Internet erreichbarer FTP-Speicher. Damit Ihre Daten dort nicht von Fremden ausspioniert werden, lassen sie sich auf Wunsch auch gleich beim Übertragen verschlüsseln.

Der Entwickler von Cobian Backup hat das Programm weniger als klassisches Backup-Tool konzipiert, sondern mehr als automatischen Dienst, der sich im Hintergrund um die Sicherung Ihrer Daten kümmert. Ein Assistent hilft bei der Planung der gewünschten Datensicherung (Bild J). Cobian Backup unterstützt auch inkrementelle Backups, bei denen nur veränderte Dateien übertragen werden.



Cobian Backup 9.5.1.212: Ein Assistent hilft bei der Planung der gewünschten Datensicherung. Der Rest erfolgt automatisch (Bild J).