Das Computer-Magazin

c.om! SONDERHEFT

8270

Digitale Version ohne Datenträger

Nur 6,– €

Microsoft Software Center 2.0

Über 200 Vollversionen von Microsoft
S. 68

5/2011

Mai, Juni, Juli 2011

Windows-Check

Notfall-Windows ▪ WLAN-Sicherheit ▪ USB-Wächter ▪ Trojaner-Schutz

WINDOWS-CHECK

- So geht's: Rettungs-Stick mit Notfall-Windows S. 84
- Großer Security-Check für Ihren PC S. 8
- Wer surft in meinem WLAN? S. 48
- Virenalarm – was tun? S. 28

- Bootfähig: Kaspersky Rescue Disk 10
- Microsoft Software Center 2.0*
- USB-Stick sichern
- Notfall-Windows
- WLAN-Tools

*teilweise Internetzugang erforderlich

Mehr Sicherheit für Ihren PC

- **Microsoft Software Center 2.0***
  Alle Sicherheits-Updates für Windows XP, Vista und 7
  Alle Setup-DVDs für Windows 7 als ISO-Dateien
  Insgesamt über 200 original Microsoft-Programme S. 68
- **Kaspersky**
  Die Rescue Disk 10 bootet sofort von der Heft-DVD S. 8
- **WLAN-Tools**
  Prüfen und schützen Sie Ihr Funknetz S. 78
- **USB-Stick sichern**
  USB Flash Copy 1.5, USB Wächter 0.7.1 und mehr S. 6
- **Notfall-Windows**
  Alles für den eigenen Rettungs-Stick S. 84

INFO-Programm gemäß § 14 JuSchG

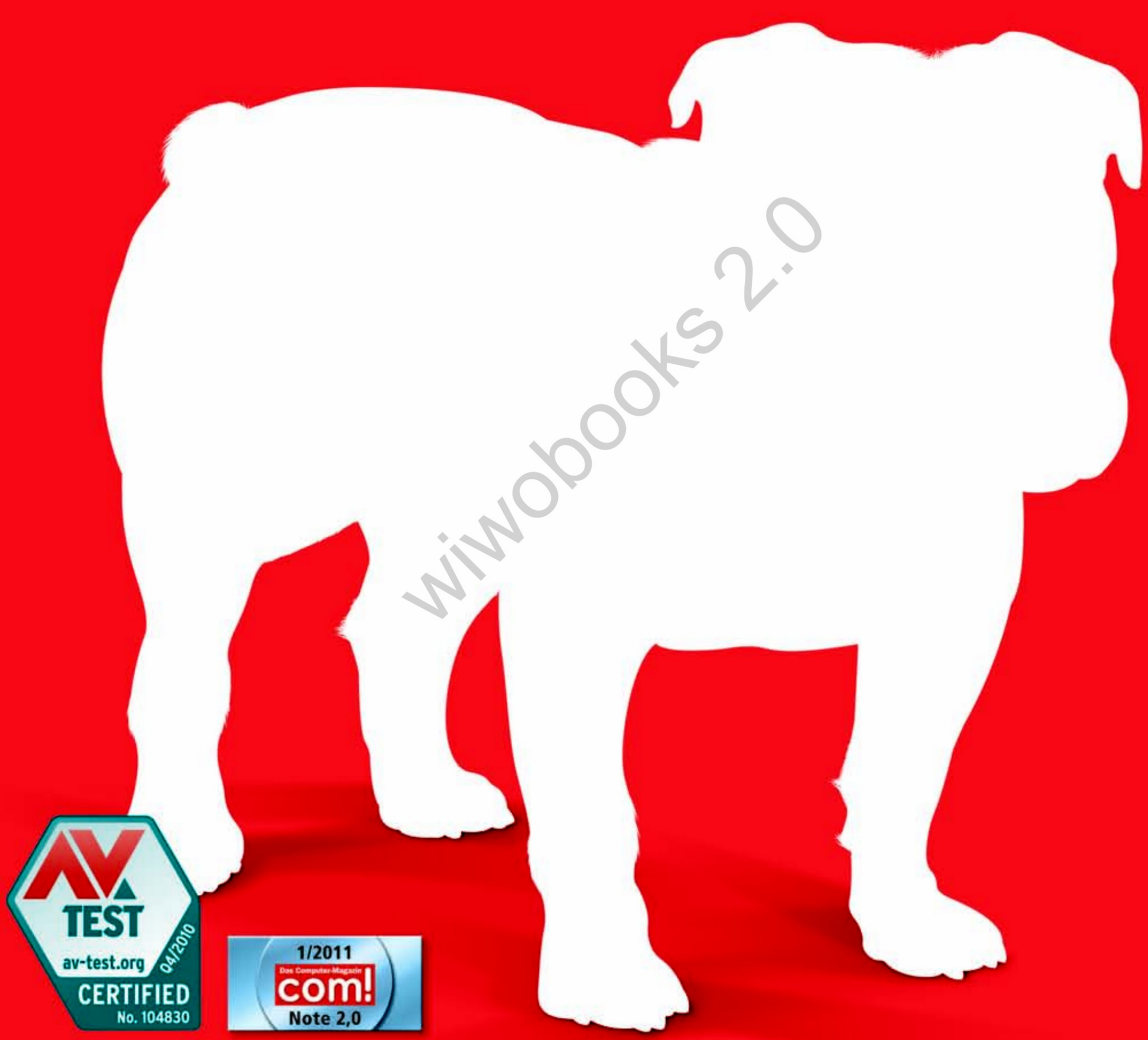
www.wowbooks.com

BullGuard™

Schützt Sie vor allen Online-Gefahren

NEU
im Handel erhältlich

wiwobooks 2.0



AV TEST av-test.org 04/2010 CERTIFIED No. 104830

1/2011 Das Computer-Magazin com! Note 2,0

- **Antivirus mit Verhaltenserkennung**
  65% höhere Erkennungsraten.
- **Safe Browsing**
  Kennzeichnet unsichere Websites in Suchergebnissen.
- **Inspector**
  Identifiziert veraltete Software mit Schwachstellen.
- **Backup**
  5 GB Online-Storage

www.bullguard.com

Windows immun

Kriminelle sind im Internet so aktiv wie nie. Sie entwickeln immer raffiniertere Methoden, um den Schutz Ihres PCs auszuhebeln. Das Ziel: Sie versuchen, Passwörter und Kreditkartennummern auszuspähen, PINs und TANs zu klauen – für die Betrüger ein lohnendes Geschäft. Gefahr droht auch aus ungeahnter Richtung: Es genügt, einen infizierten USB-Stick anzuschließen oder ungeschützt über öffentliche WLANs zu surfen.

Doch jetzt sind Sie am Zug: Dieser Ratgeber verrät Ihnen, wie Sie Windows mitsamt Anwendungen gegen die perfiden Angriffe immun machen und alle Abwehrkräfte aktivieren. Vertrauen Sie nicht nur auf Ihren Virenscanner. Die Heft-DVD enthält die besten Sicherheitsprogramme. Kombinieren Sie ihre Stärken zu einem undurchdringlichen Bollwerk.

Einen 100-prozentig sicheren PC wünscht Ihnen

J. Sedlbauer

Johann Sedlbauer, Leitender Redakteur
sonderheft@com-magazin.de

Die Heft-DVD finden Sie auf Seite 51.

www.books 2.0

WINDOWS

8 Großer Security-Check
Der Artikel stellt 20 Programme und Online-Checks vor, die auf einzelne Schädlinge spezialisiert sind und Sicherheitslücken schließen

18 Viren-Lexikon
Was ist Heap Spraying und wie schützt man sich gegen einen Buffer Overflow? Das Viren-Lexikon erklärt die Begriffe

28 Virenalarm – was tun?
Es ist passiert: Der Virenscanner schlägt Alarm und warnt vor einem Virus. Statt in Panik zu geraten, befolgen Sie zehn Schritte

34 PC von Viren säubern
Wer nach einem Virenbefall auf Nummer sicher gehen will, installiert alles neu. Das will jedoch sorgfältig geplant sein

40 Virenschleuder USB
Nach dem Internet sind USB-Sticks und -Festplatten die zweite große Infektionsquelle. So schützen Sie Ihren PC vor USB-Viren

44 Hosts-Datei für Profis
So schützen Sie Ihren Computer mit der Hosts-Datei und einem kostenlosen Tool vor gefährlichen Internetadressen

INTERNET

48 Wer surft in meinem WLAN?
Nutzen Eindringlinge die große Reichweite aus und surfen heimlich über Ihr WLAN? Machen Sie besser die Probe aufs Exempel

52 Konten-Diebstahl im WLAN
Firesheep macht das Spionieren leicht. Zwei Firefox-Erweiterungen schützen davor

54 Mit dem Notebook in fremden Netzen
Mit jedem aktuellen Notebook können Sie öffentliche WLANs nutzen. Vorher müssen Sie aber das Notebook richtig absichern

59 Zombie-Cookies
Eine neue Cookie-Art ist einfach nicht totzukriegen. Sie bleibt für immer auf Ihrem PC

Sicherheits-Check

20 Tools und Online-Checks sichern Windows, testen den Router und schützen den Browser. Spezial-Tools löschen bestimmte Schädlinge und schließen gezielt einzelne Sicherheitslücken 8

Das neue Viren-Lexikon

Backdoor und Bootkit, Heap Spraying und Pod Slurping, Buffer Overflow und Scareware: Aktuelle Gefahren für den PC und was Sie dagegen tun können 18

Wer surft in meinem WLAN?

Wer sein WLAN für jeden offen lässt, riskiert viel Ärger. So spüren Sie Eindringlinge auf und schotten Ihr WLAN in wenigen Schritten ab 48

wiwobooks

Das ist auf der Heft-DVD

Kaspersky Rescue Disk 10 8
Die Antiviren-CD prüft den PC zuverlässig auf Viren. Sie bootet direkt von der Heft-DVD

Microsoft Software Center 2.0 68
Das Microsoft Software Center bündelt über 200 System-Utilities von Microsoft unter einer Oberfläche

USB-Utilities 6
Daten sichern und fremde Sticks sperren: USB Flash Copy 1.5, USB Wächter 0.7.1 und USB-Schreibschutz

WLAN-Tools 78
Adapter Watch 1.05, Hotspot Shield 1.571, Net Surveyor 2.0, RK-WLAN-Keygen und weitere

Überblick DVD-Inhalt 6

Sicher bezahlen im Internet

Fünf neuartige Bezahlsysteme im Internet: Darunter gibt es virtuelle Kreditkarten, anonyme Prepaid-Systeme und das Bezahlen per SMS 62

Microsoft Software Center 2.0

Eine übersichtliche Bedienoberfläche bündelt mehr als 200 original Microsoft-Programme – über 140 davon sind auf der Heft-DVD 68

60 Der Trojaner Carberp
Der Trojaner Carberp hat das Potenzial, zu einem der gefährlichsten Schädlinge im Internet zu werden: Er ist aggressiv und mächtig

62 Sicher bezahlen im Internet
Fünf neue Bezahldienste wie Wirecard und Paysafecard sollen das Einkaufen verbessern. So bequem und sicher sind sie wirklich

66 Elektronischer Personalausweis
Der neue elektronische Personalausweis soll Internet-Transaktionen sicherer machen. Die Technik ist jedoch nicht in jedem Fall sicher

SECURITY-TOOLS

68 Microsoft Software Center 2.0
Das Microsoft Software Center 2.0 gibt Ihnen einen Schnellzugriff auf rund 200 der besten Tools von Microsoft

78 Die 10 besten WLAN-Tools
Die nützlichen Programme spüren Hotspots auf, ermitteln den besten Standort für Ihre WLAN-Geräte und sorgen für Sicherheit

84 Der Rettungs-Stick 1.0.4
Reanimieren Sie streikende PCs. Der Rettungs-Stick 1.0.4 bootet die wichtigsten Notfall-Systeme für Windows-PCs

90 Reparaturdatenträger
Windows 7 läuft zwar recht stabil. Sollte es aber doch einmal zu Problemen kommen, dann hilft Ihnen der Microsoft Reparaturdatenträger für Windows 7

92 USB-Stick sichern: USB Flash Copy 1.5
Das Tool USB Flash Copy 1.5 sichert die Daten des USB-Sticks auf den PC, sobald er eingesteckt wird. Mit Profilen lassen sich spezielle Sicherungsjobs anlegen

96 PC richtig abschließen
Ihr Windows-Passwort ist nicht sicher: Tools wie Ophcrack können es auslesen. Sichern Sie Ihren PC deshalb zusätzlich mit Syskey

Editorial 3, Inhalt 4, DVD-Inhalt 6, Impressum 98

wiwobooks 2.0

Antiviren-CDs und USB-Tools

Auf der Heft-DVD finden Sie unter anderem Kaspersky Rescue Disk 10, Microsoft Software Center 2.0 und USB Flash Copy 1.5.

Auf DVD

UMFASSENDER SCHUTZ

Bootfähig: Kaspersky Rescue Disk 10

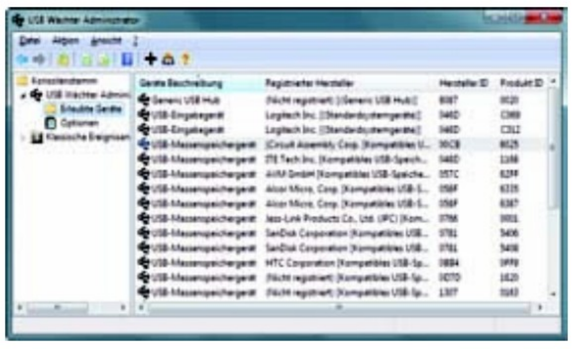
Die Heft-DVD enthält einen Komplett-Check für die Sicherheit Ihres Windows-Systems: Sie bootet die Kaspersky Rescue Disk 10, mit der Sie Ihren PC auf Viren prüfen. Das hat den Vorteil, dass eventuell vorhandene Viren sich nicht aktivieren und vor dem Sicherheits-Check verbergen können. Findet der Virenscanner Schädlinge, haben Sie die Möglichkeit, diese zu entfernen und

das Scan-Protokoll auf der Festplatte zu speichern.

Für Windows XP/Vista/7

Artikel auf Seite 8

Auf DVD



USB-STICK SICHERN

USB-Utilities

Diese Tools sichern die Daten des USB-Sticks, sperren fremde USB-Sticks und verhindern Datenklau.

Für Windows XP/Vista/7

Artikel auf Seite 40 und 92

Auf DVD

WLAN SCHÜTZEN

WLAN-Tools

Die Programme sorgen für Sicherheit: Adapter Watch 1.05, Hotspot Shield 1.571 und weitere.

Für Windows XP/Vista/7

Artikel auf Seite 78

Auf DVD

200 MICROSOFT-TOOLS

Microsoft Software Center 2.0

Das Microsoft Software Center fasst über 200 Programme aus dem Download-Center von Microsoft unter einer übersichtlichen Oberfläche zusammen. Neu in Version 2.0 des Software Centers: sämtliche Service-Packs für Windows XP, Vista und 7 sowie eine Installations-DVD für Windows 7. Sie starten das Microsoft Software Center 2.0 von der Heft-DVD oder kopieren es in ein beliebiges Verzeichnis. 143 Programme lassen sich direkt aus dem Microsoft Software Center heraus installieren.

Für Windows XP/Vista/7

Artikel auf Seite 68

www.books 2.0

Auf DVD

SCHUTZ VOR VIREN UND HACKERN

Security-Box

Diese Tools sichern Ihren PC rundherum ab: Anti Malware 1.50.1, App Remover 2.2.11.2, Avira Antivir Rescue System 3.7.16, Better Privacy 1.49, Cookie Culler 1.4, Curr Ports 1.85, Personal Software Inspector 2.0, Process Explorer 14.01, Rootkit Buster 3.60 und weitere.

Für Windows XP/Vista/7

Artikel ab Seite 8

Auf DVD

NOTFALL-SYSTEME FÜR PCS

Rettungs-Stick 1.0.4

Das Tool macht aus Ihrem USB-Stick einen bootfähigen Rettungs-Stick mit den wichtigsten Notfall-Systemen. Damit starten Sie im Ernstfall bootfähige Virenscanner von Avira und Kaspersky, Parted Magic und Windows-PE-Systeme wie die Ultimate Boot CD for Windows.

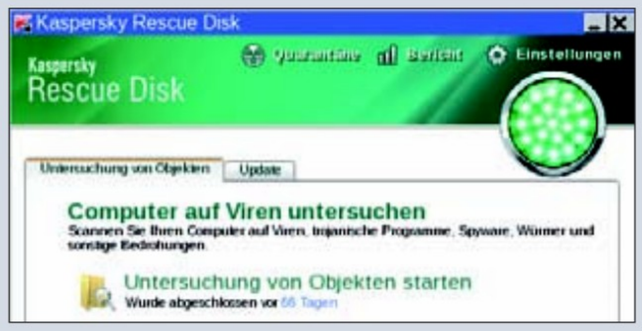
Für Windows XP/Vista/7

Artikel auf Seite 84

com! SONDERHEFT Heft-DVD Sicherheit

Kaspersky Rescue Disk 10

Die Antiviren-CD prüft den PC, ohne dass Windows und darin verborgene Viren gestartet werden. Findet der Virenscanner Schädlinge, haben Sie die Möglichkeit, diese zu entfernen und das Scan-Protokoll auf der Festplatte zu speichern. Kaspersky Rescue Disk 10 bootet direkt von der Heft-DVD.

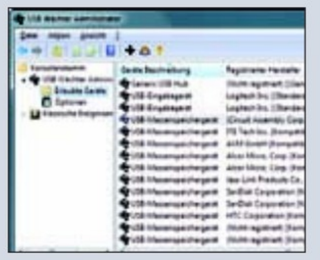


Microsoft Software Center 2.0

Das Utility fasst über 200 System-Tools aus dem Download-Center von Microsoft unter einer Oberfläche zusammen.

USB-Stick sichern

USB Flash Copy 1.5 sichert die Daten. USB Wächter 0.7.1 sperrt fremde Sticks. USB-Schreibschutz verhindert Datenklau.



Security-Box

Anti Malware 1.50.1, Avira Antivir Rescue System 3.7.16, Process Explorer 14.01, Rootkit Buster 3.60, Threatfire 4.7.0 und weitere.

WLAN-Tools

Die Programme lesen Infos zu Netzwerkadaptern aus und sorgen für Sicherheit: Adapter Watch 1.05, Net Surveyor 2.0 und weitere.

wiwobooks 2.0

com! SONDERHEFT Heft-DVD Sicherheit

WINDOWS

Security-Check
Anti-Malware 1.50.1
App Remover 2.2.11.2
Better Privacy 1.49
Cookie Culler 1.4
Curr Ports 1.85
Dr. Web Anti-Virus Link Checker 1.0.23
Hijack This 2.0.4
Kaspersky Rescue Disk 10
Noscript 2.0.9.9
Personal Software Inspector 2.0
Rootkit Buster 3.60
Threatfire 4.7.0
Web of Trust 20100908
Windows 7 Firewall Control 4.0

Viren-Lexikon
Avast Free Antivirus 6.0
Kaspersky Rescue Disk 10
Threatfire 4.7.0

Virenalarm
Anti-Malware 1.50.1
Avira Antivir Rescue System 3.7.16
Bitdefender Free Edition 2009
Blitzblank 1.0
Rootkit Buster 3.60
Unlocker 1.9.0

PC von Viren säubern
Avast Free Antivirus 6.0
Avira Antivir Rescue System 3.7.16
com! Update-Pack-Builder 5.0.7
Darik's Boot and Nuke 2.2.6 Beta
Imgburn 2.5.5.0
Kaspersky Rescue Disk 10

License Crawler 1.4 Build-135
PDF-Artikel „Service-Pack 2011 für XP, Vista und 7" aus com! 12/2010
PDF-Artikel „Tipps: Imgburn 2.5" aus com! 3/2010

Virenschleuder USB
Personal Software Inspector 2.0
USB-Schreibschutz
USB Wächter 0.7.1.130

Hosts-Datei
Hostsman 3.2.73

INTERNET

WLAN
Rogue Scanner 2.6.0

Firesheep
Blacksheep 1.7
HTTPS Everywhere 0.9.4

Notebook im Netz
Tor Browser Bundle 1.3.20

Neuer Trojaner
Carberp Removal Tool
Process Explorer 14.01

Bezahlen im Internet
PDF-Artikel „Bezahlen im Internet" aus com! 10/2009

SECURITY-TOOLS

Microsoft Software Center
com! Update-Pack-Builder 5.0.7
Imgburn 2.5.5.0
Microsoft Software Center 2.0

WLAN-Tools
Adapter Watch 1.05
Hotspot Shield 1.571
Net Surveyor 2.0 und weitere

Rettungs-Stick
com! Rettungs-Stick 1.0.4
Infrarecorder Portable 0.52
U3 Launchpad Removal 1.0.2.38

USB Flash Copy
USB Flash Copy 1.5

STANDARDS

Adobe Reader
Adobe Reader X 10.01

Browser & Runtimes
Firefox 4.0
Java-Laufzeitumgebung 6.0 Update 24

CD/DVD brennen
Imgburn 2.5.5.0

Virenscanner
Avast Free Antivirus 6.0
Bitdefender Free Edition 2009

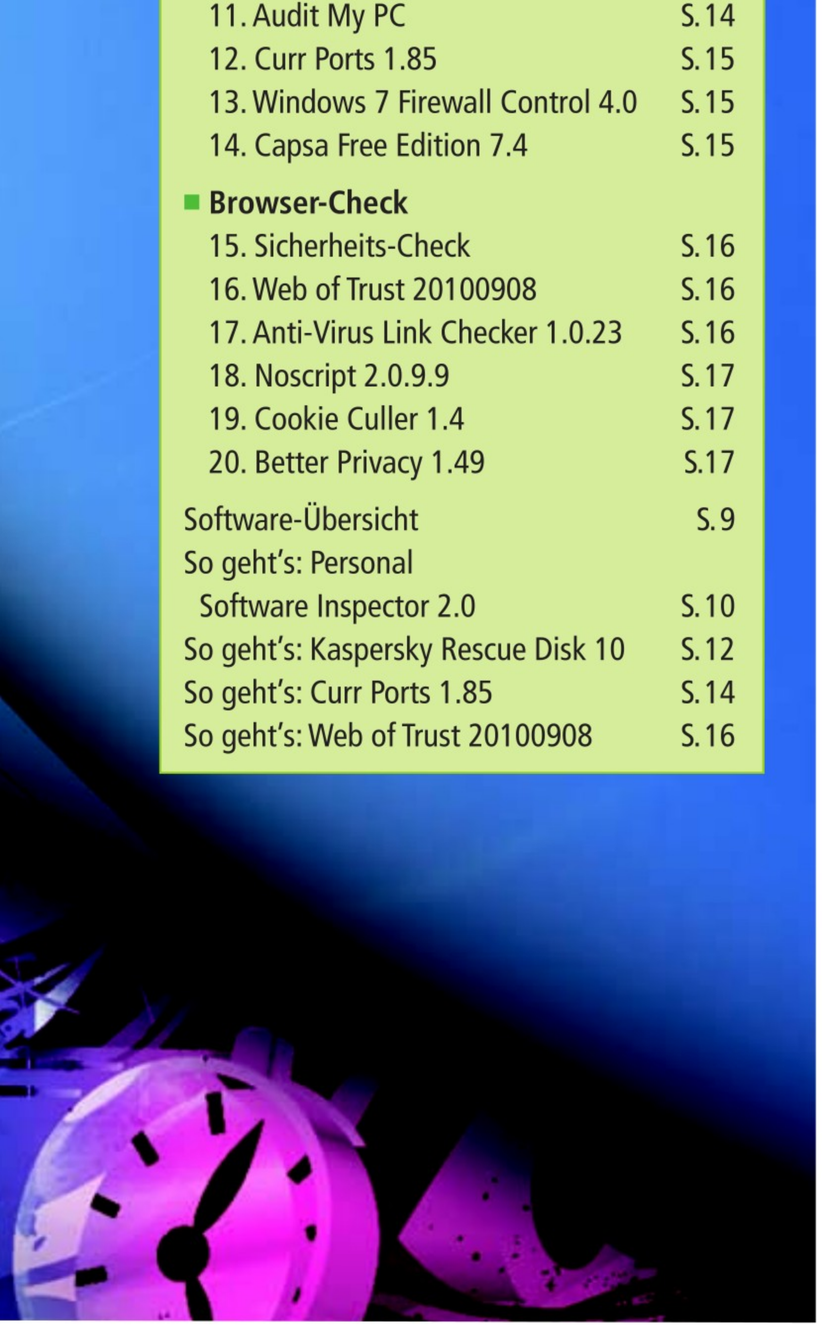
SERVICE
Probe-Abo
Lexikon
Hilfe
Impressum

com! SONDERHEFT Heft-DVD Sicherheit

Einfach entlang der punktierten Linie schneiden
Seitenlaschen nicht abtrennen, nur umbiegen
Archivieren Sie die Heft-DVD stilvoll mit Cover- und Inlay-Cards: Einfach hier ausschneiden, passend falten und in Ihr Jewel-Case legen!

Großer Secu

rity-Check



Inhalt

Großer Security-Check

- **Windows-Check**
  - 1. Baseline Security Analyzer 2.2 S. 10
  - 2. Personal Software Inspector 2.0 S. 10
  - 3. App Remover 2.2.11.2 S. 11
  - 4. Hijack This 2.0.4 S. 11
- **PC-Check**
  - 5. Anti-Malware 1.50.1 S. 12
  - 6. Kaspersky Rescue Disk 10 S. 12
  - 7. Rootkit Buster 3.60 S. 13
  - 8. Virustotal S. 13
  - 9. Threatfire 4.7.0 S. 13
- **Netzwerk-Check**
  - 10. Health Check 2.0 S. 14
  - 11. Audit My PC S. 14
  - 12. Curr Ports 1.85 S. 15
  - 13. Windows 7 Firewall Control 4.0 S. 15
  - 14. Capsa Free Edition 7.4 S. 15
- **Browser-Check**
  - 15. Sicherheits-Check S. 16
  - 16. Web of Trust 20100908 S. 16
  - 17. Anti-Virus Link Checker 1.0.23 S. 16
  - 18. Noscript 2.0.9.9 S. 17
  - 19. Cookie Culler 1.4 S. 17
  - 20. Better Privacy 1.49 S. 17

Software-Übersicht S. 9
So geht's: Personal Software Inspector 2.0 S. 10
So geht's: Kaspersky Rescue Disk 10 S. 12
So geht's: Curr Ports 1.85 S. 14
So geht's: Web of Trust 20100908 S. 16

20 Programme und Online-Checks sichern Windows, testen Ihren Router auf Lücken, spüren Schädlinge auf und schützen den Browser.

Der Artikel stellt 20 Programme und Online-Checks vor, die sich auf bestimmte Schädlinge spezialisiert haben und einzelne Sicherheitslücken gezielt schließen.

Alle Tools und Online-Checks sind kostenlos und entweder auf Heft-DVD oder im Internet verfügbar.

Kompakt

- *20 Tools und Online-Checks sichern Windows und spüren Schädlinge auf.*
- *Die bootfähige Heft-DVD scannt Ihren PC mit der Kaspersky Rescue Disk 10.*

Die Kaspersky Rescue Disk 10 bootet von der Heft-DVD. So verhindern Sie, dass ein Virus zusammen mit Windows startet und sich vor dem Virenscanner verbirgt. Sie finden die Antiviren-CD auch im Internet unter http://support.kaspersky.com/viruses/rescuedisk?level=2. ▶

wiwobooks 2.0

Software-Übersicht

Programm	Quelle	Seite
Anti-Malware 1.50.1 (Trojaner-Jäger)	www.malwarebytes.org/mbam.php	12
Anti-Virus Link Checker 1.0.23 (Link-Checker)	https://addons.mozilla.org	16
App Remover 2.2.11.2 (Reinigungs-Tool)	www.appremover.com	11
Baseline Security Analyzer 2.2 (Basis-Check)	http://technet.microsoft.com	10
Better Privacy 1.49 (Cookie-Filter)	https://addons.mozilla.org	17
Capsa Free Edition 7.4 (Netzwerk-Checker)	www.colasoft.com	15
Cookie Culler 1.4 (Cookie-Blocker)	https://addons.mozilla.org	17
Curr Ports 1.85 (Port-Checker)	www.nirsoft.net/utils/cports.html	15
Hijack This 2.0.4 (Startup-Cleaner)	http://free.antivirus.com/hijackthis	11
Kaspersky Rescue Disk 10 (Antiviren-CD)	http://support.kaspersky.com	12
Noscript 2.0.9.9 (Javascript-Blocker)	www.noscript.net	17
Personal Software Inspector 2.0 (Updater)	www.secunia.com	10
Rootkit Buster 3.60 (Rootkit-Jäger)	www.trendmicro.com/download/rbuster.asp	13
Threatfire 4.7.0 (Verhaltens-Check)	www.threatfire.com/de	13
Web of Trust 20100908 (Phishing-Filter)	www.mywot.com/de	16
Windows 7 Firewall Control 4.0 (Firewall-Tool)	www.sphinx-soft.com/Vista/order.html	15

Alle -Programme finden Sie auf Heft-DVD in der Rubrik „Windows, Security-Check".
Kaspersky Rescue Disk 10 bootet direkt von der Heft-DVD.

Windows-Check

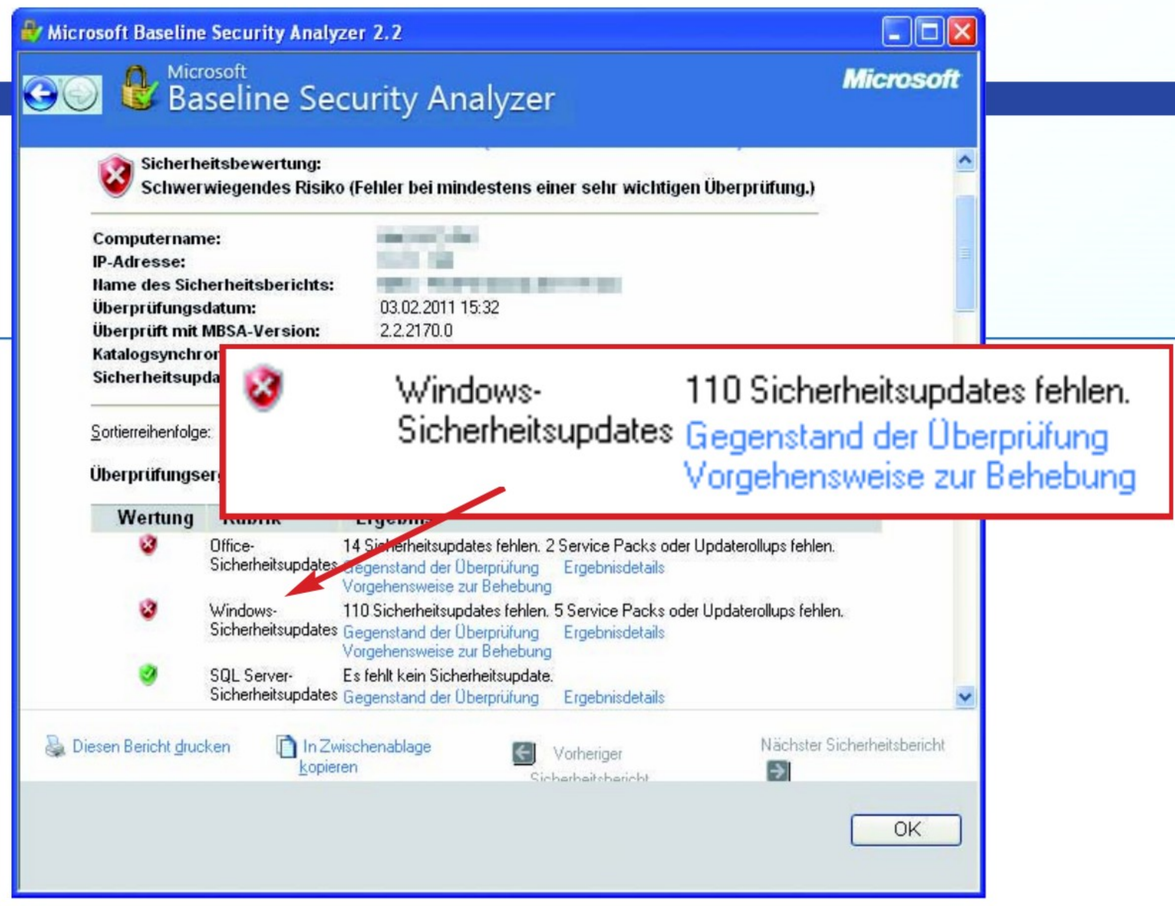
Der Windows-Check zeigt, wie Sie Windows sichern und Lücken schließen. Auch verhindert er, dass Schadprogramme automatisch starten.

1. Baseline Security Analyzer 2.2

Das Microsoft-Tool spürt Windows-Lücken auf und hilft sie zu schließen.

Testen Sie Windows mit dem Microsoft Baseline Security Analyzer 2.2 auf Schwachstellen (kostenlos, http://technet.microsoft.com/de-de/security/cc184923). Er entdeckt fehlende Updates und Konfigurationsfehler (Bild A).

So geht's: Nach dem Start des Tools klicken Sie auf den Link „Einen Computer überprüfen" und dann auf „Suche starten". Die Systemanalyse dauert mehrere Minuten. Sie erhalten dann eine Liste mit allen überprüften Parametern. Wo es Probleme gibt, zeigt das Tool mögliche Gründe und Lösungen an. Ein Klick auf „Vorgehensweise zur Behebung" führt Sie zu einer Microsoft-Seite mit Lösungswegen.



Baseline Security Analyzer 2.2: Das Tool sucht nach fehlenden Security-Patches und prüft die wichtigsten Windows-Einstellungen (Bild A)

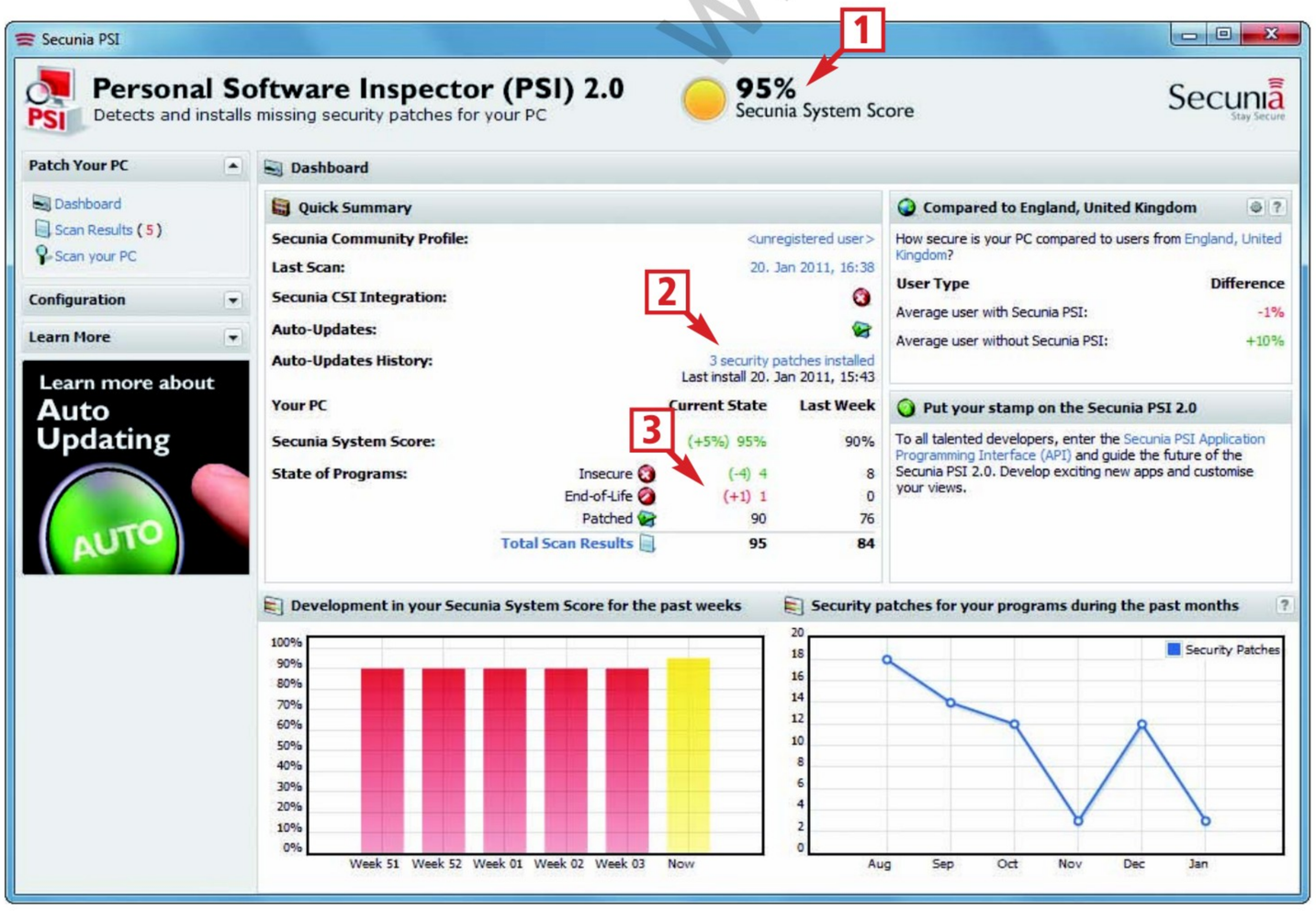
2. Personal Software Inspector 2.0

Dieses Tool aktualisiert veraltete, unsichere Programme auf Ihrem PC.

Der Personal Software Inspector 2.0 von Secunia – kurz PSI – entdeckt veraltete Software

So geht's: Personal Software Inspector 2.0

Der Personal Software Inspector 2.0 sorgt dafür, dass die Software auf Ihrem PC auf dem aktuellen Stand bleibt – bei manchen Programmen sogar vollautomatisch (kostenlos, www.secunia.com/vulnerability_scanning/personal und auf).



1 Secunia System Score
Die Prozentzahl zeigt an, wie viele Programme aktuell sind.

2 Auto-Updates History
Hier sehen Sie die Zahl der automatisch eingespielten Patches.

3 Insecure
Hier steht, wie viele Programme veraltet sind.

winobooks 2.0

und installiert Updates (kostenlos, www.secunia.com/vulnerability_scanning/personal und auf).

So geht's: Installieren und starten Sie das Tool. Es prüft nun die auf Ihrem PC installierten Anwendungen und vergleicht die Versionsnummern mit einer Datenbank. Das Ergebnis sehen Sie im „Dashboard" bei „State of Programs". Hinter „Insecure" finden Sie die Software auf Ihrem PC, von der Sicherheitslücken bekannt sind.

Eine ausführliche Übersicht erhalten Sie mit einem Klick auf „Total Scan Results". Die Liste zeigt oben alle unsicheren Anwendungen. Klicken Sie rechts auf „Install Solution", um ein Update herunterzuladen.

3. App Remover 2.2.11.2

Das Reinigungs-Tool entfernt die Reste von deinstallierten Antivirenprogrammen.

App Remover 2.2.11.2 löscht Virenscanner-Reste, die diese nach einer Deinstallation oft zurücklassen (kostenlos, www.appremover.com und auf) (Bild B). Diese Überreste machen das System instabil und können außerdem zu Fehlalarmen führen.

So geht's: Starten Sie das Tool, das keine Installation benötigt, und klicken Sie zweimal auf „Next". Nun sucht App Remover nach Resten früher installierter Antivirenprogramme. Findet es übrig gebliebene Dateien und Registry-Einträge, bietet das Tool anschließend an, sie zu entfernen.

App Remover 2.2.11.2: Das Tool entfernt Müll, den viele Virenscanner bei ihrer Deinstallation zurücklassen (Bild B)

4. Hijack This 2.0.4

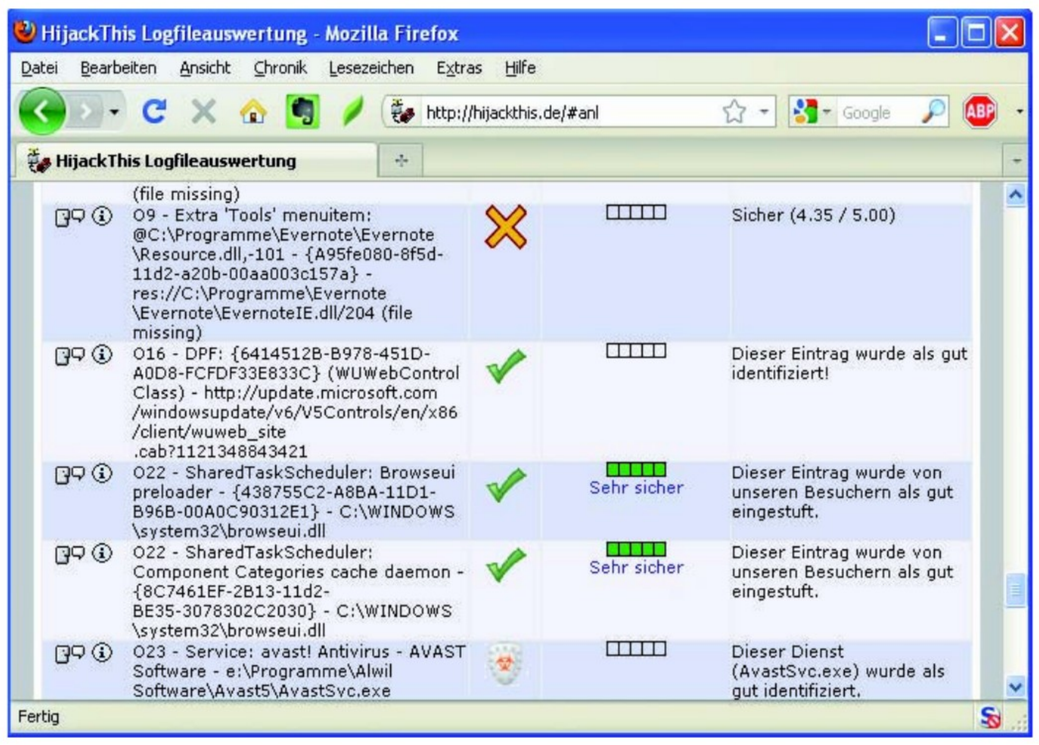
Das bewährte Sicherheits-Tool verhindert, dass Viren mit Windows starten.

Der nächste Windows-Bereich, der geprüft werden sollte, sind alle Autostart-Elemente. Hier tragen sich nicht nur gutartige Programme, sondern auch Viren ein. Kein Tool führt diese Überprüfung so zuverlässig durch wie Hijack This 2.0.4 (kostenlos, http://free.antivirus.com/hijackthis und auf).

So geht's: Unter Windows Vista und 7 benötigen Sie Administratorrechte: Klicken Sie mit der rechten Maustaste auf die Verknüpfung und wählen Sie „Eigenschaften" aus. Wechseln Sie zum Reiter „Kompatibilität" und setzen Sie unter Windows 7 ein Häkchen vor „Programm als Administrator ausführen". Unter XP genügt ein Doppelklick.

Starten Sie das Tool und klicken Sie auf „Main Menu" und dann auf „Do a system scan and save a logfile". Hijack This scannt den PC und öffnet ein Fenster des Texteditors. Klicken Sie in dieses Fenster, drücken Sie [Strg A] und danach [Strg C].

Rufen Sie jetzt die Seite www.hijackthis.de auf. Klicken Sie in die Box und drücken Sie [Strg V]. Mit „Auswerten" starten Sie den Check. Nach kurzer Zeit sehen Sie das Ergebnis der Überprüfung (Bild C). Notieren Sie sich Schädlings-Einträge und kehren Sie zu Hijack This 2.0.4 zurück. Markieren Sie die zu entfernenden Elemente und klicken Sie auf „Fix checked, Ja". ▶



Autostart-Check: Die Webseite www.hijackthis.de wertet den Scan-Bericht von Hijack This 2.0.4 aus (Bild C)

www.wobooks2.0

PC-Check

Der PC-Check besteht aus mehreren Tests und spürt so auch hartnäckige Viren auf. Threatfire 4.7.0 erweitert zudem Ihren Virenscanner um einen mächtigen Verhaltensschutz.

5. Anti-Malware 1.50.1

Das Tool ist eines der besten Programme gegen Trojaner, hat aber keinen Hintergrundwächter.

Suchen Sie zuerst mit Anti-Malware 1.50.1 nach Schädlingen (kostenlos, www.malwarebytes.org/mbam.php und auf). Das Programm analysiert die laufenden Prozesse und verschiebt gefundene Viren in eine Quarantäne, wo sie keinen Schaden mehr anrichten können (Bild D).

Anti-Malware 1.50.1: Hier hat das Tool gleich mehrere verborgene Viren aufgespürt (Bild D)

So geht's: Nach der Installation aktualisiert Anti-Malware seine Signaturen. Sobald die Oberfläche des Schutz-Tools gestartet ist, markieren Sie unter „Scanner" die Option „Vollständigen Suchlauf durchführen" und klicken auf „Scannen". Markieren Sie in dem kleinen Einstellungsfenster, das sich jetzt öffnet, alle Laufwerke und bestätigen Sie mit „Scannen".

Nachdem der Suchlauf beendet ist, klicken Sie auf „OK, Ergebnisse anzeigen" und danach auf „Entferne Auswahl".

6. Kaspersky Rescue Disk 10

Diese Antiviren-CD prüft den PC, ohne dass Windows und darin verborgene Viren gestartet werden.

Einen weiteren Komplett-Check enthält die Heft-DVD: Sie bootet die Kaspersky Rescue Disk 10, mit der Sie Ihren PC auf Viren prüfen (kostenlos, http://support.kaspersky.com/viruses/rescuedisk?level=2 und auf). Das hat den Vorteil, dass eventuell vorhandene Viren sich nicht aktivieren und vor dem Sicherheits-Check verbergen können.

So geht's: Legen Sie die Heft-DVD ein und starten Sie Ihren PC neu. Sie finden die Live-CD als ISO-Datei auch im Internet unter http://support.kaspersky.com/viruses/rescuedisk?level=2. Brennen Sie die ISO-Datei als bootfähige CD.

Nachdem das System gestartet ist, wählen Sie „Update" aus. Klicken Sie auf „Update ausführen", um die Virensignaturen zu aktualisieren. Das funktioniert jedoch nur, wenn Sie einen DSL-Router mit DHCP (Dynamic Host Control Protocol) verwenden. Hierbei erhält das Antiviren-System automatisch eine IP-Adresse von Ihrem Router. WLAN-Nutzer ver-

So geht's: Kaspersky Rescue Disk 10

Die Kaspersky Rescue Disk 10 bootet Ihren PC von der Heft-DVD. Die Live-CD führt dann einen Check auf Viren durch (kostenlos, http://support.kaspersky.com/viruses/rescuedisk?level=2 und auf).

1 Update
Führen Sie als Erstes ein Update der Virensignaturen durch.

2 Untersuchung von Objekten starten
Ein Klick auf diese Schaltfläche startet die Virensuche.

3 Bericht
Hier haben Sie die Möglichkeit, das Scan-Protokoll auf der Festplatte oder einem USB-Stick zu speichern.

www.boo ks 2.0

wenden am besten vorübergehend ein Netzwerkkabel.

Sobald das Update abgeschlossen ist, wechseln Sie wieder zum Reiter „Untersuchung von Objekten“ zurück. Ein Klick auf „Untersuchung von Objekten starten“ beginnt mit der Suche nach Viren. Findet das Antiviren-System einen Schädling, haben Sie anschließend die Möglichkeit, diesen zu entfernen.

7. Rootkit Buster 3.60

Das Tool hat sich auf tief im System versteckte Rootkits spezialisiert.

Das Programm Rootkit Buster 3.60 erkennt und entfernt Rootkits (kostenlos, www.trendmicro.com/download/rbuster.asp und auf).

So geht's: Starten Sie das Tool mit einem Doppelklick auf „RootkitBuster.exe“. Den Rootkit-Check beginnen Sie mit „Scan Now“.

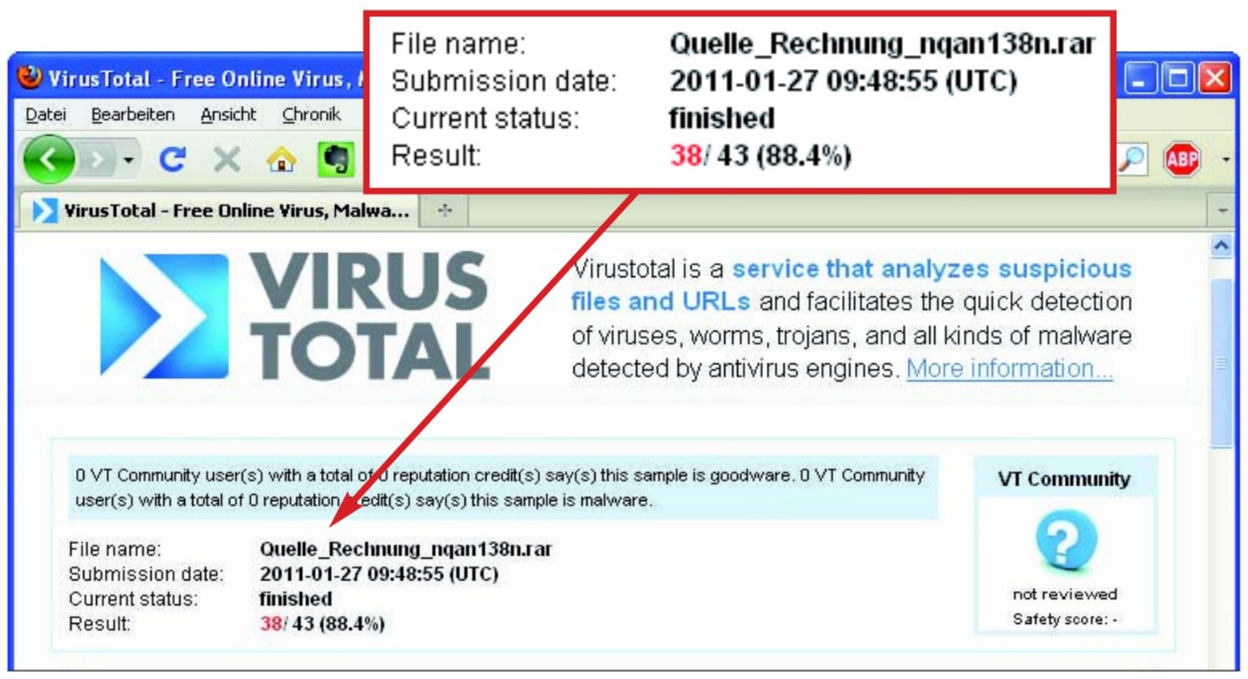
Oft finden Sie danach unter „Scan results“ auch legitime Einträge, die etwa auf das installierte Antivirenprogramm zurückzuführen sind. Öffnen Sie deswegen zuerst die ausführlichere Log-Datei mit „View Log …“ und suchen Sie den fraglichen Eintrag dort heraus. Hinter „Image Path“ finden Sie den Dateinamen. Geben Sie den Dateinamen bei Google ein und überprüfen Sie die ersten Treffer, ob sie einen Hinweis auf einen Schädling enthalten. Falls ja, markieren Sie den Eintrag und entfernen ihn mit „Delete Selected Items“.

8. Virustotal

Der Online-Dienst prüft verdächtige Dateien mit mehreren Dutzend Virenscannern.

Virustotal (www.virustotal.com) checkt jede hochgeladene Datei mit 43 Virenscannern.

So geht's: Rufen Sie die Webseite www.virustotal.com auf und klicken Sie auf „Durchsuchen …“. Wählen Sie die fragliche Datei aus und laden Sie sie anschließend mit „Send file“ hoch. Virustotal beginnt nun damit, die Datei zu prüfen. Nach kurzer Zeit füllt sich das Fenster mit den Ergebnissen. Für jeden Scanner listet die Seite genau auf, ob er einen Schädling gefunden hat oder nicht (Bild E).



Check mit Virustotal: Die Seite prüft hochgeladene Dateien kostenlos mit über 40 verschiedenen Virenscannern (Bild E)

9. Threatfire 4.7.0

Threatfire schützt, wenn Ihr Virenscanner wegen einer fehlenden Signatur versagt.

Eigentlich soll man nicht zwei Hintergrundwächter verwenden. Das Tool Threatfire 4.7.0 ist mit seiner verhaltensbasierten Erkennung jedoch die ideale Ergänzung zu einem normalen Virenscanner (kostenlos, www.threatfire.com/de und auf) (Bild F).

So geht's: Noch während der Installation führen Sie mit „Start Scan“ einen „Schnellscan“ aus. Dabei prüft das Tool, ob Firewall und Antivirenprogramm aktiv sind. Nach dem Setup ist das Programm sofort einsatzbereit und passt im Hintergrund auf, dass sich keine Schädlinge einschleichen. ▶

Threatfire 4.7.0: Das Sicherheits-Tool erkennt Viren am Verhalten. Es findet deshalb oft neue Viren, von denen es noch keine Signaturen gibt (Bild F)

www.wobooks2.0

Netzwerk-Check

Die meisten Schädlinge gelangen über ein Netzwerk auf PCs. Mehrere Checks testen Ihr Netz.

Health Check: Das Online-Tool prüft über das Web, ob Ihr PC sicher ist (Bild G)

10. Health Check 2.0

Dieser umfassende Online-Test prüft die Sicherheit Ihres Computers von außen.

Das Online-Tool Health Check 2.0 prüft in drei Schritten über das Internet, ob Ihr Rechner geschützt ist. Dazu benötigt es Java.

So geht's: Rufen Sie www.f-secure.com/de/web/home_global/protection/free-online-tools/free-online-tools auf und setzen Sie bei „Health Check" ein Häkchen vor den Lizenzbedingungen. Starten Sie den Test anschließend mit „Prüfung durchführen, Ausführen". Ein neues Fenster öffnet sich.

Der Health Check testet, ob Sicherheitssoftware installiert ist, eine Datensicherung aktiv ist und ob alle Windows-Updates vorhanden sind. Abschließend zeigt das Tool eine Übersicht der Ergebnisse samt Lösungsvorschlägen für die ermittelten Probleme an (Bild G).

11. Audit My PC

Dieser Firewall-Test prüft Ihren Router auf Lücken, die Trojaner häufig nutzen.

Nur ein externer Port-Scan legt offen, ob eine Lücke in Ihrer Router-Firewall existiert, über die ein Wurm auf Ihren PC gelangen könnte.

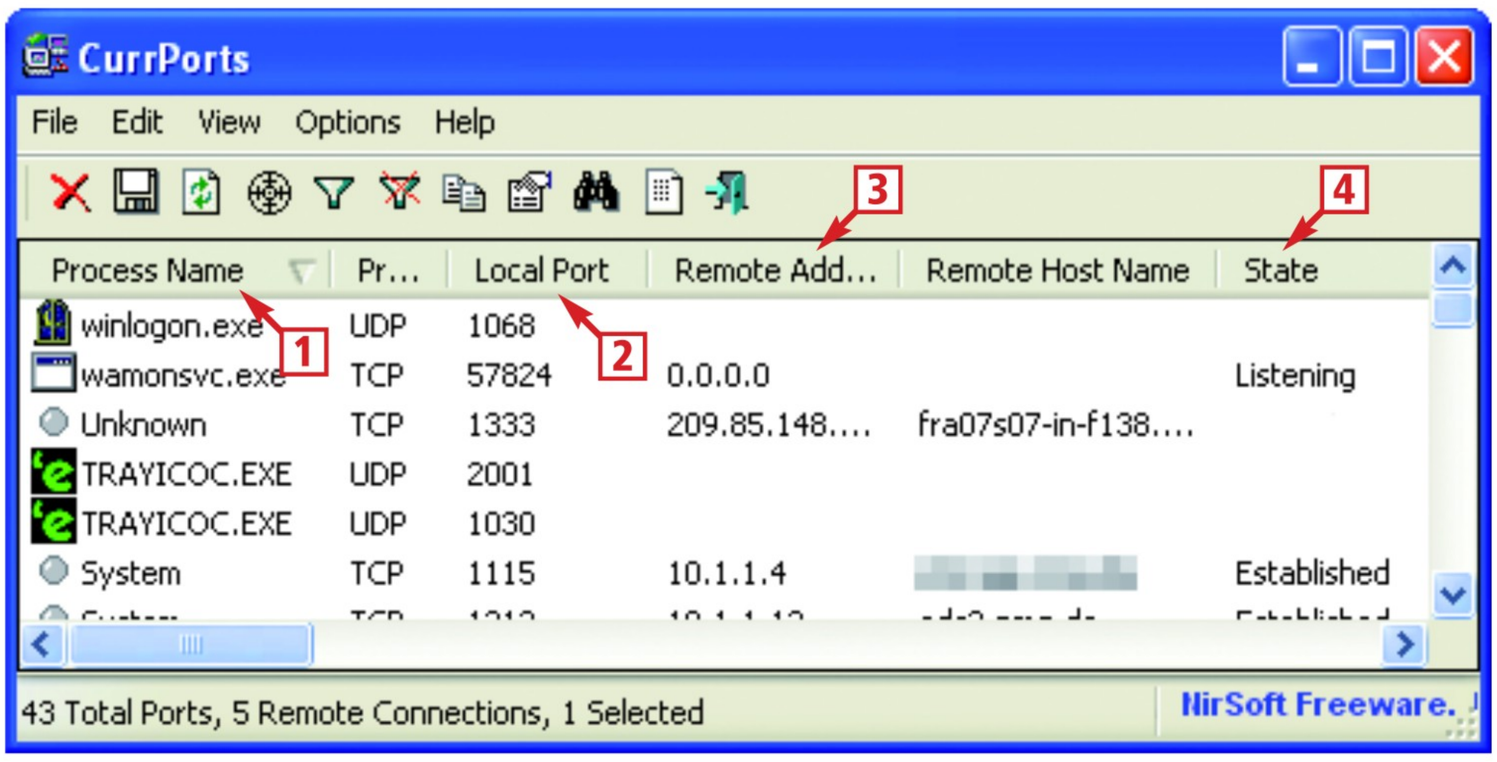
So geht's: Rufen Sie www.auditmypc.com/firewall-test.asp auf. Füllen Sie alle Felder aus und wählen Sie dann hinter „TCP port range" und „UDP port range" jeweils „Trojans" aus. Der Dienst sucht nun nach offenen Ports, die häufig von Trojanern genutzt werden. Zuletzt setzen Sie das Häkchen vor „I agree to the Terms of Service" und klicken auf „Start Now!".

Nach wenigen Minuten sehen Sie das Ergebnis des Scans (Bild H). Einen ausführlicheren Bericht erhalten Sie per E-Mail. Wurde ein

wiwobooks 2.0

So geht's: Curr Ports 1.85

Curr Ports 1.85 legt offen, welche Programme auf Ihrem Computer mit dem Internet kommunizieren und welchen Port sie dabei verwenden (kostenlos, www.nirsoft.net/utils/cports.html und auf).



1 Process Name
In dieser Spalte stehen die Dateinamen der aktiven Prozesse.

2 Local Port
Die Spalte zeigt die Port-Nummer, die das Programm geöffnet hat.

3 Remote Address
Mit dieser Adresse kommuniziert das Programm.

4 State
„Established" bedeutet, dass hier bereits Daten gesendet wurden. „Listening" heißt, dass der Prozess auf Daten wartet.

offener Port gefunden, rufen Sie die Konfiguration Ihres DSL-Routers auf. Suchen Sie nach einem Menüpunkt, der „Port-Forward“, „Port-Freigaben“ oder ähnlich heißt. Entfernen Sie dort alle überflüssigen Einträge.

12. Curr Ports 1.85

Das Mini-Tool stellt fest, ob ein Schädling einen Port auf Ihrem PC geöffnet hat.

Curr Ports 1.85 zeigt die offenen Netzwerkverbindungen auf Ihrem PC an (kostenlos, www.nirsoft.net/utils/cports.html und auf).

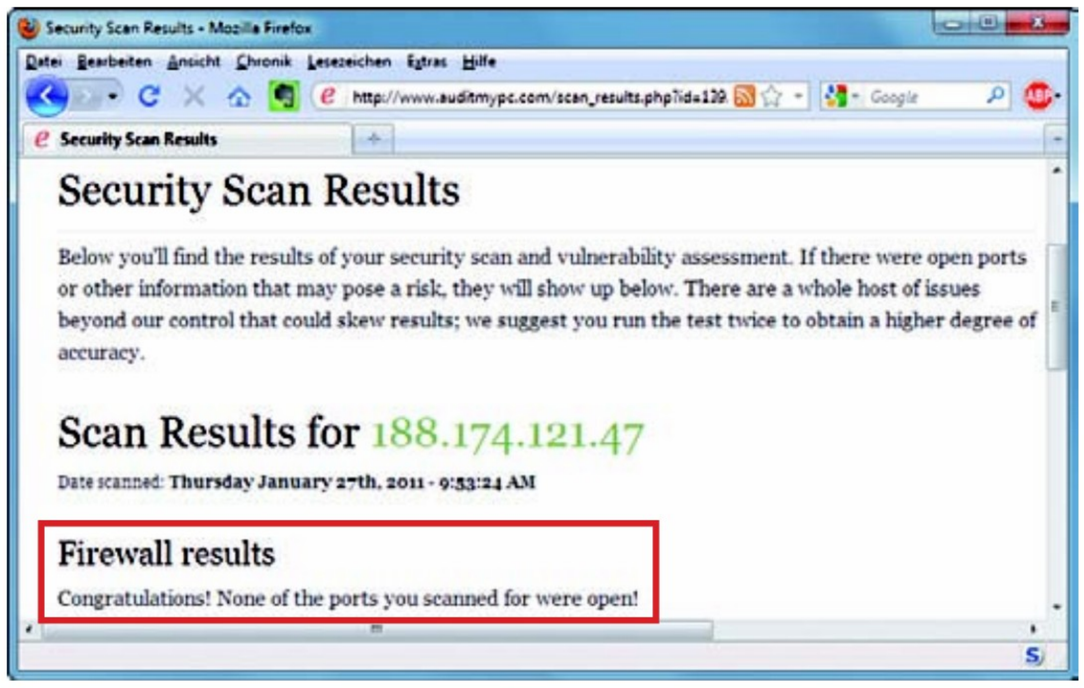
So geht's: Starten Sie Curr Ports mit einem Doppelklick auf „cports.exe“. Unter „Process Name“ sehen Sie jetzt, welche Programme Ports geöffnet haben. Finden Sie einen verdächtigen Prozess, notieren Sie sich den Namen der zugehörigen Datei. Sie finden ihn in der Spalte „Process Path“. Laden Sie die Datei anschließend bei Virustotal (www.virustotal.com) hoch, wie auf Seite 13 beschrieben.

13. Windows 7 Firewall Control 4.0

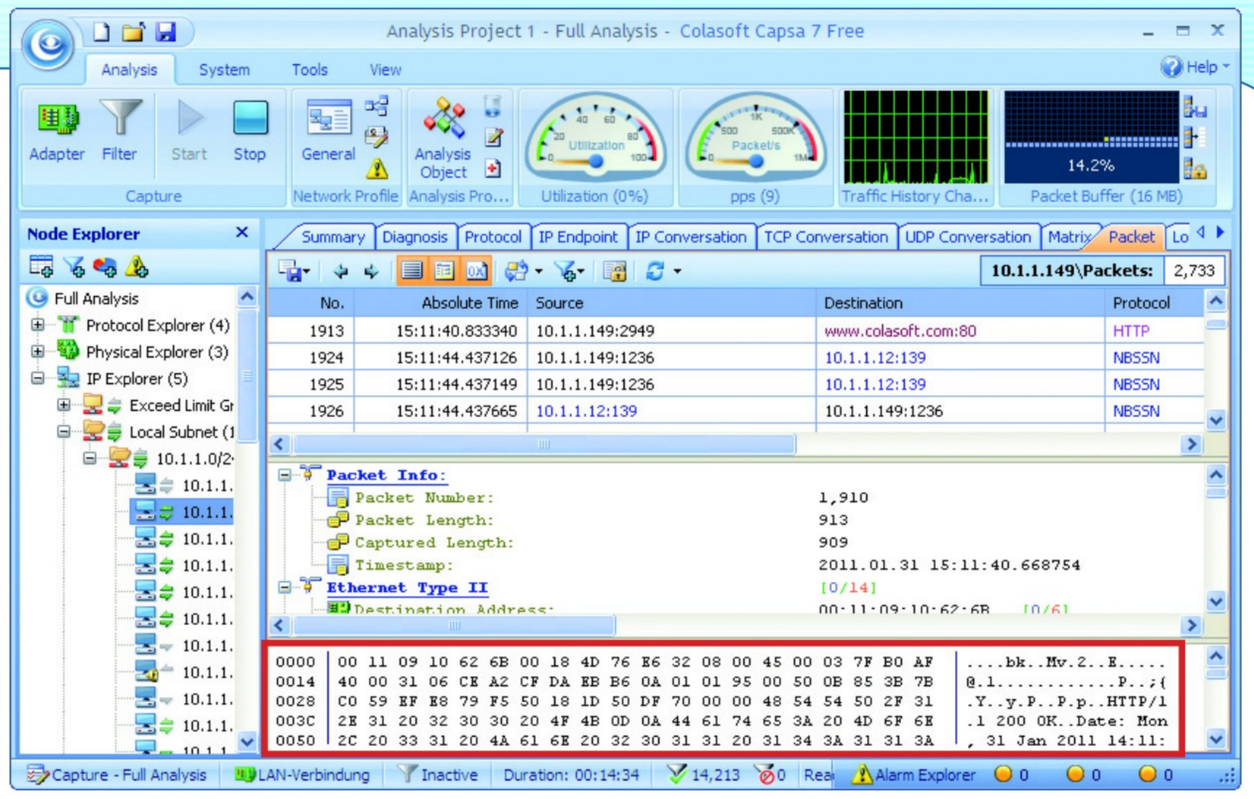
Das Tool ergänzt die Windows-Firewall um Funktionen, die sonst nur Kaufprogramme haben.

Windows 7 Firewall Control 4.0 erweitert die Windows-Firewall (kostenlos, www.sphinx-soft.com/Vista/order.html und auf).

So geht's: Nach der Installation blendet Windows 7 Firewall Control für jedes Programm, das Daten ins Internet senden will, ein Warnfenster ein. Um einem Programm die Netzwerkkommunikation zu erlauben, wählen Sie hinter „Zone“ den Punkt „EnableAll“ aus und bestätigen mit „Apply“. Die Zone „DisableAll“ sperrt dagegen alle Zugriffe.



Externer Port-Scan: Die Webseite www.auditmypc.com/firewall-test.asp findet heraus, ob in Ihrem DSL-Router Ports offen sind (Bild H)



Capsa Free Edition 7.4: Das Analyse-Tool zeichnet IP-Pakete auf und zeigt ihren Inhalt an (Bild I)

14. Capsa Free Edition 7.4

Das mächtige Analyseprogramm schneidet alle Datentransfers mit.

Mit Capsa Free Edition 7.4 finden Sie heraus, welche Daten eine Software sendet und mit welchen anderen Computern Ihr PC Daten austauscht (kostenlos, www.colasoft.com/capsa/capsa-free-edition.php).

So geht's: Zum Download von Capsa ist eine Registrierung notwendig. Nach der Installation setzen Sie bei „Adapter“ ein Häkchen vor Ihrer Netzwerkverbindung. Markieren Sie dann „Full Analysis“ und klicken Sie rechts auf das weiße Dreieck.

Das Programm beginnt nun damit, die übertragenen Netzwerkdaten mitzuschneiden. Wählen Sie links bei „IP Explorer“ die IP-Adresse Ihres PCs aus und klicken Sie dann rechts auf „Packet“. Sie sehen daraufhin jedes einzelne übertragene Datenpaket und seinen Inhalt (Bild I). Ein Klick auf „Matrix“ zeigt, mit welchen Computern Ihr PC kommuniziert. ▶

winboo ks 2.0

Browser-Check

Der Browser ist das zentrale Programm, um auf das World Wide Web zuzugreifen. Das macht ihn aber auch zum Einfallstor für viele Schädlinge. Was Sie dagegen tun können, steht in den folgenden Abschnitten.

15. Sicherheits-Check

Dieser Online-Check zeigt Ihnen, was besuchte Webseiten über Sie wissen.

Auf der Webseite der com! finden Sie einen Sicherheits-Check. Er zeigt, was andere Webseiten über Sie erfahren.

So geht's: Rufen Sie www.com-magazin.de/sicherheit/sicherheits-check.html im Browser auf. Sie finden dort vier große Checks. Beginnen Sie mit dem „Basis-Check", der Ihnen zeigt, was Ihr Browser über Sie verrät.

Der „Browser-Check" demonstriert, wie Webseiten die URLs der von Ihnen besuchten Seiten auslesen. Der „Plug-in-Check" prüft, welche Zusatzsoftware installiert ist. Zuletzt erfahren Sie mit dem „Firewall-Check", ob Ports geöffnet sind.

Einen weiteren Port-Check finden Sie unter „Audit My PC" auf Seite 14.

16. Web of Trust 20100908

Das Add-on für Firefox und Internet Explorer blockiert gefährliche Webseiten.

Web of Trust 20100908 ist eine Erweiterung für Firefox und den Internet Explorer, die vor gefährlichen Webseiten schützt (kostenlos, www.mywot.com/de und auf).

So geht's: Installieren Sie das Add-on und starten Sie Ihren Browser neu. Der Schutz ist sofort aktiv. Wenn Sie eine gefährliche Webseite aufrufen, blockiert Web of Trust den Zugriff.

17. Anti-Virus Link Checker 1.0.23

Nur mit diesem Add-on prüfen Sie Dateien noch vor dem Download auf Virenbefall.

Die Firefox-Erweiterung Dr. Web Anti-Virus Link Checker 1.0.23 prüft Links vorab auf

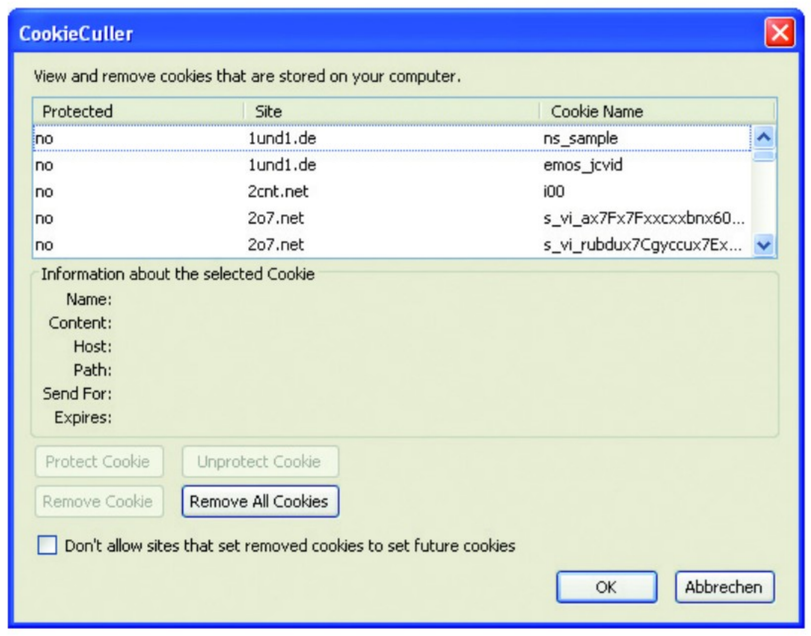
So geht's: Web of Trust 20100908

Web of Trust 20100908 schützt vor gefährlichen Webseiten (kostenlos, www.mywot.com/de und auf). Das Add-on gibt es sowohl für Firefox als auch für den Internet Explorer.

1 Symbol
Dieses Symbol zeigt die Gefährlichkeit der besuchten Seite in Ampelfarben.

2 Bewertungsdetails
Hier erfahren Sie, warum eine Seite als gefährlich eingestuft wird.

3 Warnung ignorieren
Klicken Sie hier, wenn Sie eine Seite trotz der Warnung besuchen wollen.



Cookie Culler 1.4: Die Firefox-Erweiterung löscht Cookies. Sie können einzelne Cookies davon ausnehmen (Bild L)

Anti-Virus Link Checker 1.0.23: Die Firefox-Erweiterung scannt Dateien im Internet nach Viren, bevor Sie sie herunterladen (Bild K)

schädlichen Code (kostenlos, https://addons.mozilla.org/de/firefox/addon/938 und auf). **So geht's:** Nach der Installation des Add-ons klicken Sie verdächtige Links mit der rechten Maustaste an und wählen aus dem Kontextmenü „Scannen mit Dr. Web" aus. Ein Server von Dr. Web lädt nun die Datei für Sie herunter und prüft sie auf eine Infektion (Bild K).

18. Noscript 2.0.9.9

Das Add-on blockiert aktive Webinhalte und sollte auf keinem PC fehlen.

Die Firefox-Erweiterung Noscript 2.0.9.9 ist der letzte Schutzwall im Browser, falls Sie trotz Link-Checker und Web of Trust versehentlich auf einer böswilligen Webseite landen (kostenlos, www.noscript.net und auf). Das Add-on erlaubt die von vielen Kriminellen zur Verbreitung von Schädlingen genutzten Techniken Javascript, Java und Flash nur noch auf von Ihnen freigegebenen Seiten.

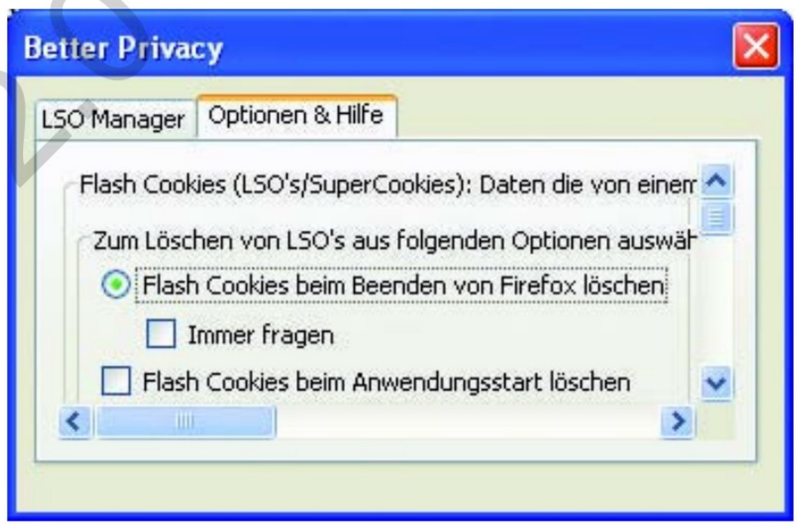
So geht's: Starten Sie nach der Installation von Noscript den Browser neu. Ab sofort blockiert das Add-on Javascript, Java und Flash. Wenn Sie einer vertrauenswürdigen Adresse, zum Beispiel www.spiegel.de, den Einsatz von Javascript gestatten wollen, klicken Sie unten rechts auf das Noscript-Symbol. Wählen Sie dann aus der Liste „spiegel.de erlauben" aus.

19. Cookie Culler 1.4

Die Erweiterung lässt nur noch Cookies zu, die Sie ausdrücklich erlaubt haben.

Cookies dienen dazu, Besucher auf Webseiten wiederzuerkennen. Das ist beispielsweise in einem Online-Forum praktisch, weil man sich nicht jedes Mal neu einloggen muss. Andererseits verwenden große Werbenetze Cookies dazu, Surfprofile zu erstellen. Die Firefox-Erweiterung Cookie Culler 1.4 erlaubt nur von Ihnen freigegebene Cookies (kostenlos, https://addons.mozilla.org/de/firefox/addon/82 und auf).

So geht's: Installieren Sie Cookie Culler und starten Sie Firefox neu. Rufen Sie dann „Extras, Einstellungen …" auf und klicken Sie bei „Datenschutz" auf „Cookies anzeigen …". Löschen Sie alle unerwünschten Cookies. Rufen Sie dann „Extras, CookieCuller" auf (Bild L) und markieren Sie die erste Cookie-Zeile mit der Maus. Scrollen Sie nach unten und klicken Sie bei gedrückter Umschalttaste auf die letzte Zeile. Klicken Sie auf „Protect Cookie". Legen Sie noch fest, dass Firefox bei jedem Neustart alle nicht geschützten Cookies löscht. Rufen Sie „Extras, Add-ons" auf und klicken Sie bei „CookieCuller" auf „Einstellungen". Setzen Sie das Häkchen vor „Delete Unprotected Cookies on Startup".



Better Privacy 1.49: Die Firefox-Erweiterung schützt vor Super-Cookies, die Flash auf Ihrem PC ablegt (Bild M)

20. Better Privacy 1.49

Das Add-on macht Schluss mit Flash-Cookies, mit denen Werbenetze Ihr Surfverhalten ausspähen.

Better Privacy 1.49 entfernt auch hartnäckige Flash-Cookies (kostenlos, https://addons.mozilla.org/de/firefox/addon/6623 und auf).

So geht's: Rufen Sie „Extras, BetterPrivacy" auf und klicken Sie im Add-on auf „Alle LSOs entfernen". Auf der Registerkarte „Optionen & Hilfe" konfigurieren Sie dann die automatische Säuberung Ihres PCs (Bild M). ■

Andreas Th. Fischer
sonderheft@com-magazin.de

Weitere Infos

- www.viruslist.com/de/viruses/analysis
  Hintergrundartikel zu Gefahren im Internet

WiWo Books 2.0

Viren-Lexikon

www.ebooks2c

Was ist ein Downloader und was ein Stealer? Wie funktioniert Heap Spraying und wie schützt man sich gegen einen Buffer Overflow? Das Viren-Lexikon erklärt die Begriffe aus dem Jargon der Sicherheitsexperten.

Fachzeitschriften und Online-Magazine sind voll mit Schlagwörtern aus der IT-Sicherheit. Doch was davon ist wirklich gefährlich und wovor müssen Sie sich besonders in Acht nehmen?

Der Artikel erklärt mehr als zwanzig aktuelle Begriffe und gibt Tipps, wie Sie sich schützen. In fünf Kästen finden Sie außerdem die wichtigsten Tools und Online-Dienste, mit denen Sie Schädlinge aufspüren und neue Infektionen vermeiden.

Auf DVD

Die Tools zum Artikel finden Sie auf in der Rubrik „Windows, Viren-Lexikon“.

Adware

Adware sind Programme, die Werbung einblenden und oft heimlich Daten sammeln.

Unter Adware versteht man Software, die sich – mehr oder weniger aufdringlich – durch Werbung finanziert. Das ist an sich nicht verwerflich, solange der Anwender offen informiert wird.

Während beispielsweise Werbe-Toolbars früher häufig heimlich mitinstalliert wurden, informieren heute immer mehr Anbieter über mitgelieferte Werbe-Elemente und bieten auch die Möglichkeit, sie abzuwählen.

So schützen Sie sich: Klicken Sie sich bei der Installation eines kostenlosen Programms nicht einfach durch die Set-up-Fenster. Wählen Sie, wenn möglich, immer die benutzerdefinierte Installation aus.

Entfernen Sie gegebenenfalls das Häkchen vor der optionalen Installation einer Toolbar. Die meisten Werbe-Toolbars stammen eigentlich von Anbietern wie Yahoo und Google und werden nur umbenannt.

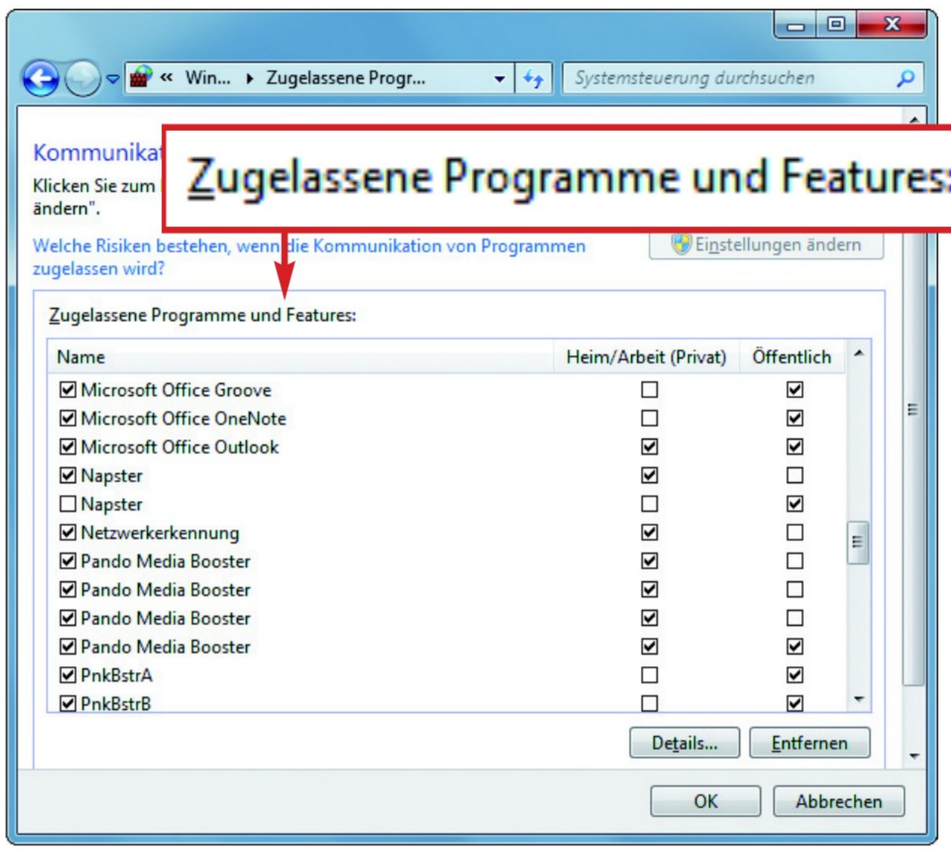
Kompakt

- *Der Artikel erklärt neue und alte Fachbegriffe aus der IT-Sicherheit.*
- *Drei Schutz-Tools finden Sie auf Heft-DVD. Die Kaspersky Rescue Disk 10 bootet direkt von der Heft-DVD.*

Backdoor

Über eine Backdoor steuern Kriminelle Ihren PC aus der Ferne, klauen Daten und installieren Schadcode.

Eine Backdoor ist eine Hintertür auf einem PC. Bei einer Backdoor kann es sich um versteckte Funktionen in einer Software handeln oder um einen Trojaner (➔ Trojaner, Seite 25), der von außen gesteuert wird.



Windows-Firewall: Während der Installation darf sich jedes Programm selbst in die Ausnahmeliste der Firewall eintragen (Bild A)

So schützen Sie sich: Gegen versteckte Backdoors kann man sich nur schwer wappnen. Eine Desktop-Firewall stoppt zwar theoretisch ausgehende Netzwerkverbindungen. In der Praxis ist es für eine schädliche Anwendung jedoch leicht, ihre Netzwerkkommunikation über eine erlaubte Software zu tunneln.

Die Liste der Programme auf dem PC, die Daten frei ins Internet senden dürfen, ist meist länger als viele Anwender denken. Beim Setup darf sich nämlich jedes Programm in die Ausnahmeliste der Windows-Firewall eintragen (Bild A). Unter Windows 7 rufen Sie „Start, Systemsteuerung, System und Sicherheit“ auf, klicken auf „Programm über die Windows-Firewall kommunizieren lassen“ und dann auf „Einstellungen ändern“. Wählen Sie das zu sperrende Programm aus und sperren Sie seinen Internetzugriff mit einem Klick auf „Entfernen“.

Der beste Schutz gegen Backdoors ist die Installation eines verhaltensbasierten Sicherheits-Tools wie Threatfire 4.7.0 (➔ Tool 2, Seite 22). Das Tool bemerkt sofort, wenn ein Schädling versucht, Daten über eine andere Anwendung zu versenden.

Botnetz: Diese Karte zeigt mit dem Trojaner Zeus verseuchte PCs, die sich zu einem weltumspannenden Netz zusammengeschlossen haben (Bild B)

Inhalt

Viren-Lexikon

Adware	S. 18
Backdoor	S. 19
Bootkit	S. 19
Botnetz	S. 20
Buffer Overflow	S. 20
Crapware	S. 20
Dekomprimierungsbombe	S. 20
Downloader	S. 21
Exploit	S. 21
Heap Spraying	S. 21
Keylogger	S. 21
Malware	S. 22
Pod Slurping	S. 22
Ransomware	S. 22
Remote Administration Tool	S. 23
Rootkit	S. 23
Scareware	S. 24
Spyware	S. 24
Stealer	S. 25
Trojaner	S. 25
USB-Virus	S. 25
Virus	S. 26
Wurm	S. 26

Tool 1: Avast Free Antivirus 6.0	S. 21
Tool 2: Threatfire 4.7.0	S. 22
Tool 3: Kaspersky Rescue Disk 10	S. 24
Tool 4: Virustotal	S. 25
Tool 5: Threat Expert	S. 26

Bootkit

Ein Bootkit startet noch vor Windows und schließt das System wie in einer Kapsel ein.

Ein Bootkit ist ein spezielles Rootkit (➔ Rootkit, Seite 23), das sich im Master Boot Record (MBR) verankert. Damit startet es vor Windows und kann so das Betriebssystem beliebig manipulieren.

So schützen Sie sich: Wenn Sie ein Bootkit auf Ihrem PC vermuten, starten Sie den Rechner mit der Wiederherstellungskonsole, um den MBR zu säubern: Booten Sie vom Windows-Datenträger und drücken Sie [R]. Wählen Sie die Windows-Installation, bei der Sie sich anmelden möchten, und tippen Sie das Kennwort ein. Geben Sie unter XP `fixmbr` ein und bestätigen Sie die Nachfrage mit [J]. Starten Sie den PC neu mit dem Kommando `exit`.

Bei Vista und 7 booten Sie ebenfalls zunächst vom Setup-Datenträger und rufen dann die „Computerreparaturoptionen“ auf. Klicken Sie auf „Ein- ▶

www.pcwebooks2.0

gabeaufforderung“ und geben Sie dann den Befehl **bootrec·/fixmbr** ein, um den MBR zu reparieren. Weitere Informationen finden Sie unter www.com-magazin.de/tipps/2886.

Botnetz

Ein Botnetz ist eine Gruppe verseuchter PCs, die aus der Ferne gesteuert werden und meist massenhaft Spam versenden.

Von einem Botnetz spricht man, wenn zwei oder mehr mit Trojanern (➔ Trojaner, Seite 25) verseuchte PCs über das Internet ferngesteuert werden. Es gibt kleine Botnetze mit einer Handvoll ferngesteuerter Rechner bis hin zu gigantischen Netzen mit mehreren Millionen infizierten Computern (Bild B).

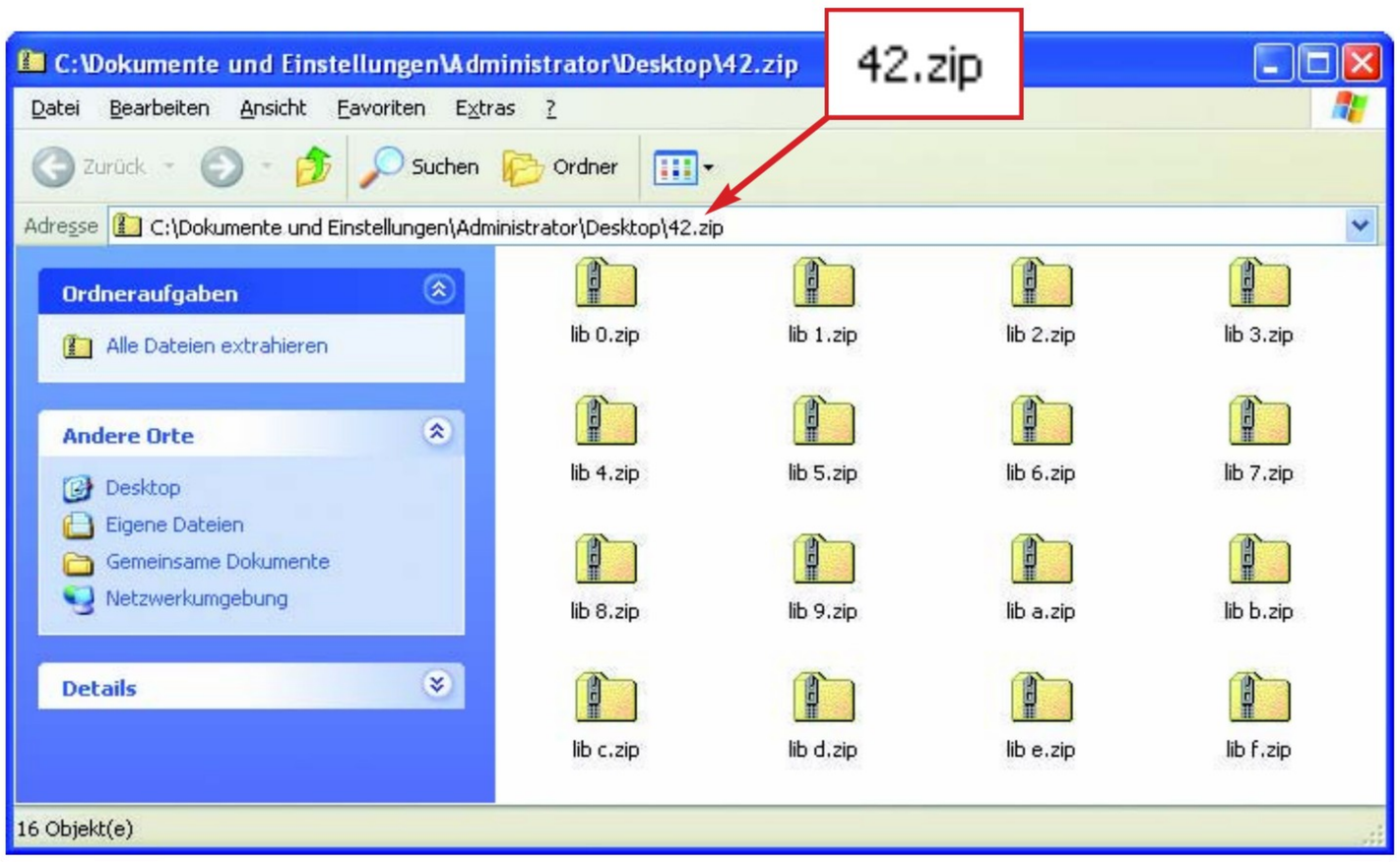
PCs in einem Botnetz werden oft gemeinsam eingesetzt, um große Mengen an Spam zu versenden oder um Internetserver mit Anfragen zu bombardieren und damit lahmzulegen.

So schützen Sie sich: Eine Kombination aus aktuellem Virenscanner (➔ Tool 1, Seite 21) und dem Verhaltenswächter Threatfire 4.7.0 (➔ Tool 2, Seite 22) verhindert Infektionen mit Botviren.

Buffer Overflow

Ein Buffer Overflow ist eine Sicherheitslücke in einem Programm.

Ein Buffer Overflow, zu Deutsch Pufferüberlauf, wird dazu verwendet, um eine Software zum Absturz zu bringen oder um fremden Code einzuschleusen.



Dekomprimierungsbombe: Die nur 42 KByte große Datei „42.zip“ wächst beim Auspacken auf 4500 Terabyte an und soll so den Virenscanner zum Absturz bringen (Bild C)

Dabei wird ein Speicherbereich mit zu vielen Daten gefüllt, so dass es zu einem Absturz kommt. Besonders häufig werden Flash und Java angegriffen. Meist finden sich zu Buffer Overflows auch schnell Exploits (➔ Exploit, Seite 21), die die Lücke ausnutzen.

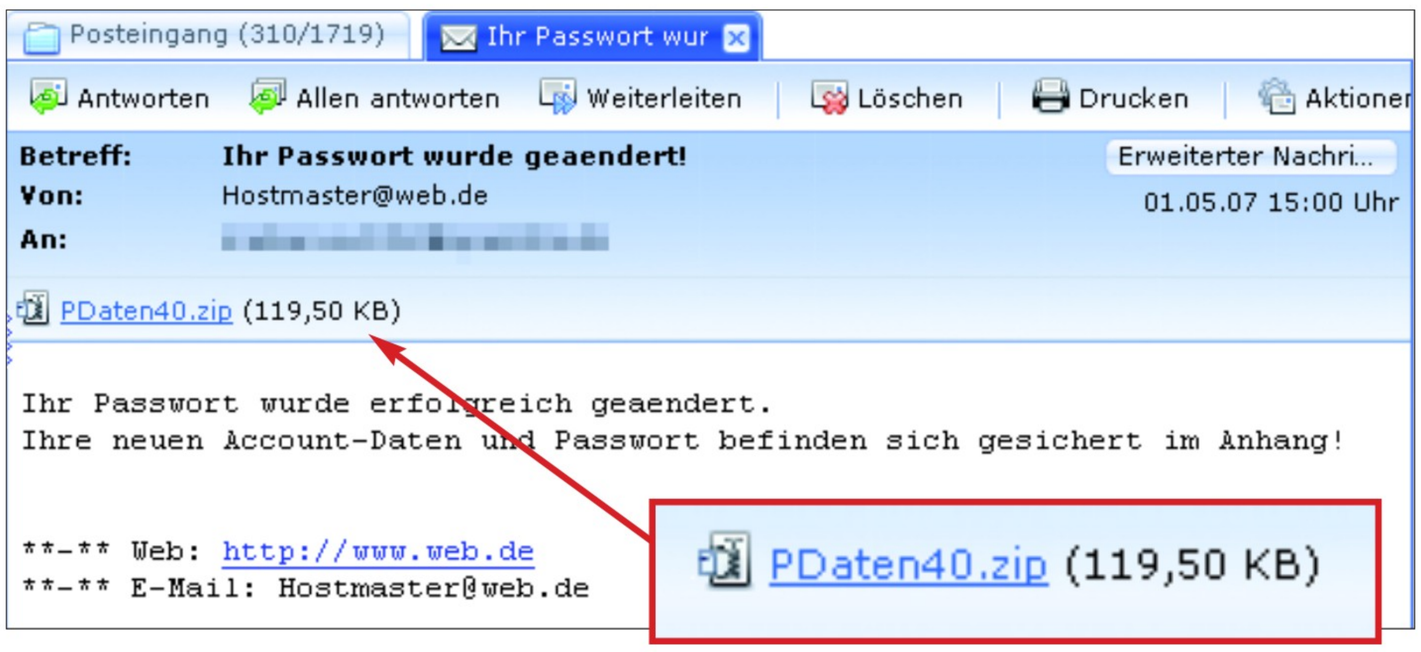
So schützen Sie sich: Halten Sie die Software auf Ihrem PC auf dem aktuellen Stand. Installieren Sie außerdem nur Programme, die Sie auch wirklich benötigen.

Crapware

Crapware ist überflüssiger Schrott, der sich auf vielen vorinstallierten PCs findet.

Manche PC-Hersteller installieren auf ihren Computern Dutzende überflüssiger Programme und Spiele, die den PC nur belasten und keinen Nutzen bringen. Diese Art von Software wird als Crapware bezeichnet. Der Begriff leitet sich vom englischen Wort crap für Schrott ab. Echten Schadcode enthält Crapware meist aber nicht.

So schützen Sie sich: Gegen Crapware hilft kein Antivirenprogramm. Entweder installieren Sie das Betriebssystem selbst neu oder Sie nehmen sich nach dem Kauf eines neuen PCs etwas Zeit und entfernen all die überflüssigen Beigaben. Der Computer läuft dadurch schneller und in den meisten Fällen auch stabiler.



Verseuchte Mail: Viele Schädlinge gelangen über verseuchte Spam-Mails auf fremde PCs. Hier enthält der Anhang „PDaten40.zip“ einen Downloader, der dann einen Trojaner installiert (Bild D)

Dekomprimierungsbombe

Dekomprimierungsbomben sind vielfach gepackte Archive, die einen Virenscanner zum Absturz bringen sollen.

Dekomprimierungsbomben sind speziell gepackte Archive, die den Virenscanner beim Entpacken (Dekomprimieren) abstürzen lassen sollen.

Ein im Internet frei kursierendes Beispiel für eine solche Bombe ist „42.zip“. Die Datei enthält wiederkehrende Daten, die sich sehr effektiv komprimieren lassen. Im gepackten Zustand ist sie nur 42 KByte groß. Im ausgepackten Zustand belegt sie jedoch 4,5 Millionen GByte. Das sind 4500 Terabyte (Bild C).

WinBook 2.0

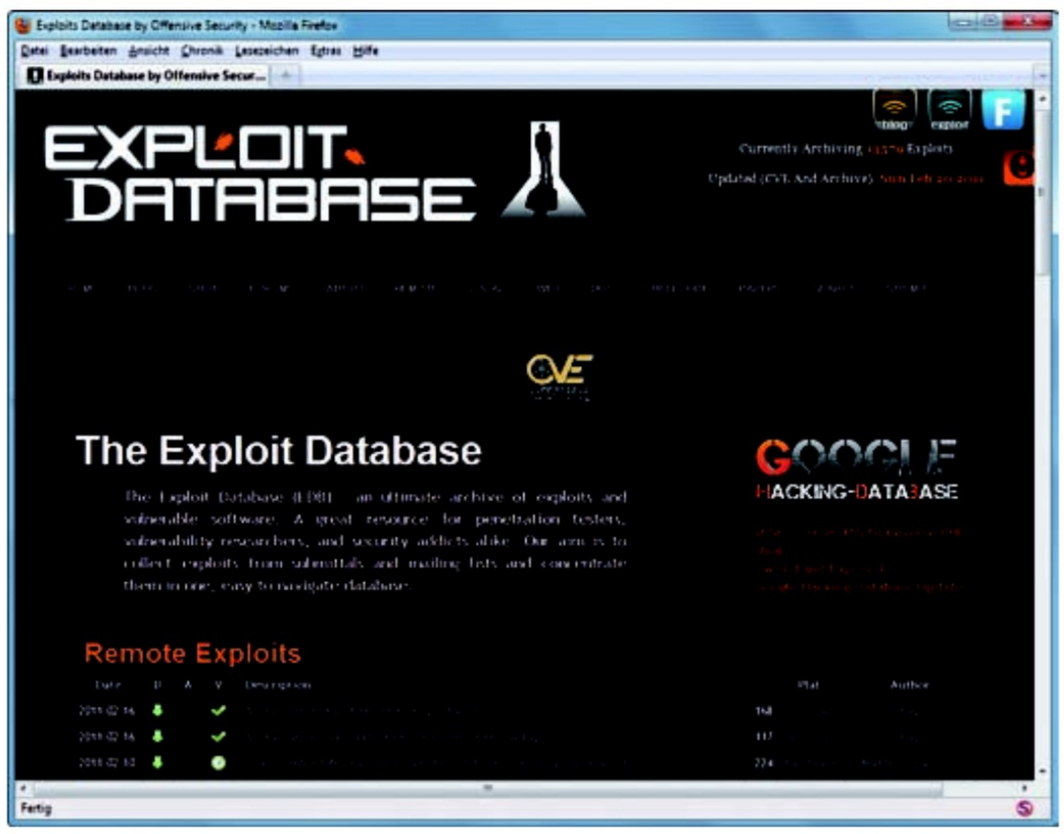
So schützen Sie sich: Heute geht von Dekomprimierungsbomben keine akute Gefahr mehr aus. Die meisten Antivirenprogramme erkennen gefährliche Archive, bevor sie versuchen, diese auszupacken. Ein guter moderner Virenscanner ist Avast Free Antivirus 6.0 (➔ Tool 1, siehe unten).

Downloader

Ein Downloader hat die Aufgabe, weitere Schadprogramme einzuschleusen.

Viren (➔ Virus, Seite 26) und Trojaner (➔ Trojaner, Seite 25) gelangen oft erst über einen Umweg auf einen PC.

Zunächst schleusen die Kriminellen etwa über eine Spam-Mail einen Downloader ein (Bild D), der selbst jedoch keinen echten Schadcode enthält. Der Downloader nimmt dann selbstständig Kontakt mit einem Steuerserver auf und lädt den jeweils aktuellsten Schädling nach.



Exploits: Programme, die gezielt Sicherheitslücken ausnutzen – Exploits genannt – kann jeder aus dem Internet herunterladen (Bild E)

Exploit

Exploits sind Programme, die gezielt Sicherheitslücken ausnutzen.

Ein Exploit – abgeleitet vom englischen to exploit für ausnutzen – ist eine Software, die eine Sicherheitslücke in einem anderen Programm ausnutzt. Exploits werden vor allem dazu benutzt, Schadcode auf einem fremden Computer einzuschleusen. Viele lassen sich frei aus dem Internet herunterladen (Bild E).

So schützen Sie sich: Gegen Exploits hilft es, alle Programme und das Betriebssystem aktuell zu halten. Zusätzliche Sicherheit bietet der Verhaltensschutz von Threatfire 4.7.0 (➔ Tool 2, Seite 22), der auch bei neuen Gefahren wirkt.

Heap Spraying

Heap Spraying ist eine Angriffstechnik, um Schadcode in einen Prozess einzuschleusen.

Meist wird Heap Spraying als Exploit (➔ Exploit, siehe oben) im Browser eingesetzt, indem eine Webseite manipulierten Javascript-Code enthält. Dieser Code überschreibt Teile des Arbeitsspeichers. Dabei wird ein Speicherbereich so lange mit Daten gefüllt, bis er überläuft und der Schadcode ausgeführt wird. Darin ist das Verfahren einem Buffer Overflow (➔ Buffer Overflow, Seite 20) sehr ähnlich.

Auch Besucher auf seriösen Webseiten sind nicht gegen Heap Spraying gefeit. Die Angreifer hacken die Seiten und binden ihren Code über unsichtbare iFrames ein.

Keylogger

Ein Keylogger speichert Tastatureingaben und macht Screenshots.

Ein Keylogger ist ein Schädling, der alle Tastatureingaben aufzeichnet (Bild G). Aktuelle Keylogger erstellen da- ▶

Tool 1: Avast Free Antivirus 6.0

Der kostenlose Virenscanner scannt zuverlässig nach Schädlingen und nervt nicht mit täglichen Werbeeinblendungen.

Eines vorweg: Wenn Sie bereits einen aktuellen Virenscanner installiert haben und mit diesem zufrieden sind, benötigen Sie Avast Free Antivirus 6.0 nicht (kostenlos für Privatanwender, www.avast.com und auf).

Ansonsten lohnt sich jedoch ein Umstieg auf diesen Virenscanner, der den Nutzer nicht mit Werbung nervt.

Das Setup-Programm von Avast bietet die Installation einer „avast! Community" sowie des Google-Browsers Chrome an. Beide haben keinerlei Einfluss auf die Schutzwirkung des Scanners. Sie können also bedenkenlos deaktiviert werden.

Nach der Installation haben Sie 30 Tage Zeit, um das Programm kostenlos zu registrieren. Klicken Sie dazu auf das Avast-Symbol unten rechts im System-Tray und wählen Sie „ÜBERSICHT" aus. Klicken Sie danach auf „Jetzt registrieren, Registrieren". Es öffnet sich ein Fenster, in dem nur „Name" und „E-Mail" Pflichtfelder sind. Ein Klick auf „Sich für die kostenlose Lizenz registrieren" verlängert die Nutzungsdauer um zwölf Monate.

Trojaner, die sich einschleichen wollen, erkennt das Sicherheitsprogramm zuverlässig und blockiert ihre Installation (Bild F).

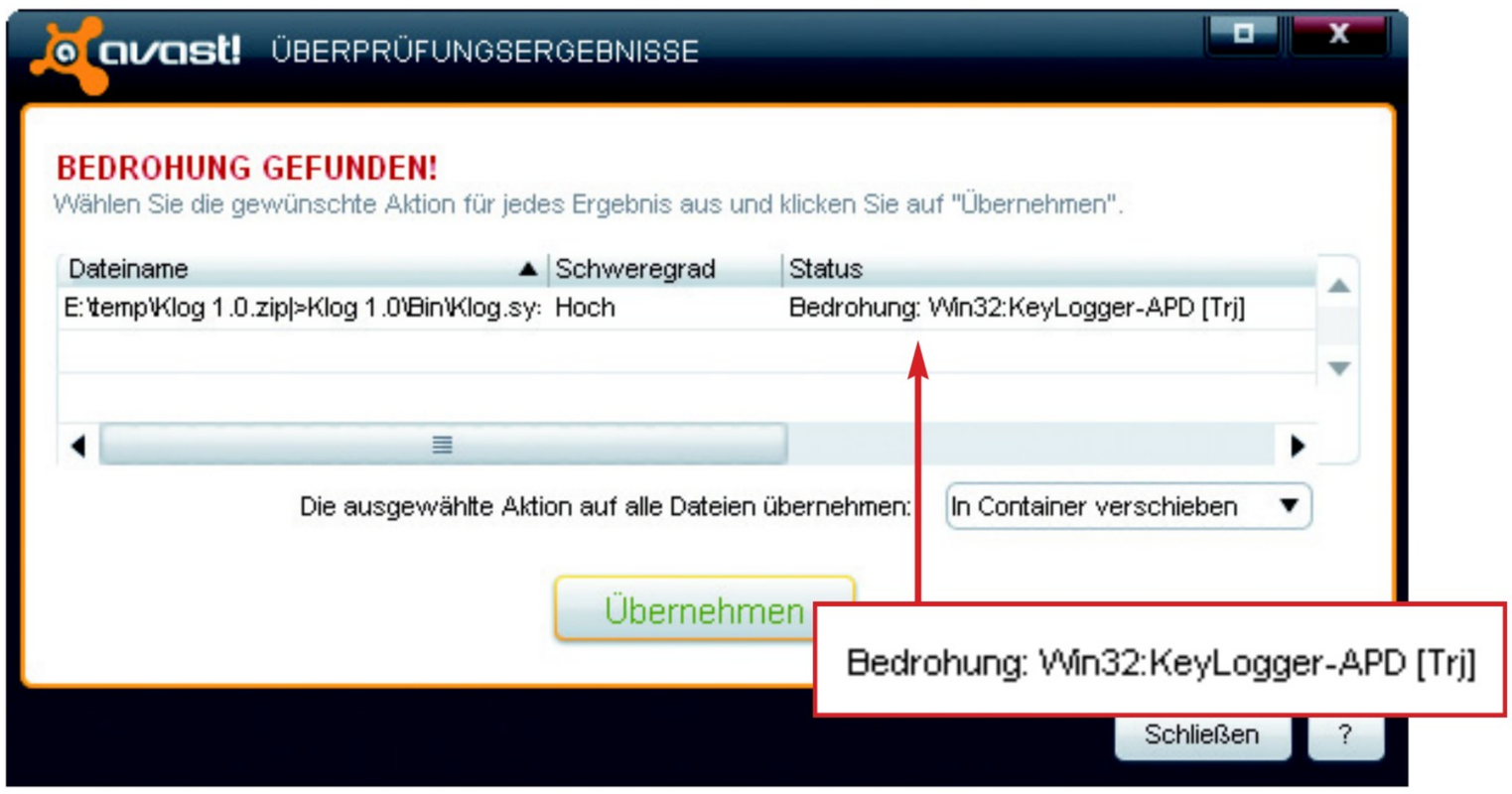
Avast Free Antivirus 6.0: Der Hintergrundwächter hat einen Schädling erkannt und ihn unschädlich gemacht (Bild F)

www.vivobooks2.0

rüber hinaus oft Screenshots des Bildschirminhalts. Die meisten Trojaner (➔ Trojaner, Seite 25) verfügen ebenfalls über Keylogger-Fähigkeiten.

Die vom Keylogger erfassten Daten werden dann von kriminellen Banden eingesammelt und meist als Paket weiterverkauft, zum Beispiel in Form von 1000 gestohlenen Kreditkartendaten.

So schützen Sie sich: Gegen Keylogger helfen ein aktueller Virenscanner wie Avast Free Antivirus 6.0 (➔ Tool 1, Seite 21) und Threatfire 4.7.0 (➔ Tool 2, siehe unten).



Keylogger: Ein Keylogger schneidet Tastatureingaben mit und klaut Zugangsdaten und Passwörter und versendet sie dann per Internet (Bild G)

Malware

Malware ist der Oberbegriff für alle Viren, Trojaner, Würmer und andere Schädlinge.

Malware ist das englische Wort für gefährliche Software. Darunter fallen Viren (➔ Virus, Seite 26), Trojaner (➔ Trojaner, Seite 25), Keylogger (➔ Keylogger, Seite 21) und viele andere in diesem Artikel vorgestellte Gefahren.

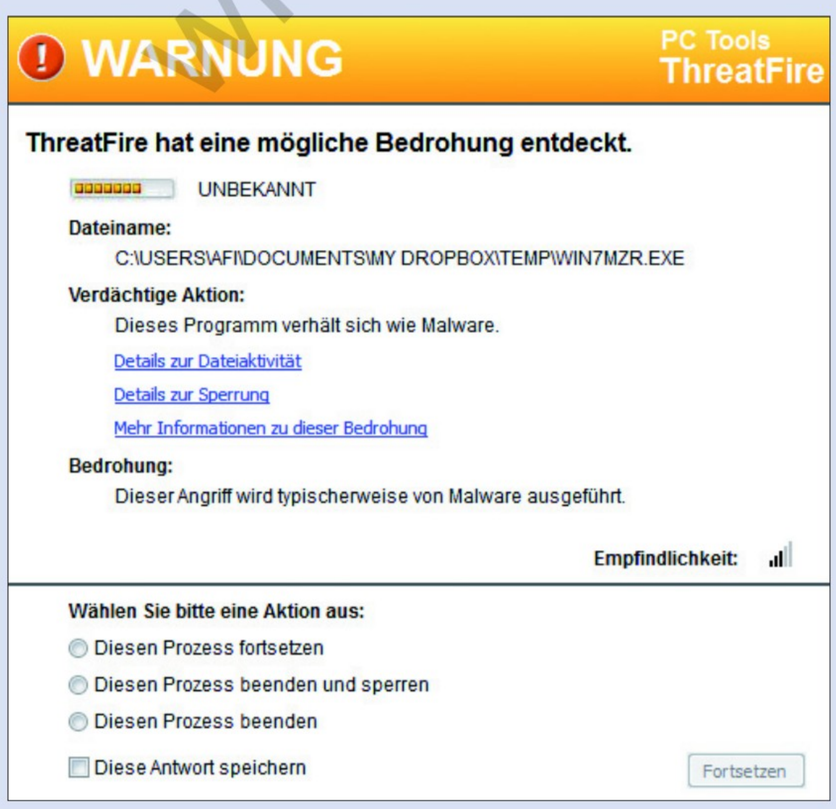
So schützen Sie sich: Der effektivste Schutz gegen Malware besteht in drei Maßnahmen. Die erste ist die Installation eines Virenscanners (➔ Tool 1, Seite 21). Die zweite das regelmäßige Aktualisieren von Betriebssystem und allen installierten Anwendungen. Die dritte ist die Verwendung einer Firewall, die Angriffe von außen verhindert.

Eine Firewall ist in allen aktuellen DSL-Routern und in allen Windows-Versionen seit Windows XP Service Pack 2 enthalten.

Tool 2: Threatfire 4.7.0

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

Eigentlich soll man ja nicht zwei Hintergrundwächter verwenden. Das Tool Threatfire 4.7.0 ist mit seiner verhaltensbasierten Erkennung jedoch die ideale Ergänzung zu einem normalen Virenscanner und läuft in der Regel problemlos nebenher (kostenlos, www.threatfire.com/de und auf).



Threatfire 4.7.0: Der Verhaltenswächter warnt, wenn sich eine Software verdächtig verhält (Bild H)

Eine verhaltensbasierte Suche schützt auch bei neuen, bislang unbekannten Gefahren. Threatfire erkennt einen Schädling beispielsweise daran, dass er mehrere Kopien von sich an verschiedenen Orten auf der Festplatte ablegt und dass er Tastatureingaben mitschneidet und über das Internet versendet. Treffen mehrere verdächtige Eigenschaften zusammen, schlägt das Tool Alarm (Bild H).

Pod Slurping

Von Pod Slurping spricht man, wenn ein USB-Stick Daten von einem PC klaut.

USB-Sticks sind das ideale Werkzeug, um Daten heimlich von einem fremden PC zu kopieren. Während der USB-Stick angeschlossen ist, um etwa Urlaubsfotos anzusehen, kopiert ein USB-Virus (➔ USB-Virus, Seite 25) in aller Ruhe Dokumente auf den Stick.

Der Begriff Pod Slurping ist eine Kombination aus Pod für iPod und dem englischen to slurp, was übersetzt schlürfen heißt. Der Begriff wird auch für USB-Sticks verwendet, die Daten schlürfen.

So schützen Sie sich: Gegen USB-Viren hilft meist der installierte Virenscanner (➔ Tool 1, Seite 21).

Problematisch sind allerdings spezielle Schädlinge, mit denen eine einzelne Person oder Firma angegriffen wird. Zu so einem Virus gibt es meist noch keine Signatur. In diesem Fall schützt der Verhaltenswächter Threatfire 4.7.0 (➔ Tool 2, siehe links).

Ransomware

Ransomware verschlüsselt Dateien oder sperrt den Zugriff auf den PC und fordert dann Geld für die Freigabe.

Anders als praktisch alle aktuellen Trojaner (➔ Trojaner, Seite 25), die im Ver-

WiWobooks 2.0

borgenen ihr Werk verrichten, bemerkt der Anwender eine Infektion mit Ransomware meist sofort. Ransomware verschlüsselt wichtige Dateien, blockiert Dienste oder gaukelt dem Anwender vor, sein Windows sei eine Raubkopie (Bild I).

Um wieder Zugriff zu erhalten, soll der Anwender einen Freischalt-Code beziehungsweise ein Entschlüsselungs-Tool kaufen.

Der Name Ransomware leitet sich vom englischen to ransom ab, was so viel heißt wie erpressen.

Quelle: GFI Labs

Ransomware: Das ist keine echte Microsoft-Meldung, sondern ein erpresserischer Schädling, der den Zugriff auf Windows sperrt (Bild I)

So schützen Sie sich: Das wichtigste Hilfsmittel gegen erpresserische Viren ist Ihr Virenscanner (➔ Tool 1, Seite 21). Schwieriger ist die Lage, wenn der Schädling bereits eingedrungen ist und Ihre Daten verschlüsselt hat. In diesem Fall kann nämlich eine Desinfektion – zum Beispiel mit der Kaspersky Rescue Disk 10 (➔ Tool 3, Seite 24) – zu einem Verlust der Daten führen.

Manche Antiviren-Hersteller haben Tools veröffentlicht, die den PC reinigen oder Dokumente entschlüsseln.

Remote Administration Tool

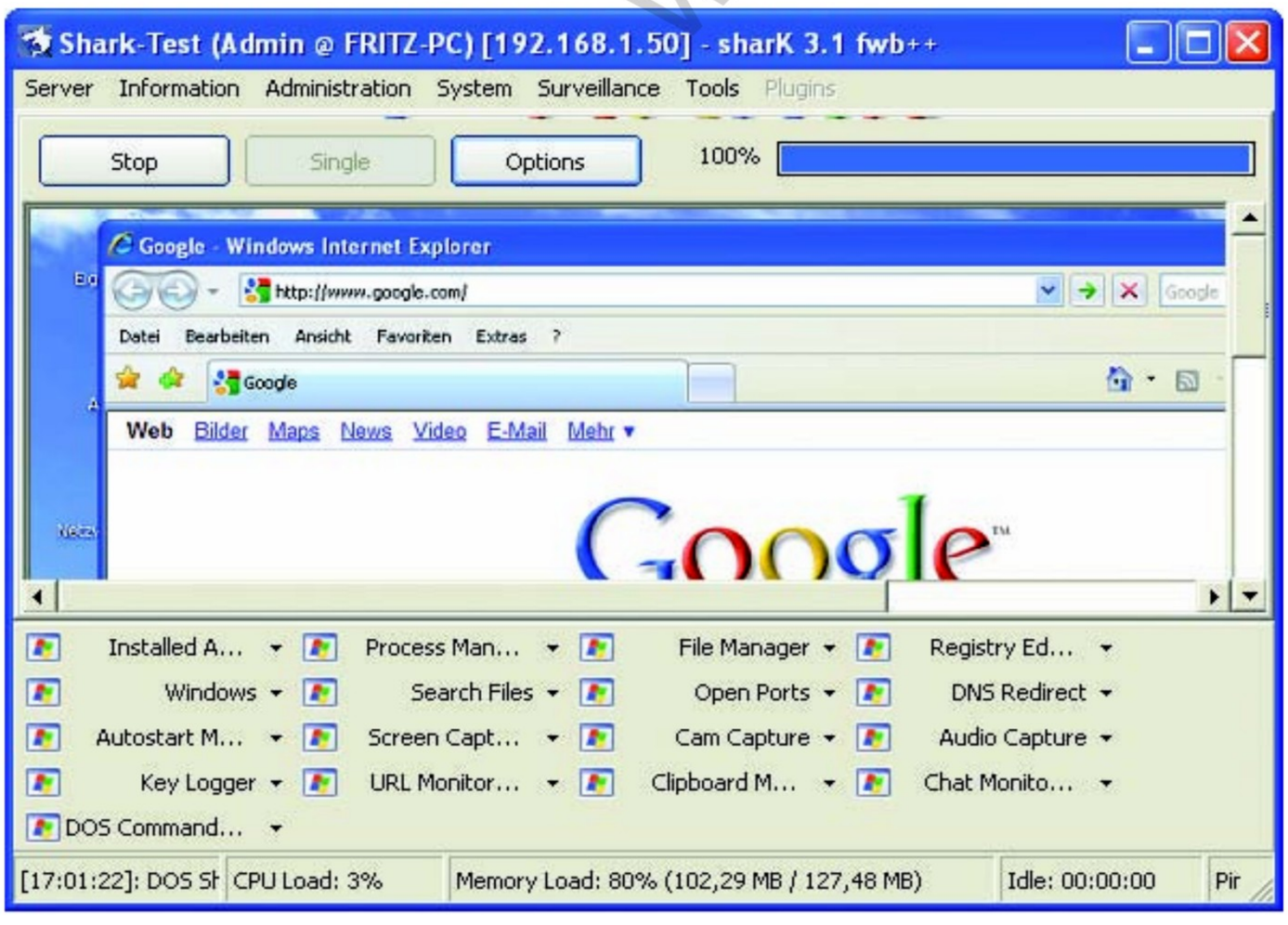
Remote Administration Tools steuern PCs heimlich aus der Ferne.

Software zur Fernsteuerung von Computern wird in Unternehmen und teils auch im Verwandten- oder Bekanntenkreis eingesetzt. Legale Vertreter dieser Softwaregattung zeigen deutlich an, wenn ein PC aus der Ferne kontrolliert wird.

Ganz anders verhalten sich Remote Administration Tools, die nach ihrer Abkürzung auch als RATs (deutsch: Ratten) bezeichnet werden. RATs lassen sich heimlich installieren und weisen auf ihre Anwesenheit auch nicht hin. Der Benutzer des ferngesteuerten PCs merkt also nicht, dass jemand anderes die Kontrolle über seinen Rechner übernommen hat.

Verbreitete Remote Administration Tools sind Back Orifice, Netbus und Shark (Bild J).

So schützen Sie sich: Ein aktueller Virenscanner (➔ Tool 1, Seite 21) erkennt ein RAT in der Regel und entfernt es zuverlässig. Ein Scan mit der Kaspersky Rescue Disk 10 (➔ Tool 3, Seite 24) schafft zudem Sicherheit, dass sich kein RAT auf dem PC befindet.



Remote Administration Tool: Das Hacker-Tool Shark kontrolliert fremde Rechner heimlich über das Internet. Hier sieht man den Bildschirminhalt des ferngesteuerten PCs (Bild J)

Rootkit

Rootkits verbergen Schadcode vor Virenscannern und dem Benutzer.

Ein Rootkit greift tief in das Betriebssystem ein, tauscht Treiber aus oder manipuliert den Windows-Kernel und macht sich so unsichtbar. Deshalb taucht ein aktiviertes Rootkit auch im Windows-Explorer nicht mehr auf – als wäre es auf dem Computer gar nicht vorhanden.

Der Begriff Rootkit stammt ursprünglich aus dem Linux-Umfeld. Dort wurden damit spezielle Tools bezeichnet, die sich erfolgreich vor dem „root“ versteckten, dem Administrator des Linux-Rechners.

So schützen Sie sich: Die Antiviren-CD Kaspersky Rescue Disk (➔ Tool ▶

www.books2.0

Tool 3: Kaspersky Rescue Disk 10

Die Antiviren-CD startet den PC mit einem Linux-System und sucht dann nach Viren.

Von Heft-DVD bootet die Kaspersky Rescue Disk 10, mit der Sie Ihren PC auf Viren prüfen (kostenlos, http://support.kaspersky.com/viruses/rescuedisk?level=2 und auf). Das hat den Vorteil, dass vorhandene Viren sich nicht aktivieren und vor dem Sicherheits-Check schützen können.

Legen Sie die Heft-DVD ein und starten Sie Ihren PC neu. Sie finden die Kaspersky Rescue Disk 10 als ISO-Datei auch unter http://support.kaspersky.com/viruses/rescuedisk?level=2. Brennen Sie die ISO-Datei als bootfähige CD.

Nachdem das System gestartet ist, wählen Sie „Update" aus. Klicken Sie auf „Update ausführen", um die Virensignaturen zu aktualisieren. Das funktioniert jedoch nur, wenn Sie einen DSL-Router mit DHCP (Dynamic Host Control Protocol) verwenden.

Sobald das Update abgeschlossen ist, wechseln Sie wieder zum Reiter „Untersuchung von Objekten" zurück. Ein Klick auf „Untersuchung von Objekten starten" beginnt mit der eigentlichen Suche nach Viren. Findet das Antiviren-System einen Schädling, haben Sie anschließend die Möglichkeit, diesen von Ihrem PC zu entfernen (Bild L).

Kaspersky Rescue Disk 10: Die Antiviren-CD hat einen Downloader in einer EXE-Datei aufgespürt, die sich als PDF tarnt (Bild L)

3, siehe oben) startet Ihren PC mit einem Linux-System und scannt dann nach Schädlingen. Rootkits haben so keine Chance, sich zu aktivieren und vor dem Scanner zu verbergen.

Scareware

Scareware sind gefälschte Sicherheits-Tools, die dem Benutzer Angst einjagen und so zum Kauf nutzloser Software verleiten sollen.

Der Begriff Scareware leitet sich vom englischen to scare, Angst einjagen, ab. Demzufolge versucht Scareware beim Benutzer ein Gefühl der Bedrohung zu erwecken, indem sie ihm beispielsweise eine Infektion seines Computers mit Hunderten Schädlingen vorgaukelt (Bild K).

Damit soll der Nutzer zum Kauf der in der Regel komplett nutzlosen Software gebracht werden. Manche dieser Tools enthalten sogar selbst echten Schadcode und klauen Daten.

So schützen Sie sich: Installieren Sie nur Sicherheitsprogramme bekannter Hersteller. Um Verwechslungen zu vermeiden, überprüfen Sie den Namen jedes Sicherheits-Tools, das Sie installieren wollen oder das sich ohne Ihr Zutun auf Ihrem PC befindet. Sunbelt Software hat eine Liste gefälschter Sicherheitsprogramme zusammengestellt. Sie finden die Liste unter www.sunbeltsecurity.com/BrowseLibrary.aspx. Klicken Sie unten links bei „Misc" auf „Rogue Security Program".

Außerdem finden Sie auf der Webseite www.virustotal.com/about.html#credits eine Liste seriöser Anbieter von Sicherheitssoftware.

Spyware

Moderne Spyware sammelt Daten, speichert Screenshots und macht sogar Fotos mit der Webcam Ihres PCs.

Spyware sind Programme, die sich auf fremden PCs einschleichen, dort Daten sammeln und diese dann per Internet an die Spyware-Urheber senden.

Scareware: Mit gefälschten Virenfunden jagt Scareware dem Anwender Angst ein (Bild K)

Quelle: GFI Labs

wiwobooks 2.0

Die meisten Spyware-Tools klauen Kontodaten, schnüffeln in Dokumenten, schneiden Tastatureingaben mit und erstellen Screenshots des aktuellen Bildschirminhalts. Manche greifen sogar auf die eingebaute Webcam zu, um Fotos des Anwenders zu machen.

So schützen Sie sich: Gegen Spyware-Tools hilft neben einem herkömmlichen Virenscanner (➔ Tool 1, Seite 21) die zusätzliche Installation von Threatfire 4.7.0 (➔ Tool 2, Seite 22).

Stealer

Ein Stealer klaut die Zugangsdaten zu Online-Diensten und -Spielen.

Stealer sind Schadprogramme, die gezielt Kennungen und Passwörter klauen. Der Begriff kommt vom englischen Wort für stehlen.

Die meisten Stealer spionieren die Zugangsdaten zu Online-Diensten wie Facebook, Twitter, Ebay und Webmailern sowie zu Spielen wie World of Warcraft aus und versenden sie dann über das Internet. Praktisch jeder aktuelle Trojaner (➔ Trojaner, siehe unten) und Wurm (➔ Wurm, Seite 26) verfügt ebenfalls über eine Funktion zum Klauen von Zugangsdaten.

So schützen Sie sich: Wie auch bei anderen Schädlingen hilft eine Kombination aus Virenscanner (➔ Tool 1, Seite 21) und Verhaltenswächter (➔ Tool 2, Seite 22) gegen Stealer. Seien Sie außerdem vorsichtig bei E-Mails, die Sie zum Aufrufen einer Webseite auffordern, um dort Ihre Kontodaten zu überprüfen. Dabei handelt es sich meist um Phishing-Mails, die Sie auf gefälschte Webseiten locken wollen.

Trojaner

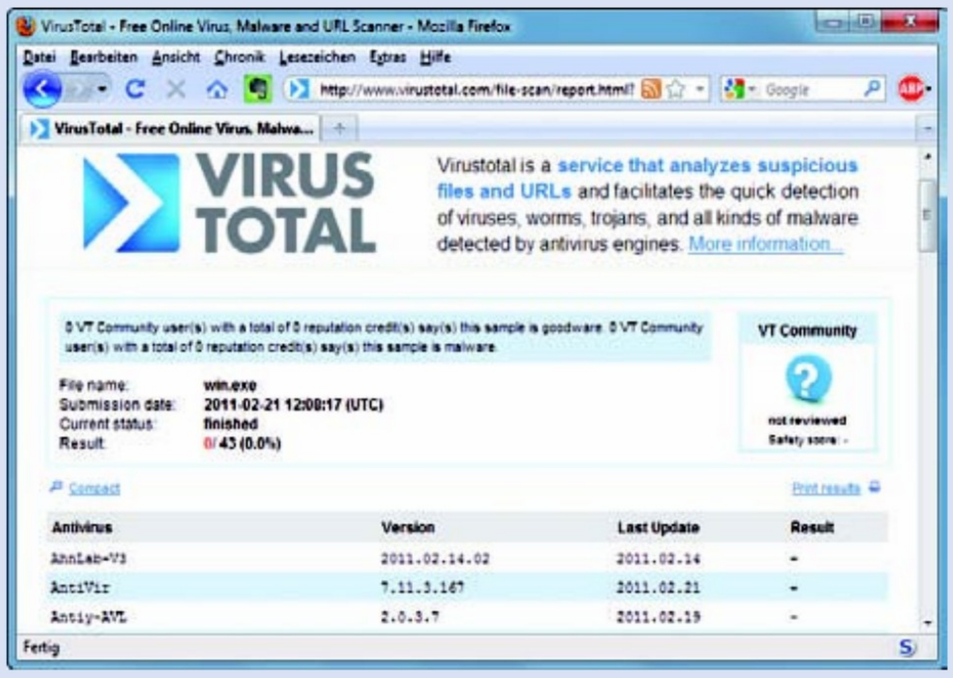
Ein Trojaner tarnt sich als nützliche Anwendung, spioniert aber in Wirklichkeit den Anwender aus.

Trojaner oder genauer Trojanische Pferde sind als nützliche Programme getarnt, indem sie etwa den Dateinamen einer bekannten Datei benutzen oder neben ihrem versteckten Schadcode tatsächlich eine nützliche Funktion haben. Häufig werden mit dem Begriff Trojaner aber auch einfach alle Arten von verborgenen Schädlingen bezeichnet.

So schützen Sie sich: Das Eindringen eines Trojaners in den Computer verhindern Sie am besten mit einer Kombination aus einem herkömmlichen Virenscanner (Bild M) wie Avast Free Antivirus 6.0 (➔ Tool 1, Seite 21) und der Spezialsoftware Threatfire 4.7.0 (➔ Tool 2, Seite 22).

Tool 4: Virustotal

Der kostenlose Online-Dienst prüft jede hochgeladene Datei mit mehr als 40 Virenscannern.



Virustotal: Die Webseite scannt jede hochgeladene Datei mit 43 Virenscannern (Bild N)

Ein Check mit Virustotal (www.virustotal.com) findet heraus, ob eine Datei mit einem Virus verseucht ist oder nicht (Bild N). Die Webseite ist leicht zu bedienen: Klicken Sie auf „Durchsuchen …“, wählen Sie die verdächtige Datei aus und bestätigen Sie mit „Öffnen, Send file“. Der Browser lädt die fragliche Datei dann hoch. Nach kurzer Zeit beginnt sich das Fenster mit den Ergebnissen zu füllen.

Nicht immer ist das Ergebnis jedoch eindeutig. Glauben nur wenige Scanner einen Schädling entdeckt zu haben, handelt es sich eventuell um einen Fehlalarm. Laden Sie die Datei dann auch bei Threat Expert (➔ Tool 5, Seite 26) hoch. Der Dienst startet die Datei in einer abgesicherten Sandbox und wertet dann ihre Aktionen aus.

USB-Virus: Der Schädling manipuliert das USB-Menü, damit Sie ihn starten. Unten sehen Sie den echten Menüeintrag, oben den gefälschten (Bild O)

USB-Virus

USB-Viren verbergen sich auf USB-Sticks und klauen dann heimlich Daten von fremden Computern.

Ein USB-Virus ist ein spezieller Virus, der auf einem USB-Stick versteckt ist und darauf wartet, dass der Stick an einen PC angeschlossen wird. Dann beginnt der USB-Virus damit, heimlich Dokumente auf den Stick zu kopieren.

Weil aktuelle Windows-Versionen Dateien auf USB-Sticks nicht mehr automatisch starten, verwenden USB-Viren andere Tricks, um sich zu aktivieren. So manipulieren sie etwa die ▶

www.pcbooks 2.0

Ordneransicht im USB-Menü (Bild O). Ein anderer Trick ist es, wenn jemand ein präpariertes Tool auf dem Stick startet, um beispielsweise ein darauf befindliches Foto anzuzeigen oder um eine Präsentation zu starten. Dabei wird dann der USB-Virus aktiviert. Diese Technik wird auch als Pod Slurping (➔ Pod Slurping, Seite 22) bezeichnet.

So schützen Sie sich: Der beste Schutz gegen USB-Viren ist der Einsatz eines Virenscanners (➔ Tool 1, Seite 21) zusammen mit Threatfire 4.7.0 (➔ Tool 2, Seite 22). Außerdem sollten Sie nur möglichst wenige oder gar keine fremden USB-Sticks an Ihrem Rechner erlauben.

Virus

Ein Virus infiziert einen PC mit Schadcode und verbreitet sich anschließend weiter.

Viren verbreiten sich über infizierte Dateien, die ein Anwender per Doppelklick startet. Im Gegensatz dazu verteilen sich Würmer (➔ Wurm, siehe rechts) automatisch und ohne Zutun des PC-Nutzers.

Die Bezeichnung wird häufig auch als Oberbegriff für alle Arten von Schädlingen verwendet.

So schützen Sie sich: Der beste Schutz gegen Viren sind der Virenscanner (➔ Tool 1, Seite 21) sowie der Verhaltenswächter Threatfire 4.7.0 (➔ Tool 2, Seite 22). Bereits eingedrungene Viren lassen sich mit der Kaspersky Rescue Disk 10 (➔ Tool 3, Seite 24) entfernen.

Trojaner gefunden: Der Virenscanner, in diesem Fall Microsoft Security Essentials, hat die Installation eines Trojaners verhindert (Bild M)

Wurm

Ein Wurm verbreitet sich automatisch über das Internet oder zum Beispiel über USB-Sticks.

Würmer verbreiten sich über Sicherheitslücken im Betriebssystem oder in installierten Anwendungen. Ist ein PC erst einmal mit einem Wurm verseucht, dann verteilt er anschließend selbst den Schädling weiter. So infizieren Würmer in kürzester Zeit Abertausende Rechner. Manche Vertreter, etwa Conficker, sollen in kürzester Zeit sogar mehr als 50 Millionen PCs verseucht haben.

So schützen Sie sich: Halten Sie Betriebssystem und installierte Programme immer auf dem aktuellsten Stand. Nur so ist Ihr PC weitgehend vor Sicherheitslücken geschützt, über die Würmer eindringen können.

Sie finden die Einstellungen für Windows-Update in XP unter „Start, Systemsteuerung, Sicherheitscenter“. Klicken Sie auf „Automatische Updates“ und aktivieren Sie die Option „Empfohlene Updates automatisch herunterladen (…)“.

Unter Vista und Windows 7 rufen Sie „Start, Systemsteuerung, System und Sicherheit, Automatische Updates aktivieren oder deaktivieren“ auf. Wählen Sie „Nach Updates suchen, aber Zeitpunkt zum Herunterladen und Installieren manuell festlegen“, wenn Sie selbst genau bestimmen wollen, wann die Updates installiert werden.

Oder Sie wählen „Updates automatisch installieren (empfohlen)“ aus. Dann brauchen Sie sich nicht weiter um die Aktualisierungen zu kümmern. ■

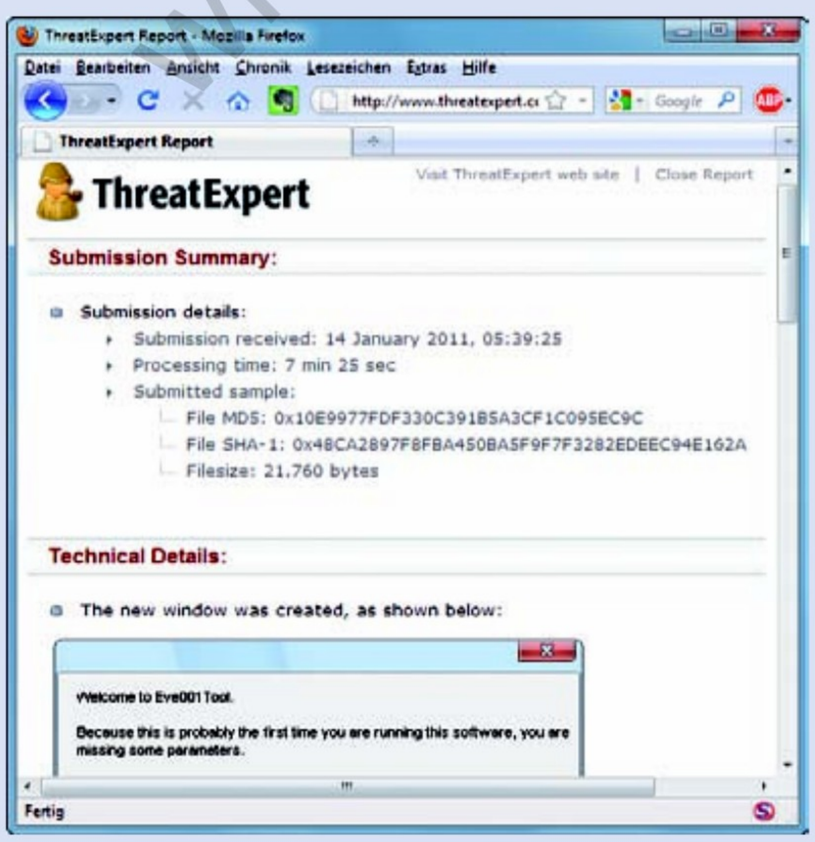
Andreas Th. Fischer
sonderheft@com-magazin.de

Tool 5: Threat Expert

Threat Expert startet hochgeladene Dateien in einer abgeschotteten Sandbox.

Das Besondere an dem Dienst Threat Expert (kostenlos, www.threatexpert.com) ist, dass die Webseite verdächtige Dateien in einer Sandbox laufen lässt. Aus dem Verhalten der Datei in der Sandbox und einem Virencheck mit acht Scannern erstellt der Dienst dann einen ausführlichen Report, der sogar Screenshots enthält (Bild P).

Senden Sie die fragliche Datei über www.threatexpert.com/submit.aspx an Threat Expert. Nach wenigen Minuten erhalten Sie eine E-Mail mit einem Link zu dem Prüfergebnis. Außerdem ist der Nachricht eine Datei im ZIP-Format angehängt, die den kompletten Bericht enthält. Das Passwort, um dieses Archiv zu öffnen, lautet `threatexpert`.



Threat Expert: Die Webseite startet hochgeladene Dateien in einer Sandbox und erstellt einen Bericht mit Screenshots (Bild P)

Weitere Infos

- www.viruslist.com/de/viruses/encyclopedia
  Umfangreiches Viren-Lexikon plus Hintergrundartikel

www.wowbooks2.0

STRATO

Bei unserer Bilderflut brauchen wir einen starken Partner – unser V-Server von STRATO überzeugt in jeder Minute.

Maria Courtial
Jörg Courtial

Maria und Jörg Courtial
(Gründer des Unternehmens)
www.faber-courtial.de
Website liegt auf einem STRATO V-Server

STRATO V-Server

Jede Menge Leistung zum Spitzenpreis

Neu!

Virtual Windows Server - die ideale Lösung für eine Vielzahl von Anwendungen

- ✓ Virtualisierungslösung Microsoft Hyper-V Server 2008 R2
- ✓ Bis zu 4 GB RAM und 200 GB Festplatte (RAID 1)
- ✓ Microsoft SQL Server, . NET Framework
- ✓ Unlimited Traffic, garantierter RAM, Admin-Rechte

Virtual Windows Server

statt ~~12,90~~
dauerhaft ab: **9,90** €/mtl.

Keine Einrichtungsgebühr!
Keine Vertragsbindung!

Preisaktion bis zum 31.05.2011

com! Hoster des Jahres 2011 WHD 2011
(Leserwahl Ausgabe 6/11)

Jetzt bestellen unter: **strato.de/server**

Servicetelefon: 0 18 05 - 007 677
(0,14 €/Min. aus dem dt. Festnetz, Mobilfunk max. 0,42 €/Min.)

Preis inkl. MwSt.

wiwobooks 2.0

Virenalarm – was tun?

Es ist passiert: Der Virenscanner schlägt Alarm und warnt vor einem Virus. Statt in Panik zu geraten, befolgen Sie zehn einfache Schritte und befreien Ihren PC von Viren und anderen Schädlingen.

Ein Anwender, der auf seinem Rechner einen Virus findet, stellt sich zunächst viele Fragen: Handelt es sich um einen gefährlichen Virus? Was hat der Schädling auf meinem PC angerichtet? Wurden persönliche Daten geklaut? Befinden sich vielleicht noch mehr Viren auf dem PC?

Der Artikel zeigt zuerst, wie Sie zusätzliche Informationen über den Virus finden. Dann stellt er fünf Sicherheits-Tools vor, die weitere Viren auf dem PC aufspüren – meist installiert ein erster Schädling nämlich noch weitere Schadprogramme und versteckt sie.

Kompakt

- ***Der Artikel zeigt, nach welchem Muster Sie nach einem Virenfund am besten vorgehen.***
- ***Alle Tools finden Sie auf Heft-DVD sowie kostenlos im Internet.***

Außerdem lesen Sie, wie Sie besonders hartnäckige Viren und ihre Reste löschen, wenn deren Dateien durch Windows gesperrt sind.

Informationen sammeln

Der erste wichtige Schritt nach einem Virenfund ist die Suche nach weiteren Informationen über den Schädling. Dazu zählen insbesondere die verschiedenen Bezeichnungen, unter denen er er-

Fotos: Mathias Vietmeier

Inhalt

Virenalarm – was tun?

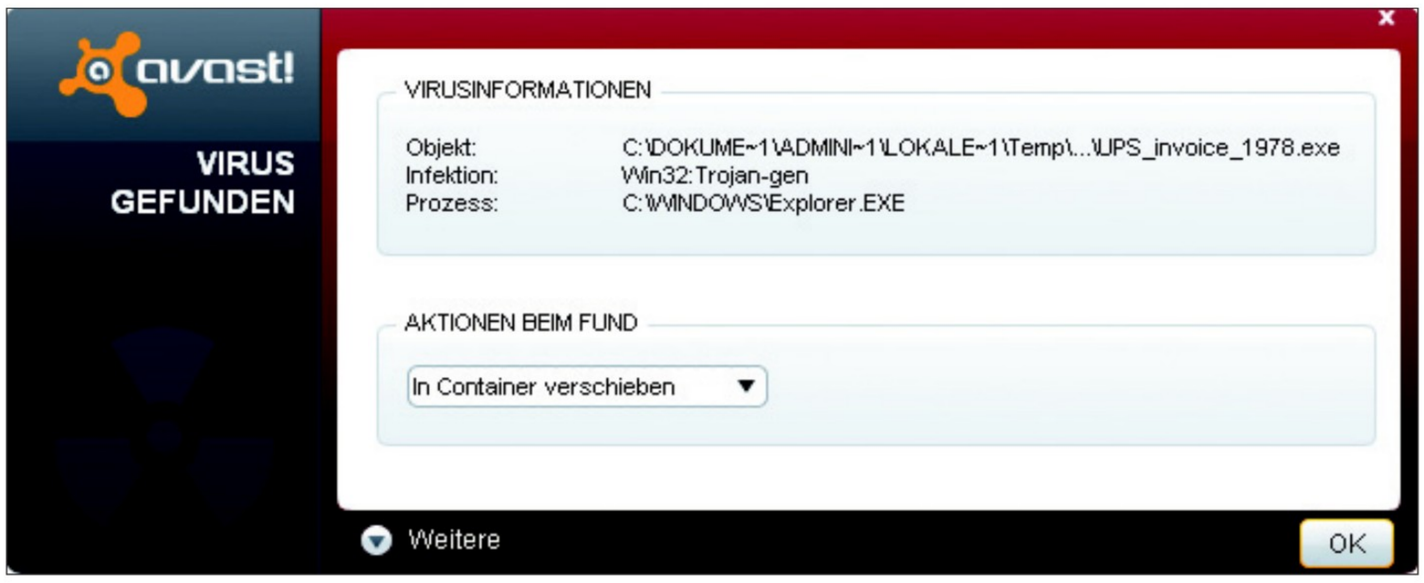
- **Informationen sammeln**
  - 1. Check mit Virustotal S. 29
  - 2. Recherche im Internet S. 29
  - 3. Test mit Threat Expert S. 29
- **Noch mehr Viren?**
  - 4. F-Secure Online-Scanner 4.2 S. 30
  - 5. Bitdefender Free Edition 2009 S. 30
  - 6. Anti-Malware 1.50.1 S. 31
  - 7. Antivir Rescue System 3.7.16 S. 31
  - 8. Rootkit Buster 3.60 S. 32
- **Hartnäckige Viren löschen**
  - 9. Löschen mit Unlocker 1.9.0 S. 32
  - 10. Aufräumen mit Blitzblank 1.0 S. 33

Software-Übersicht S. 30

So geht's: Enttarnen Sie Schädlinge mit Threat Expert S. 30

Info: Fehlalarm S. 32

Info: Virenkürzel S. 33



Virenfund: Notieren Sie den Namen der infizierten Datei. Lassen Sie die Datei dann von der kostenlosen Webseite Virustotal (www.virustotal.com) untersuchen (Bild A)

kannt wird, sowie die Anzahl der Kopien, die er von sich erstellt, und die Information, wo er sie ablegt. Dabei sind besonders die beiden Webseiten Virustotal und Threat Expert nützlich.

Als Beispiel dient eine Infektion mit dem Trojaner Bredolab, der sich vor allem über E-Mails und verseuchte Anhänge verbreitet.

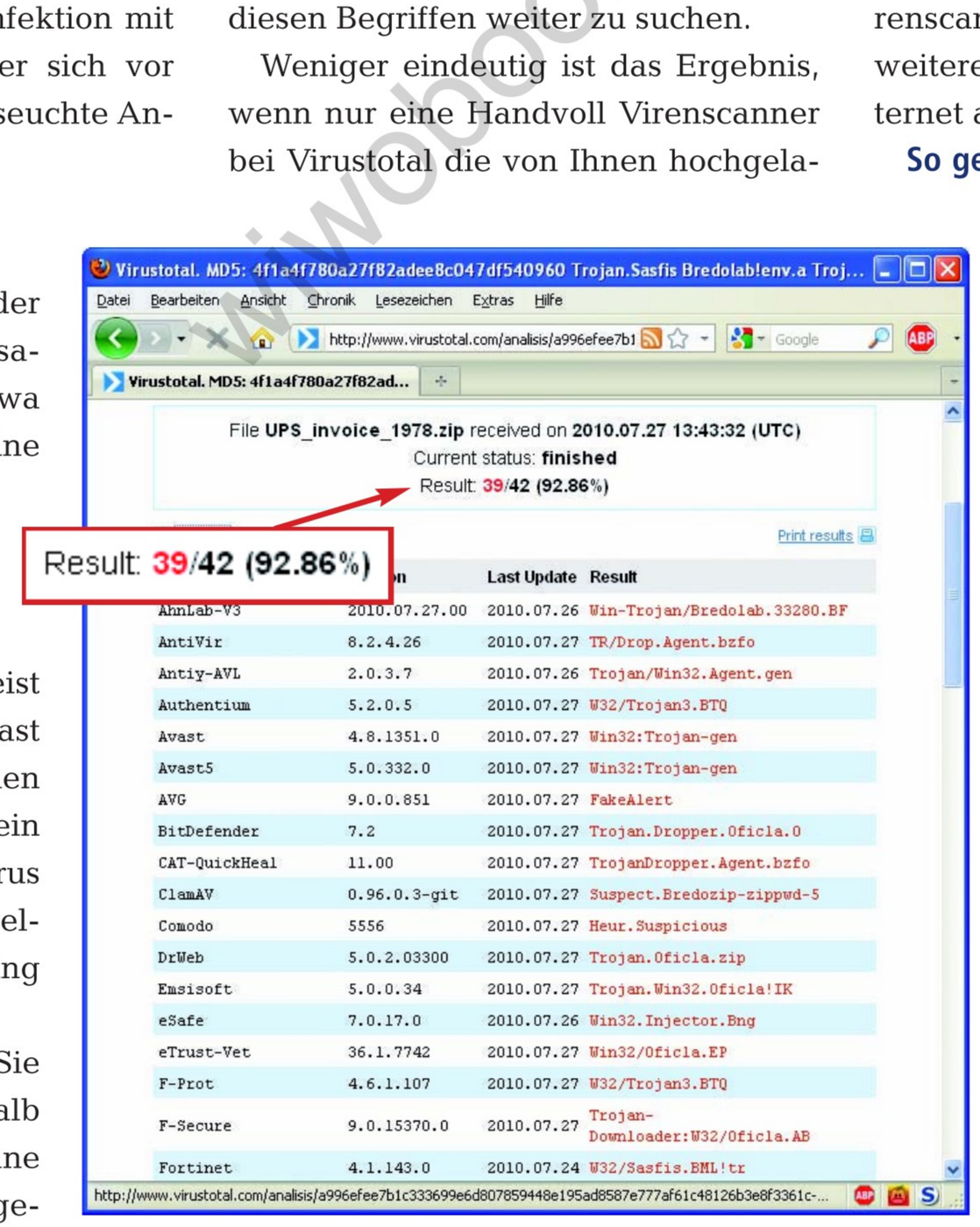
1. Check mit Virustotal

Oft sind die Warnfenster der Virenscanner nicht sehr aussagekräftig. So meldet etwa Avast 5.0 beim Versuch, eine mit Bredolab verseuchte Datei zu öffnen, eine Infektion mit „Win32:Trojan-gen". Diese Bezeichnung ist sehr ungenau und beweist eigentlich nur, dass Avast nicht genau weiß, um welchen Virus es sich handelt. Erst ein Scan mit Virustotal (www.virustotal.com) zeigt, unter welchen Namen der Schädling bereits bekannt ist.

So geht's: Verschieben Sie die fragliche Datei deshalb nicht sofort in die Quarantäne – von Avast „Container" genannt. Laden Sie den Schädling unter www.virustotal.com hoch und lassen Sie ihn dort von 42 Virenscannern prüfen (Bild A).

Das Ergebnis ist im Fall von Bredolab eindeutig: Rund 39 der bei Virustotal eingebundenen Virenscanner haben den Schädling erkannt (Bild B) und in den meisten Fällen auch eine eindeutige Bezeichnung zurückgemeldet. Besonders häufig tauchen in der Liste sowohl die Bezeichnung „Bredolab" als auch „Oficla" auf. Es lohnt sich also, nach diesen Begriffen weiter zu suchen.

Weniger eindeutig ist das Ergebnis, wenn nur eine Handvoll Virenscanner bei Virustotal die von Ihnen hochgeladene Datei als Schädling einstufen. In diesem Fall sollten Sie die fragliche Datei bei Threat Expert hochladen, wie im übernächsten Abschnitt beschrieben. Vergessen Sie aber nicht, den Schädling nach den Tests in die Quarantäne zu verschieben.



Check mit Virustotal: In diesem Beispiel stufen 39 von 42 Virenscannern die hochgeladene Datei als schädlich ein (Bild B)

2. Recherche im Internet

Die Virennamen, die Sie über Virustotal herausgefunden haben oder die Ihr Virenscanner gemeldet hat, dienen dazu, weitere Informationen und Tipps im Internet aufzuspüren.

So geht's: Geben Sie die Namen einfach bei Google ein und rufen Sie einige der Ergebnisse auf. Speziell in Online-Foren finden sich oft gute Tipps zur Bereinigung.

Eine hilfreiche Informationsquelle ist auch die große Virendatenbank von Kaspersky Lab unter www.securelist.com/en/descriptions. Allein zu Bredolab finden sich in dieser Datenbank mehr als 9000 Einträge. Klicken Sie auf einen Eintrag, um zum Beispiel zu erfahren, welche Dateien der Schädling anlegt (Bild C).

3. Test mit Threat Expert

Threat Expert (www.threatexpert.com) ist ein kostenloser Online-Dienst, der hochgeladene Dateien in einer abgeschotteten Sandbox ausführt und analysiert. Zusätzlich ▶

Wiwobooks 2.0

Software-Übersicht

Programm	Quelle	Seite
Anti-Malware 1.50.1 (Trojaner-Jäger)	www.malwarebytes.org/mbam.php	31
Avira Antivir Rescue System 3.7.16 (Antiviren-CD)	www.avira.com	31
Bitdefender Free Edition 2009 (Virenscanner)	www.bitdefender.de	30
Blitzblank 1.0 (Lösch-Tool)	www.emsisoft.de/de/software/blitzblank	33
Rootkit Buster 3.60 (Rootkit-Jäger)	www.trendmicro.com/download/rbuster.asp	32
Unlocker 1.9.0 (Lösch-Tool)	http://unlocker.emptyloop.com	32

Alle -Programme finden Sie auf Heft-DVD in der Rubrik „Windows, Virenalarm“ und im Internet auf den Websites der Hersteller.

prüft Threat Expert die Datei mit mehreren Virenscannern. Aus den Ergebnissen erstellt der Dienst einen ausführlichen Report, der viele nützliche Informationen zu dem Schädling enthält.

So geht's: Senden Sie die fragliche Datei über www.threatexpert.com/submit.aspx an Threat Expert. Nach wenigen Minuten erhalten Sie eine E-Mail mit einem Link zu dem Prüfergebnis. Außerdem ist der Nachricht eine Datei im ZIP-Format angehängt, die den kompletten Bericht enthält. Das Passwort, um dieses Archiv zu öffnen, lautet `threatexpert`. Der nebenstehende Kasten erläutert, wie das Scan-Ergebnis zu interpretieren ist.

Noch mehr Viren?

Ein PC, auf dem ein Virus entdeckt wurde, sollte auf jeden Fall mit weiteren Sicherheitsprogrammen untersucht werden. Meist lädt ein Schädling weitere Viren herunter und installiert sie heimlich.

Im Folgenden finden Sie Tipps zu vier Sicherheits-Tools und einem Online-Dienst, die jeweils ihre eigene Scan-Technik und eigene Signaturen haben, um Viren aufzuspüren.

Konflikte mit dem auf dem PC installierten Virenscanner sind nicht bekannt.

4. F-Secure Online-Scanner 4.2

Der F-Secure Online-Scanner 4.2 ist eine Java-Anwendung, die in jedem Browser läuft. Falls Java noch nicht auf Ihrem PC installiert ist, finden Sie alle benötigten Komponenten zum kostenlosen Download unter www.java.com.

So geht's: Rufen Sie zunächst die Seite www.f-secure.com/en_EMEA-Labs/security-threats/tools/online-scanner auf. Wählen Sie dann die Sprache, setzen Sie ein Häkchen vor „Ich habe die Lizenzbedingungen gelesen und stimme diesen zu“ und klicken Sie auf „Prüfung durchführen“. Der Online-Scanner startet jetzt.

Wählen Sie „Vollständiger Scan“ aus und bestätigen Sie mit „Start“. Die Anwendung lädt nun alle benötigten Dateien herunter und startet danach automatisch. Sobald der Scan durchgelaufen ist, erhalten Sie eine Meldung, ob und wie viele Viren gefunden wurden.

Außerdem haben Sie die Möglichkeit, zu entscheiden, wie mit den Funden umgegangen wird. Wählen Sie „Ich möchte von Datei zu Datei entscheiden“ aus und klicken Sie auf „Weiter“. Auf der folgenden Seite sehen Sie eine ausführliche Übersicht über die Schädlinge (Bild D). Klicken Sie auf „Weiter“, um die gefundenen Viren zu löschen.

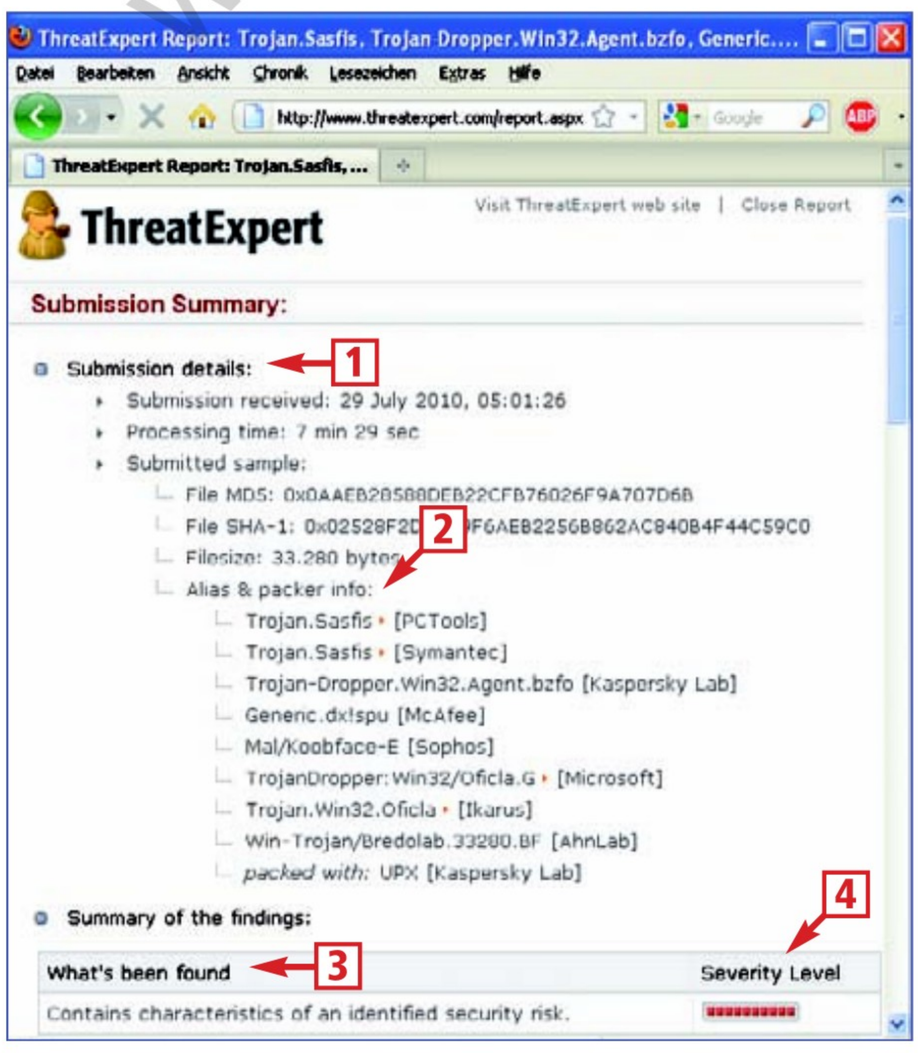
5. Bitdefender Free Edition 2009

Der kostenlose Virenscanner Bitdefender Free Edition 2009 verfügt über keinen Hintergrundwächter. Er eignet sich daher gut als Zweitscanner (kostenlos, www.bitdefender.de und auf).

www.books 2.0

So geht's: Enttarnen Sie Schädlinge mit Threat Expert

Die Webseite Threat Expert (www.threatexpert.com) startet jede hochgeladene Datei in einer abgeschotteten Sandbox. Dort wird die Datei analysiert und von mehreren Virenscannern überprüft.



1 Submission details
Hier finden Sie allgemeine Infos über die hochgeladene Datei.

2 Alias & packer info
Wurde ein Virus gefunden, steht hier der Name und dahinter der verwendete Scanner.

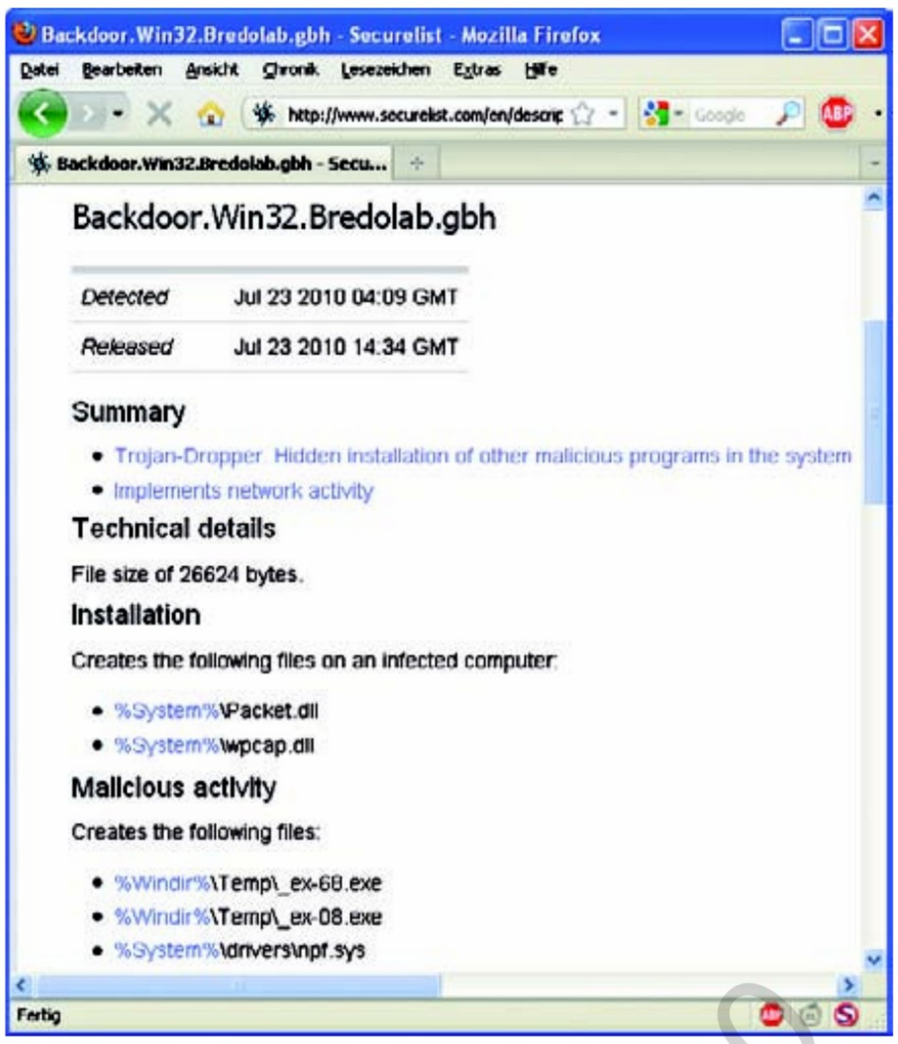
3 What's been found
Die Liste zeigt die wichtigsten Eigenschaften des Schädlings.

4 Severity Level
Ähnlich wie bei einer Ampel sehen Sie hier auf einen Blick, wie gefährlich die Datei ist.

So geht's: Nach der Installation und einem Neustart des Computers öffnen sich zwei Fenster automatisch. Klicken Sie auf „Fortfahren“ und wählen Sie dann „Später registrieren“ sowie „Fertigstellen“ aus, um mit der Überprüfung Ihres PCs zu beginnen.

Öffnen Sie dann die Bedienoberfläche mit einem Doppelklick auf das rote Bitdefender-Icon im System-Tray unten rechts. Wählen Sie „Update (Aktualisierung)“ aus und klicken Sie auf „Jetzt aktualisieren“.

Wählen Sie dann „Antivirus“ sowie den Punkt „Systemprüfung“ aus. Ein Klick auf das Symbol rechts neben „Systemprüfung“ startet den Scan-Vorgang. Standardmäßig ist der Scanner so eingestellt, dass gefundene Schädlinge automatisch gelöscht werden.



Vireninfos von Kaspersky: In der kostenlosen Online-Datenbank erfahren Sie, aus welchen Dateien der Virus besteht (Bild C)

6. Anti-Malware 1.50.1

Anti-Malware 1.50.1 ist wegen seiner schnellen und gründlichen Suche eines der besten Tools gegen Trojaner (kostenlos, www.malwarebytes.org/mbam.php und auf).

So geht's: Nach der Installation aktualisiert Anti-Malware zuerst seine Signaturen. Sobald die Oberfläche des Schutz-Tools gestartet ist, markieren Sie unter „Scanner“ die Option „Vollständigen Suchlauf durchführen“ und klicken auf „Scan“. Markieren Sie in dem kleinen Einstellungsfenster, das sich jetzt öffnet, alle Laufwerke und bestätigen Sie mit „Scan starten“.

Nachdem der Suchlauf beendet ist, klicken Sie auf „OK“ und „Ergebnisse anzeigen“. Schließen Sie alle geöffneten Anwendungen, bevor Sie mit „Entferne Auswahl“ die gefundenen Schädlinge in Quarantäne verschieben“ (Bild E).

7. Antivir Rescue System 3.7.16

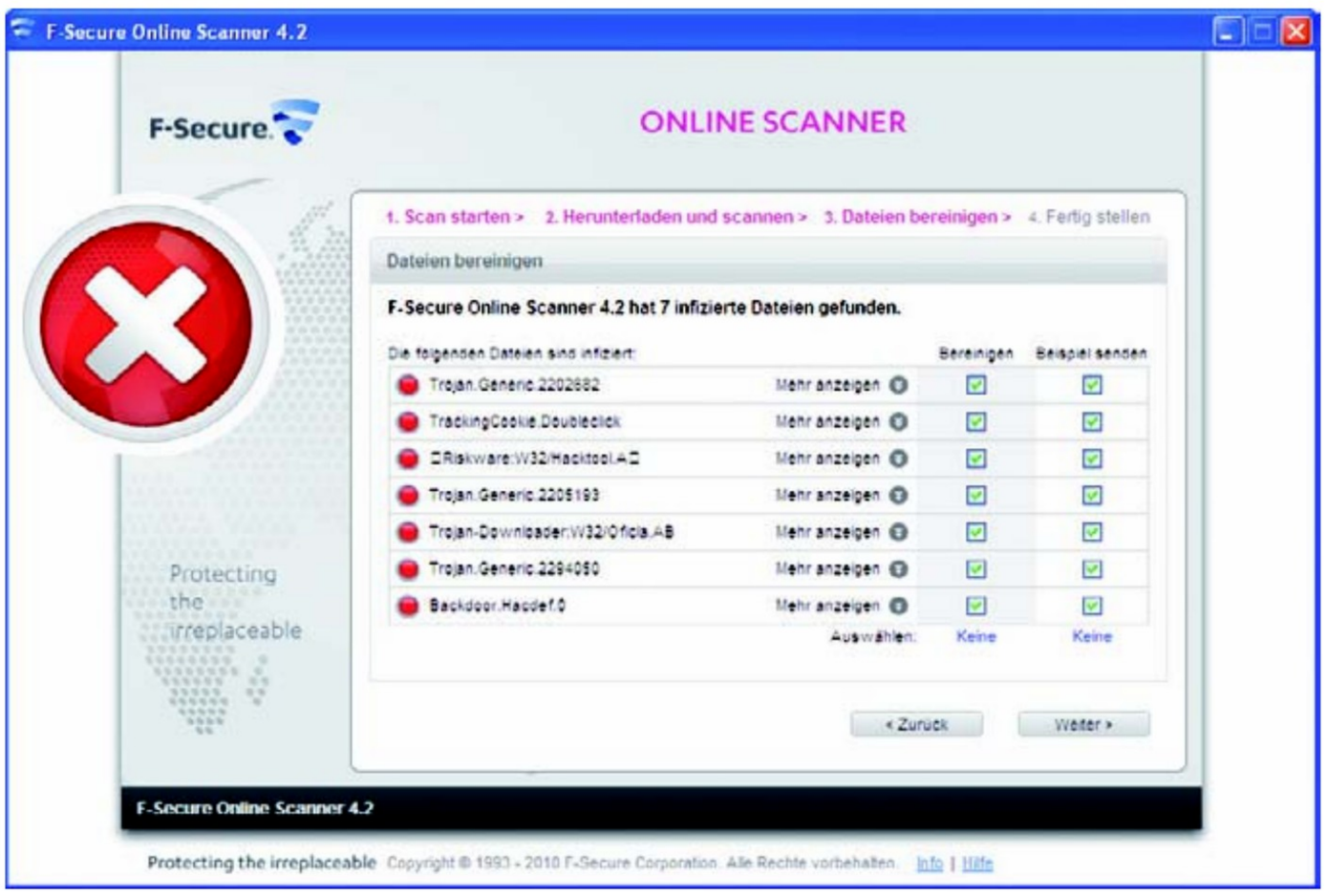
Das bootfähige Avira Antivir Rescue System 3.7.16 spürt auch Schädlinge auf, die sich erfolgreich vor dem Virenscanner verbergen (kostenlos, www.avira.com/de/support-download-avira-antivir-rescue-system und auf). Einziger Nachteil: Das Ergebnisprotokoll nach einem Scan lässt sich nicht abspeichern.

So geht's: Brennen Sie zuerst eine bootfähige CD, die ein schlankes Linux-System und den Avira-Scanner enthält. Dazu genügt ein Doppelklick auf die EXE-Datei, die Sie auf Heft-DVD sowie kostenlos unter der genannten Webadresse finden.

Lassen Sie die gebrannte CD im Laufwerk und starten Sie Ihren PC neu, um nach Viren zu suchen. Sobald das Boot-Menü erscheint, drücken Sie die Eingabetaste und warten, bis die grafische Oberfläche geladen ist. Klicken Sie jetzt auf „Update, Ja“, um die Signaturen zu aktualisieren.

Die eigentliche Suche nach Schädlingen starten Sie mit „Virenscanner, Virenscanner starten“. In der Standardeinstellung meldet der Virenscanner gefundene Schädlinge nur, löscht sie aber nicht. Diese Einstellung lässt sich unter „Konfiguration, Aktion bei Malware-Fund“ ändern. Optimal sind die beiden Einstellungen „Versuchen, infizierte Dateien zu reparieren“ sowie „Dateien umbenennen, wenn sie nicht repariert werden können“.

Unter „Sonstiges“ finden Sie den Punkt „Herunterfahren“, um Ihren PC nach dem Scan auszuschalten. Entfernen Sie beim nächsten Start zuerst die CD, um Windows normal zu booten. ▶



F-Secure Online-Scanner 4.2: Detailliert lässt sich bei jeder einzelnen verseuchten Datei festlegen, was mit ihr geschehen soll (Bild D)

www.books 2.0

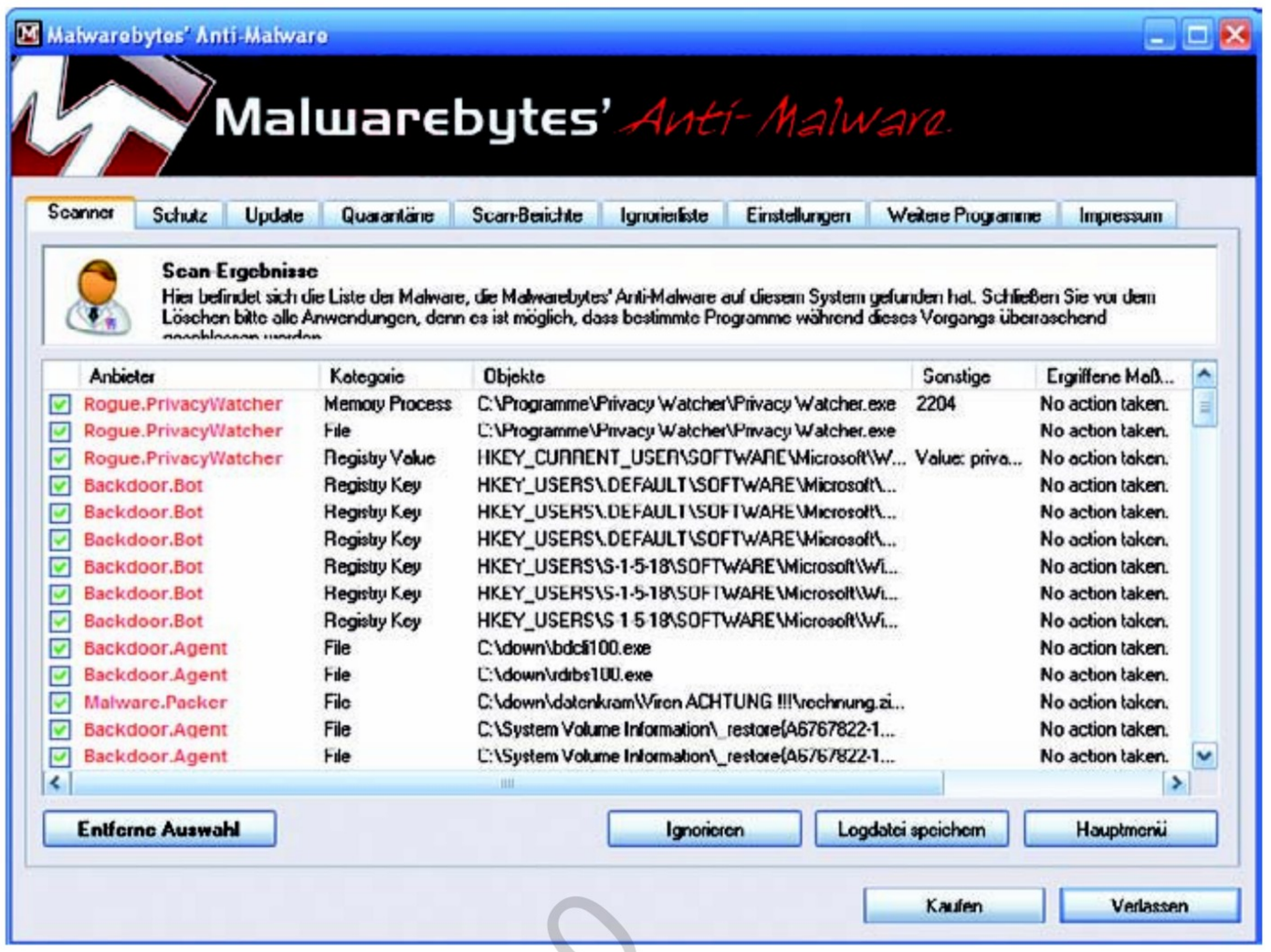
8. Rootkit Buster 3.60

Das Programm Rootkit Buster 3.60 sucht in verborgenen Dateien, in Registry-Einträgen, Prozessen und sogar in Treibern sowie dem Master Boot Record (MBR) nach Rootkits (kostenlos, www.trendmicro.com/download/rbuster.asp und auf). Die Version unterstützt Windows XP, Vista und 7, allerdings noch keine 64-Bit-Systeme.

So geht's: Entpacken Sie das ZIP-Archiv mit Rootkit Buster und starten Sie das Tool mit einem Doppelklick auf „RootkitBuster.exe". Die Suche nach Rootkits beginnen Sie mit „Scan Now".

Findet Rootkit Buster Hinweise auf verborgene Schädlinge, listet das Programm sie unter „Scan Results" auf. Wählen Sie mit der Maus den ersten Eintrag in der Liste aus und scrollen Sie bis ans Ende der Liste. Halten Sie [Umschalt] gedrückt, während Sie auf den letzten Eintrag klicken. So markieren Sie die komplette Liste. Falls Sie einzelne Einträge vom Löschvorgang ausnehmen wollen, klicken Sie darauf und halten Sie währenddessen [Strg] gedrückt.

Mit „Delete Selected Items" entfernen Sie die gefundenen Rootkits von Ihrem PC. Eventuell muss dazu der Computer neu gestartet werden.



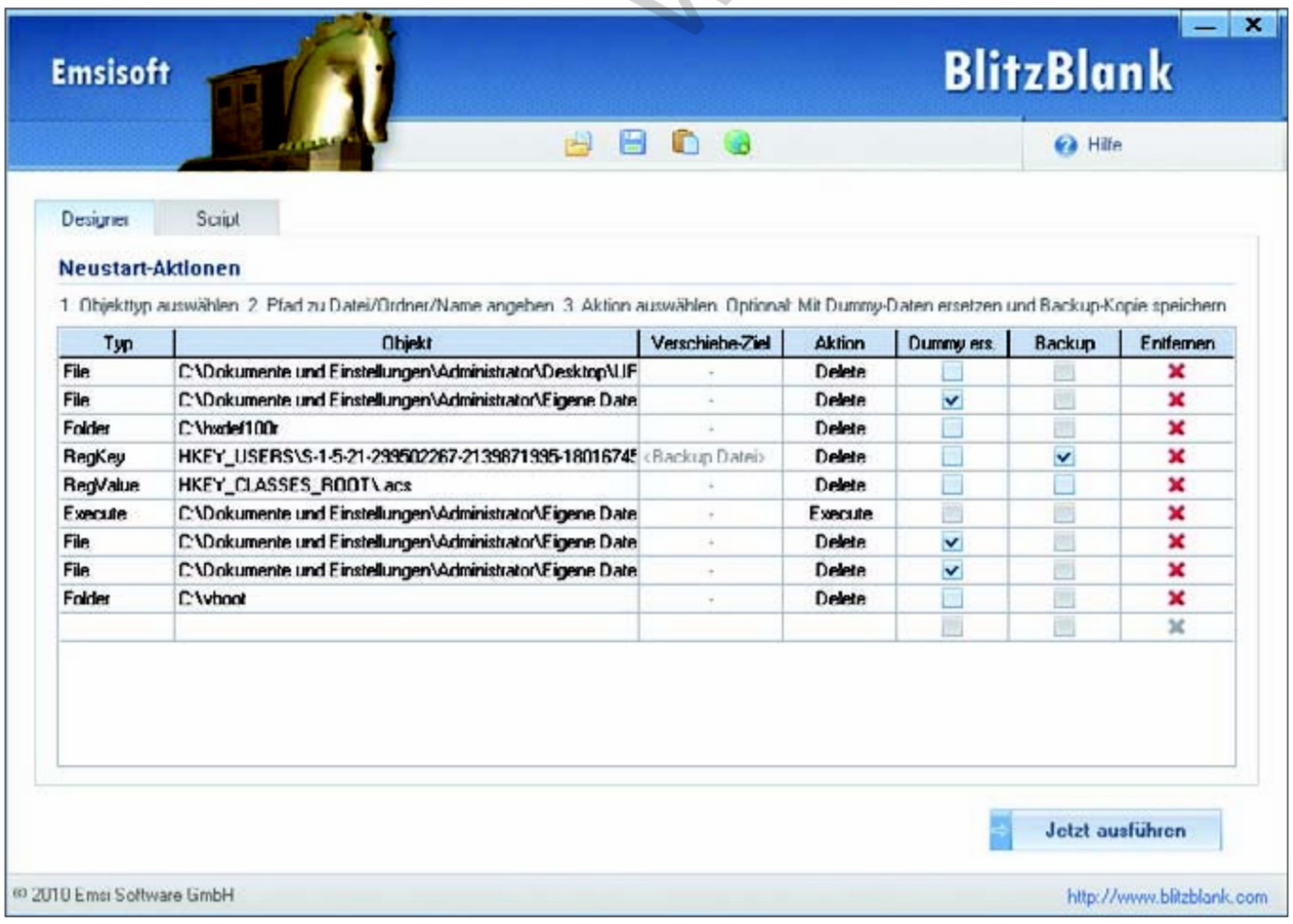
Anti-Malware 1.50.1: Das Tool ist auf die Jagd nach Trojanern spezialisiert. Oft findet es mehr als einen Schädling auf einem PC (Bild E)

Hartnäckige Viren löschen

Wenn ein Virus oder eine verseuchte Datei sich partout nicht löschen lassen, dann helfen die beiden Spezial-Tools Unlocker 1.9.0 und Blitzblank 1.0.

9. Löschen mit Unlocker 1.9.0

Manche aktive Viren lassen sich nicht löschen, weil Windows die Datei nicht freigibt. Hier hilft Unlocker 1.9.0, das sich direkt in den Windows-Explorer integriert und über einen Hintergrundagenten verfügt (kostenlos, http://unlocker.emptyloop.com und auf).



Blitzblank 1.0: Hier definieren Sie, welche Lösch- und Reinigungsaktionen vor dem Windows-Start erledigt werden sollen (Bild F)

Info: Fehlalarm

Es gibt zwei Arten von Fehlalarmen, bei denen ein Virenscanner harmlose Dateien als gefährlich einstuft.

Oft sind fehlerhafte Signaturen schuld an einem Fehlalarm. Diese Signaturen verteilen die Hersteller von Antivirensoftware automatisch über ihre Update-Routinen. So hatten Kaspersky und F-Secure die beliebte Videoplayer-Software VLC 1.0.5 versehentlich als Trojaner eingestuft.

Virenscanner warnen auch gern vor bestimmten Programmen, die sich für Angriffe auf fremde PCs missbrauchen lassen. Ein Beispiel ist die Fernsteuerungssoftware Real VNC 4.1.3. Das Programm ist kein Virus. Hacker könnten mit ihm aber auch versuchen, fremde Rechner unerlaubt zu steuern.

www.books 2.0

So geht's: Während der Installation bietet Ihnen Unlocker an, die Browser-Toolbar Quickstores Bar mitzuinstallieren. Wenn Sie dies nicht wollen, entfernen Sie das Häkchen vor „Install the new QuickStores Bar". Entfernen Sie im folgenden Dialog auch gleich das Häkchen vor „Ebay shortcuts (...)".

Anschließend genügt ein Rechtsklick auf eine gesperrte Datei und die Auswahl „Unlocker", um das Lösch-Tool zu öffnen. Wählen Sie unten links „Löschen" aus und bestätigen Sie mit „OK".

Zudem öffnet sich das Tool fortan automatisch, wenn Sie eine Datei löschen wollen und Windows dies verhindert.

10. Aufräumen mit Blitzblank 1.0

Das Freeware-Tool Blitzblank 1.0 integriert sich nicht in den Windows-Explorer und hat keinen Hintergrundagenten. Es bietet aber mehr Möglichkeiten, um Dateien, Ordner und Registry-Einträge zu löschen (kostenlos, www.emsisoft.de/de/software/blitzblank und auf). Der eigentliche Löschvorgang erfolgt dabei erst beim nächsten Neustart Ihres Computers. Ein Virus kann sich so nicht aktivieren und vor dem Löschen schützen.

Hartnäckige Viren löschen mit Blitzblank 1.0: Hier laufen die Aktionen, die Sie zuvor in Blitzblank definiert haben, vor dem eigentlichen Windows-Start ab (Bild G)

So geht's: Blitzblank benötigt keine Installation. Nach dem Starten richten Sie unter „Neustart-Aktionen" Ihre Löschaufgaben ein (Bild F).

Klicken Sie dazu zuerst auf das leere Feld unter „Typ" und wählen Sie „File" aus, um eine Datei zu löschen. Danach klicken Sie in derselben Zeile in das Feld unter „Objekt" und dann auf den Button mit den drei Punkten. Wählen Sie die zu löschende Datei aus und bestätigen Sie mit „Öffnen". In der Spalte „Aktion" lässt sich nun noch zwischen „Delete" für Löschen und „Move" für das Verschieben der Datei auswählen.

Wählen Sie „Folder" in der Spalte „Typ" aus, um einen ganzen Ordner zu löschen. Mit „RegKey" beziehungsweise „RegValue" entfernen Sie Einträge aus der Registrierungsdatenbank.

Sobald Sie alle Löschaufträge angelegt haben, klicken Sie auf „Jetzt ausführen". Der Rechner startet neu und führt noch während des Bootens die angelegten Aufgaben aus (Bild G). ■

Andreas Th. Fischer
sonderheft@com-magazin.de

Info: Virenkürzel

Nur wer die wichtigsten Abkürzungen in Virennamen kennt, kann eine Warnmeldung richtig einschätzen.

Die wichtigsten Abkürzungen sind **Win32**, **gen** und **TR**. **Win32** steht für die Plattform, auf der der Schädling aktiv ist. In diesem Beispiel also Windows in 32 Bit.

Die Abkürzung **gen** steht für generic und bedeutet, dass der Virenscanner den Virus nicht eindeutig erkennt, sondern ihn einer größeren Schädlingsfamilie zuordnet (Bild H). Oder er hält ihn einfach nur für verdächtig. **TR** schließlich ist die Abkürzung für Trojaner, die heutzutage häufigste Schädlingsart.

Stehen am Ende eines Schädlingsnamens ein oder zwei meist kleingeschriebene Zeichen, handelt es sich oft um eine Klassifizierung nach dem Alphabet. So unterscheidet sich **Virus.Win32.Sality.c** nur minimal von **Virus.Win32.Sality.b**.

heur.suspicious bedeutet, dass der Virenscanner keine Signatur in seiner Datenbank gefunden hat, die Datei aber trotzdem anhand einiger Merkmale als verdächtig einstuft. Man nennt dieses Verfahren Heuristik, daher auch die Abkürzung **heur**.

Virusmeldung: Die verwendeten Kürzel sind oft schwer zu verstehen. „gen" bedeutet etwa, dass der Scanner den Virus nicht eindeutig kennt (Bild H)

Weitere Infos

- http://de.wikipedia.org/wiki/Computervirus
  Sehr detaillierte Infos zu Computerviren
- www.com-magazin.de/tipps/2110
  So ändern Sie die Boot-Reihenfolge am PC

WiWobooks 2.0

PC von Viren säubern

Wer nach einem Virenbefall auf Nummer sicher gehen will, kommt um eine Neuinstallation nicht herum. Die will jedoch sorgfältig geplant sein.

Der Artikel beschreibt, wie Sie Ihre Daten von einem verseuchten Computer retten und wie Sie den Rechner dann wieder sauber aufsetzen.

Der PC wird komplett ohne Internetanschluss gesäubert. Deswegen erstellen Sie vorab ein Update-Pack mit allen Sicherheits-Patches für Windows und brennen danach die Kaspersky Rescue Disk 10, das Avira Antivir Rescue System 3.7.16 und Darik's Boot and Nuke 2.2.6 Beta auf CD.

Anschließend sichern Sie Ihre Daten auf einen externen Datenträger, zum Beispiel einen USB-Stick oder eine USB-Festplatte, und säubern die Daten danach mit der Kaspersky Rescue Disk und dem Avira Antivir Rescue System.

Im nächsten Schritt überschreiben Sie den MBR (Master Boot Record) und die komplette Festplatte mit Darik's Boot and Nuke, so dass garantiert kein Schädling die Neuinstallation übersteht.

Danach installieren Sie Windows und aktualisieren das Betriebssystem mit dem vorab erstellten Update-Pack. Abschließend installieren Sie einen Virenscanner. Nun können Sie das Netzwerkkabel wieder einstecken und mit dem geschützten PC unbesorgt im Internet surfen.

Kompakt

- *Der Artikel erklärt in zehn Schritten, wie Sie Ihren PC neu aufsetzen.*
- *Alle dazu benötigten Live-CDs und Programme finden Sie auf Heft-DVD und kostenlos im Internet.*

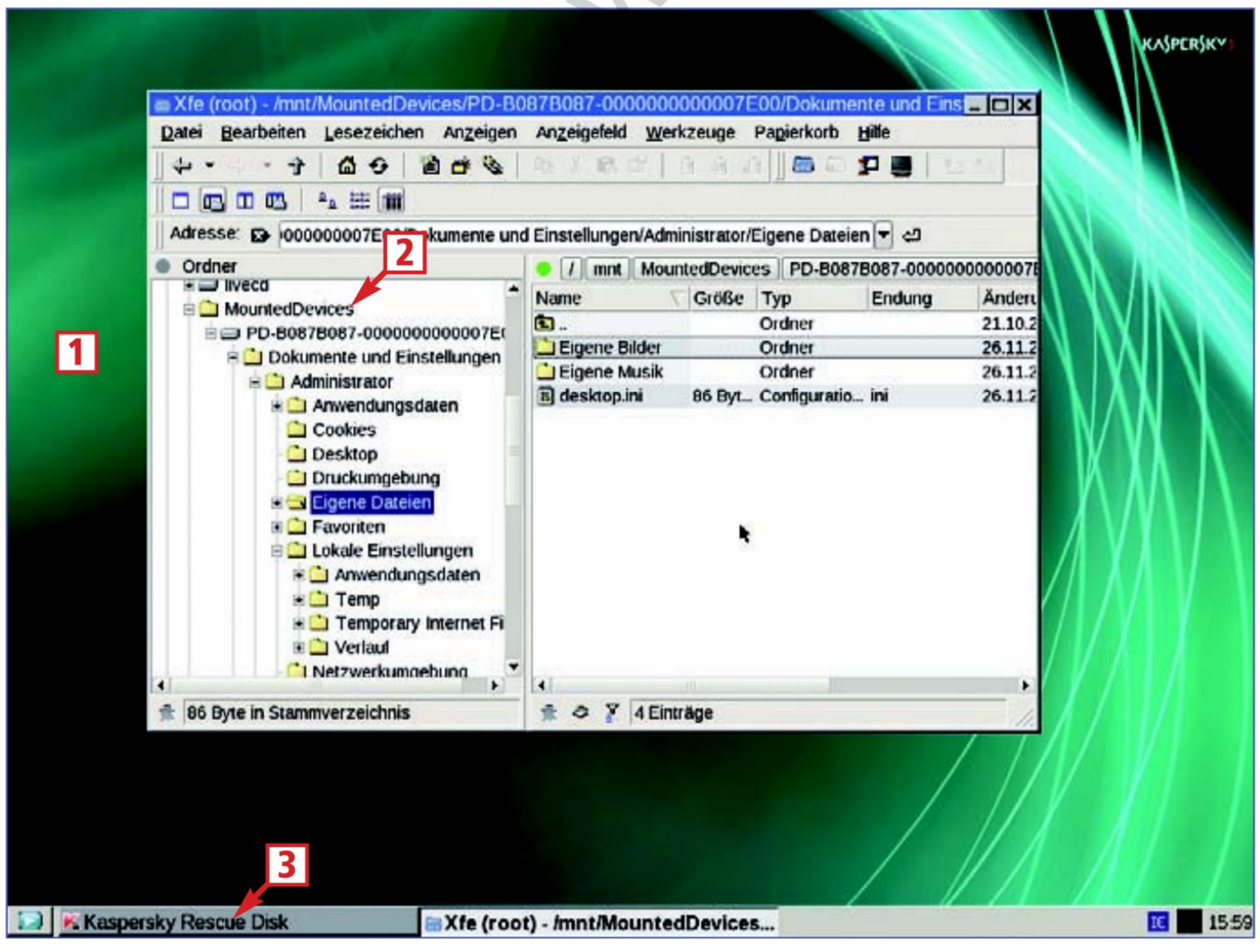
Vorbereitungen

Wenn möglich, bitten Sie einen Bekannten, ob Sie die folgenden beiden Schritte auf seinem – hoffentlich – sauberen PC ausführen können. Nur notfalls nehmen Sie Ihren eigenen Rechner.

www.wobooks2.0

So geht's: Kaspersky Rescue Disk 10

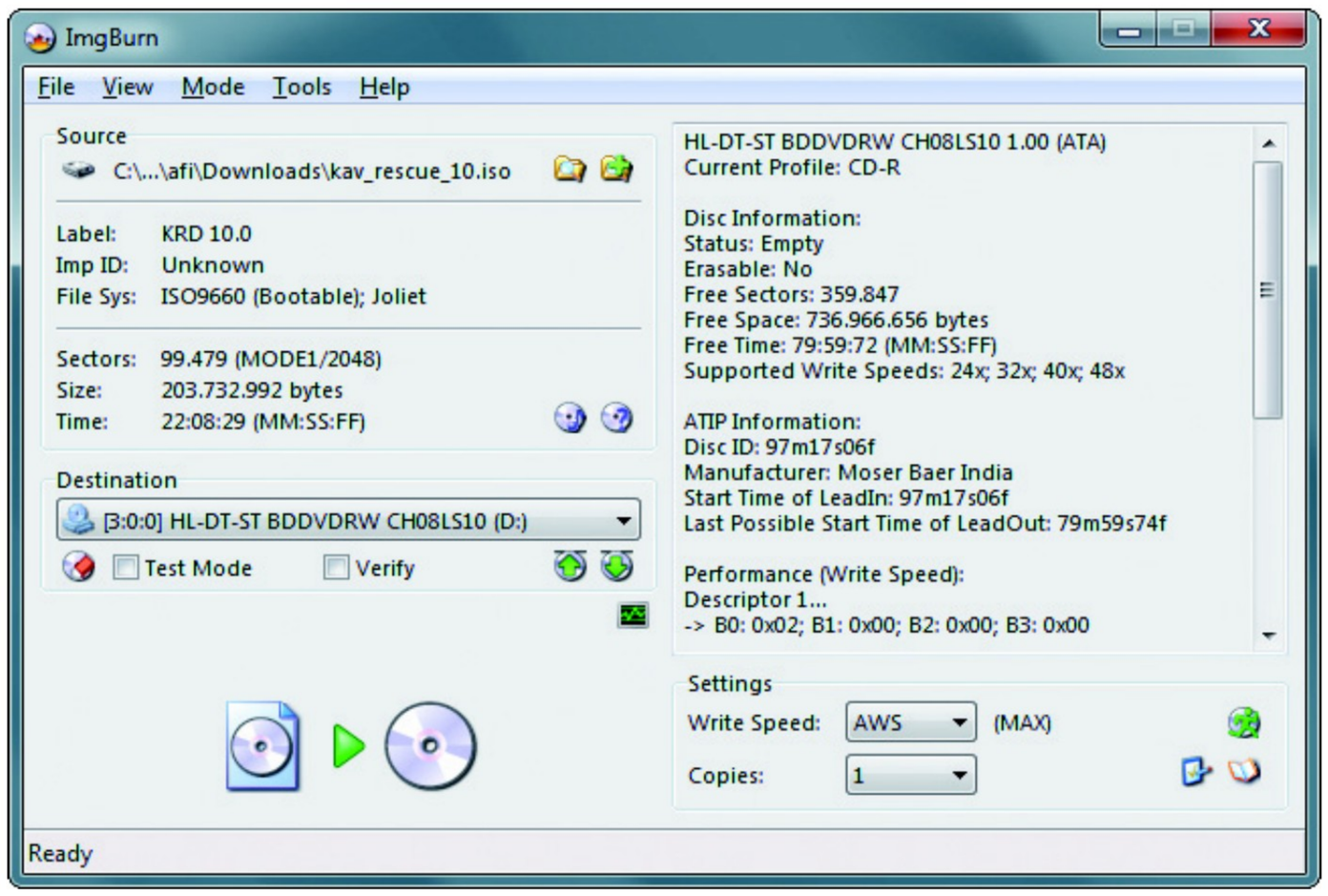
Die Kaspersky Rescue Disk 10 sucht nicht nur nach Viren, sondern sichert auch Ihre Dateien (kostenlos, http://support.kaspersky.com /viruses/rescuedisk?level=2 und auf CD). Sie basiert zwar auf Linux, lässt sich aber fast wie ein Windows-Programm bedienen.



1 Desktop
Ein Rechtsklick auf den Desktop öffnet den Dateimanager.

2 Mounted Devices
Hier finden Sie die Festplatte und angeschlossene USB-Platten.

3 Kaspersky Rescue Disk
Über diese Schaltfläche wechseln Sie zum Virenscanner.



Imgburn 2.5.5.0: Bevor Sie Ihren PC neu aufsetzen, brennen Sie die Kaspersky Rescue Disk 10, das Avira Antivir Rescue System 3.7.16 und den Daten-Schredder Darik's Boot and Nuke 2.2.6 Beta auf CD (Bild B)

Inhalt

PC von Viren säubern

- **Vorbereitungen**
  - 1. Update-Pack erstellen S. 35
  - 2. Software vorbereiten S. 36
- **Dateien retten**
  - 3. Daten sichern S. 36
  - 4. Virencheck I S. 37
  - 5. Virencheck II S. 37
- **PC säubern und neu aufsetzen**
  - 6. Festplatte überschreiben S. 37
  - 7. Windows installieren S. 38
  - 8. Windows aktualisieren S. 38
  - 9. Virenscanner installieren S. 38
  - 10. PC ans Internet anschließen S. 38

So geht's: Kaspersky Rescue Disk 10 S. 34

Tipp: License Crawler 1.4 S. 35

Software-Übersicht S. 36

So geht's: Antiviren-CDs aktualisieren S. 38

Sonst könnte es passieren, dass ein Trojaner heimlich eine der verwendeten EXE-Dateien infiziert und so den ganzen Bereinigungsprozess überlebt.

1. Update-Pack erstellen

Direkt nach einer Neuinstallation und ohne die vielen Security-Patches, die Microsoft jeden Monat veröffentlicht, ist Windows offen wie ein Scheunentor.

Der com! Update-Pack-Builder 5.0.7 erstellt eine ausführbare Datei, mit der Sie Ihr Windows in einem Schwung auf den aktuellen Stand bekommen – ohne dass der PC mit dem Internet verbunden ist (kostenlos, www.com-magazin.de /software und auf).

Installieren Sie das Tool und entfernen Sie im letzten Dialog das Häkchen vor „com! Update Pack Builder starten". Rufen Sie das Programm danach über „Start, Alle Programme, com!, com! Update Pack Builder starten" auf.

Wählen Sie „Neues Projekt" aus und verneinen Sie die Frage, ob Sie das Update-Pack in eine Windows-CD/-DVD integrieren wollen. Wählen Sie Ihr Betriebssystem bei „Microsoft Windows" aus. XP-Nutzer nehmen „Microsoft Windows XP ohne Service Pack", Vista-Anwender „Microsoft Windows Vista ohne Service Pack" und Windows-7-User „Microsoft Windows 7 ohne Service Pack". So stellen Sie sicher, dass Ihr Update-Pack alle Aktualisierungen enthält.

Klicken Sie danach auf „Weiter" und auf „Alles auswählen". Ein Klick auf „Herunterladen" lädt alle Updates herunter. Sobald der Download abgeschlossen ist, klicken Sie dreimal auf „Weiter" und danach auf „Projekt speichern, Schließen". Geben Sie eine Bezeichnung für das Projekt ein und bestätigen Sie mit „Speichern". Ein letzter Klick auf „Jetzt erstellen" speichert Ihr Update-Pack.

Kopieren Sie die erstellte EXE-Datei anschließend auf einen USB-Stick, eine CD oder eine DVD. ▶

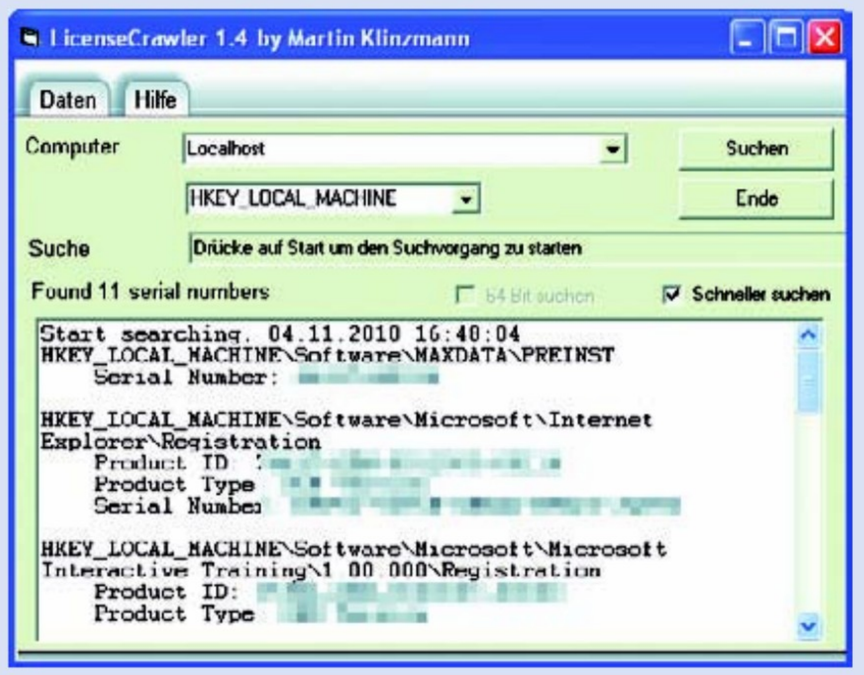
www.books 2.0

Tipp: License Crawler 1.4

License Crawler 1.4 sammelt die Seriennummern der auf Ihrem PC installierten Programme (kostenlos, www.klinzmann.name/licensecrawler_de.htm und auf).

Bevor Sie loslegen und Ihren PC neu aufsetzen, lohnt sich ein Durchlauf mit dem Tool License Crawler. Es durchsucht die Registrierungsdatenbank Ihres Computers nach Seriennummern installierter Software und speichert sie als Textdatei ab (Bild A).

Entpacken Sie das ZIP-Archiv und starten Sie das Programm mit einem Doppelklick auf „LicenseCrawler.exe". Akzeptieren Sie die Lizenzbedingungen und ändern Sie dann die Sprache mit „Help, Language, Deutsch". Starten Sie die Suche nach Seriennummern mit „Suchen". Sichern Sie die gefundenen Seriennummern dann mit „Daten, Speichern".



License Crawler 1.4: Das Programm rettet die Seriennummern auf Ihrem PC und speichert sie in einer Textdatei (Bild A)

2. Software vorbereiten

Die Kaspersky Rescue Disk 10, das Avira Antivir Rescue System 3.7.16 und der Daten-Schredder Darik's Boot and Nuke 2.2.6 Beta sorgen dafür, dass Ihr PC nach der Bereinigung nicht gleich wieder zum Opfer neuer Viren wird.

Brennen Sie zuerst die drei Live-CDs. Falls Sie über kein geeignetes Brennprogramm verfügen, verwenden Sie Imgburn 2.5.5.0 (kostenlos, www.imgburn.com und auf) (Bild B).

Die erste zu brennende Live-CD ist die **Kaspersky Rescue Disk 10** (kostenlos, http://support.kaspersky.com/viruses/rescuedisk?level=2 und auf). Sie enthält den Virenscanner von Kaspersky und ist mit ihrer an Windows angelehnten Oberfläche besonders leicht zu bedienen. Außerdem hat diese Live-CD einen Dateimanager, der sich zum Sichern Ihrer Daten auf einen USB-Stick oder eine USB-Festplatte eignet.

Die zweite Live-CD ist das **Avira Antivir Rescue System 3.7.16** (kostenlos, www.avira.com/de/support-download-avira-antivir-rescue-system und auf). Zuletzt brennen Sie noch eine CD mit dem Daten-Schredder **Darik's Boot and Nuke 2.2.6 Beta** (kostenlos, www.dban.org und auf).

Jetzt benötigen Sie noch einen Virenscanner, den Sie direkt nach der Windows-Neuinstallation einrichten können. Nehmen Sie zum Beispiel **Avast Free Antivirus 6.0** (kostenlos, www.avast.com und auf). Kopieren Sie die Setup-Datei von Avast auf einen USB-Stick, eine CD oder eine DVD, damit Sie die Datei nach dem Windows-Setup zur Hand haben.

Dateien retten

Nehmen Sie sich ausreichend Zeit, um alle wichtigen Dateien und Dokumente von Ihrem PC zu retten. Zwei Virenchecks suchen anschließend verborgene Schädlinge.

Software-Übersicht

Programm	Quelle	Seite
Avast Free Antivirus 6.0 (Virenscanner)	www.avast.com	36
Avira Antivir Rescue System 3.7.16 (Antiviren-CD)	www.avira.de	36
com! Update-Pack-Builder (Update-Manager)	www.com-magazin.de/software	35
Darik's Boot and Nuke 2.2.6 Beta (Löschsystem)	www.dban.org	36
Imgburn 2.5.5.0 (Brenn-Tool)	www.imgburn.com	36
Kaspersky Rescue Disk 10 (Antiviren-CD)	www.kaspersky.de	36
License Crawler 1.4 (Seriennummern-Retter)	www.klinzmann.name	35

Alle -Programme finden Sie auf Heft-DVD in der Rubrik „Windows, PC von Viren säubern" und kostenlos im Internet.

3. Daten sichern

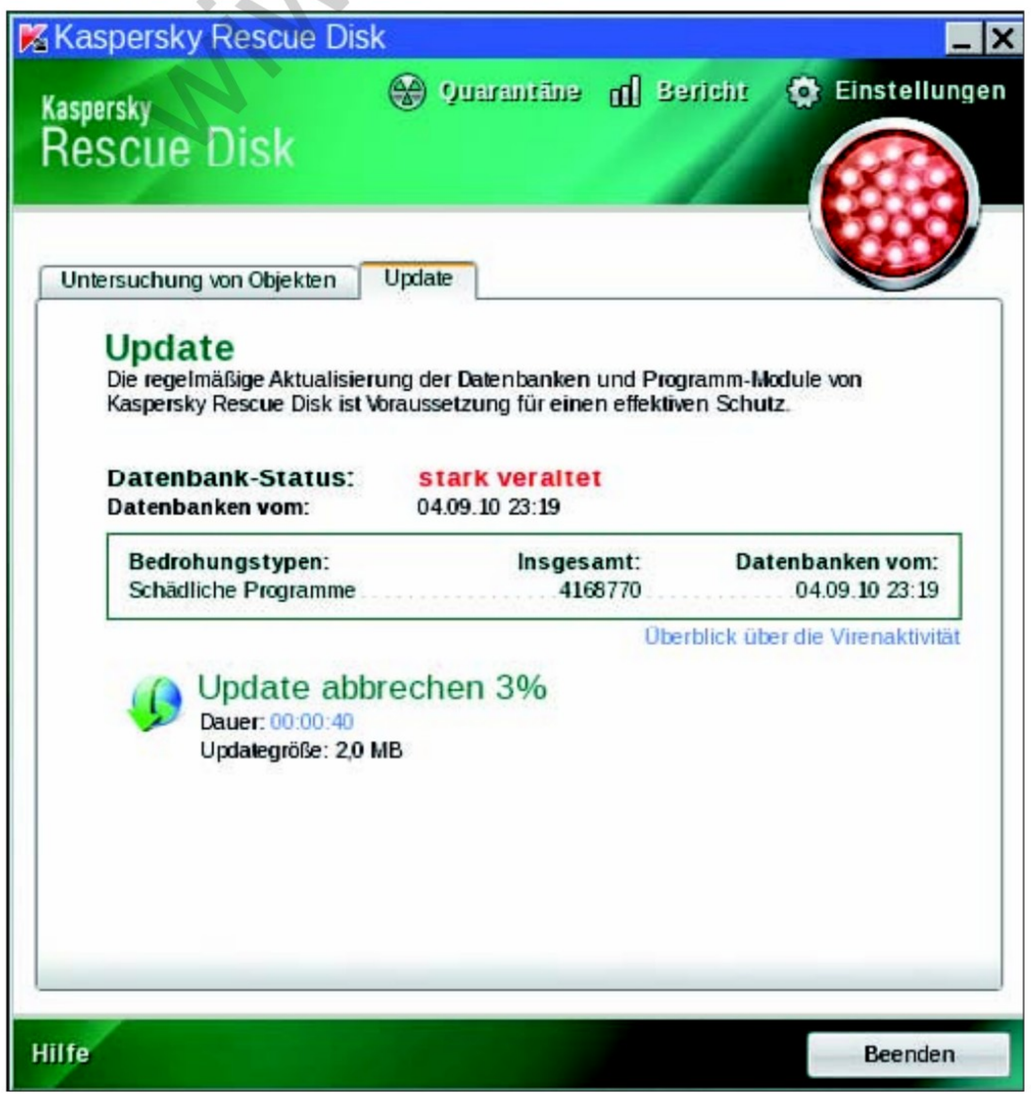
Zur Sicherung Ihrer Daten benötigen Sie die zuvor gebrannte Kaspersky Rescue Disk und eine USB-Festplatte. Der Datenträger sollte im FAT32-Format formatiert sein. Auf Datenträgern mit dem NTFS-System können sich Schädlinge in Alternate Data Streams (ADS) verstecken.

Legen Sie die Kaspersky Rescue Disk in Ihren Computer ein und starten Sie ihn neu. Schließen Sie nun auch bereits die USB-Platte an, auf die Sie Ihre Daten sichern wollen. Falls der PC nicht von der CD bootet, rufen Sie das BIOS auf und ändern Sie die Boot-Reihenfolge. Wie Sie die Boot-Reihenfolge ändern, lesen Sie unter www.com-magazin.de/tipps/2110.

Wählen Sie zunächst als Sprache „Deutsch" und dann im folgenden Dialog „Kaspersky Rescue Disk. Grafikmodus" aus. Zuletzt präsentiert Ihnen das System die Lizenzbedingungen, die Sie mit [A] bestätigen.

Sobald sich das Fenster des Virenscanners öffnet, ist das System einsatzbereit. Klicken Sie neben dem Scanner-Fenster mit der rechten Maustaste auf den Desktop und wählen Sie „Dateimanager" aus. Wechseln Sie dann zum Ordner „mnt/Mounted Devices". Sie sehen mehrere Kennungen, die Linux vergibt und die für die einzelnen Datenträger stehen.

Kopieren Sie nun alle wichtigen Daten von Ihrem PC auf die USB-Platte. Unter Windows 7 liegen viele Dateien unter „C:\Documents and Settings". Am besten klicken Sie mit der rechten Maustaste auf den Ordner mit Ihrem Benutzernamen und wählen „Kopieren" aus. Wechseln Sie dann zur USB-Platte, klicken Sie mit der rechten Maustaste darauf und wählen Sie „Einfügen" aus. Bestätigen Sie den Kopiervorgang



Kaspersky Rescue Disk 10: Sie sollten vor dem Virencheck auf jeden Fall die Virensignaturen aktualisieren (Bild C)

www.wobooks 2.0

mit „Übernehmen“. Wiederholen Sie diesen Vorgang dann mit allen Ordnern und Dateien, die Sie sichern wollen.

4. Virencheck I

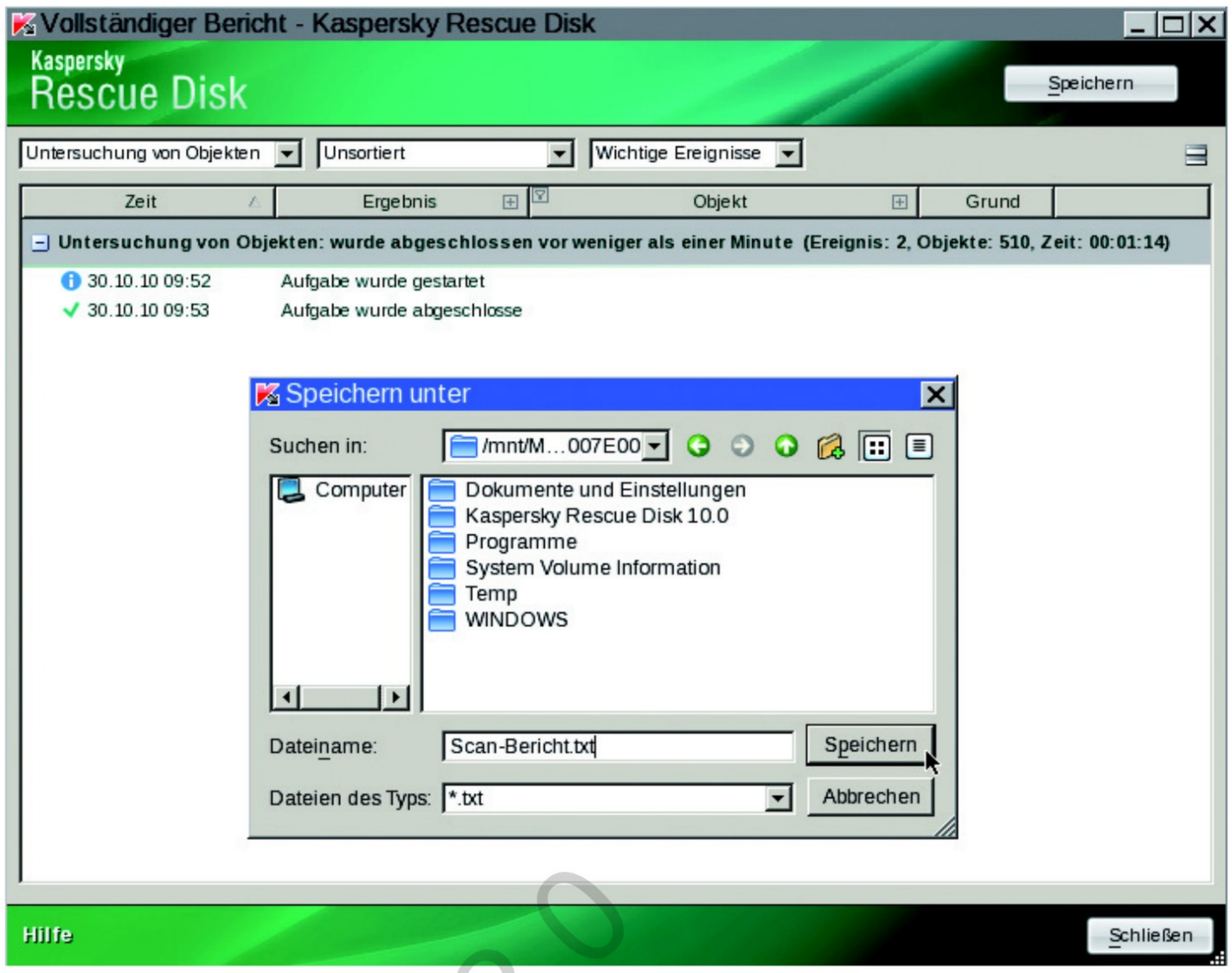
Prüfen Sie Ihre gesicherten Daten nun auf Viren. Der erste Check erfolgt mit der Kaspersky Rescue Disk 10, die Sie bereits zum Sichern der Dateien verwendet haben.

Die auf der Rescue Disk mitgelieferten Signaturen sind jedoch stark veraltet. Rufen Sie deshalb das Fenster „Kaspersky Rescue Disk“ auf und wählen Sie den Reiter „Update“ aus. Klicken Sie auf „Update ausführen“, um die Virensignaturen zu aktualisieren (Bild C).

Sobald das Update abgeschlossen ist, wechseln Sie wieder zum Reiter „Untersuchung von Objekten“ zurück. Setzen Sie nun das Häkchen vor Ihrer USB-Platte. Meist ist sie als „sdb1“ eingebunden. „sda1“ ist die Antiviren-CD, die müssen Sie nicht scannen.

Falls Sie sich nicht sicher sind, welches das richtige USB-Laufwerk ist, klicken Sie auf „Hinzufügen“. Es öffnet sich das Fenster „Untersuchungsobjekt auswählen“. Klicken Sie auf das Kreuz neben den einzelnen Einträgen, um den Inhalt der Datenträger zu sehen. So finden Sie leicht heraus, welche Bezeichnung Ihr USB-Datenträger hat.

Ein Klick auf „Untersuchung von Objekten starten“ beginnt mit der Suche nach Viren. Findet das Antiviren-System einen Schädling, haben Sie anschließend die Möglichkeit, diesen zu entfernen. Nach dem Ende des Scans klicken Sie oben auf „Bericht“, um sich eine Zusammenfassung anzeigen zu lassen. Über die Schaltfläche „Vollständiger Bericht“ sichern Sie den Scan-Bericht auf dem USB-Stick (Bild D).



Scan-Bericht speichern: Die Kaspersky Rescue Disk 10 speichert den Scan-Bericht auf Wunsch zum Beispiel auf Ihrem USB-Stick oder einer externen USB-Festplatte (Bild D)

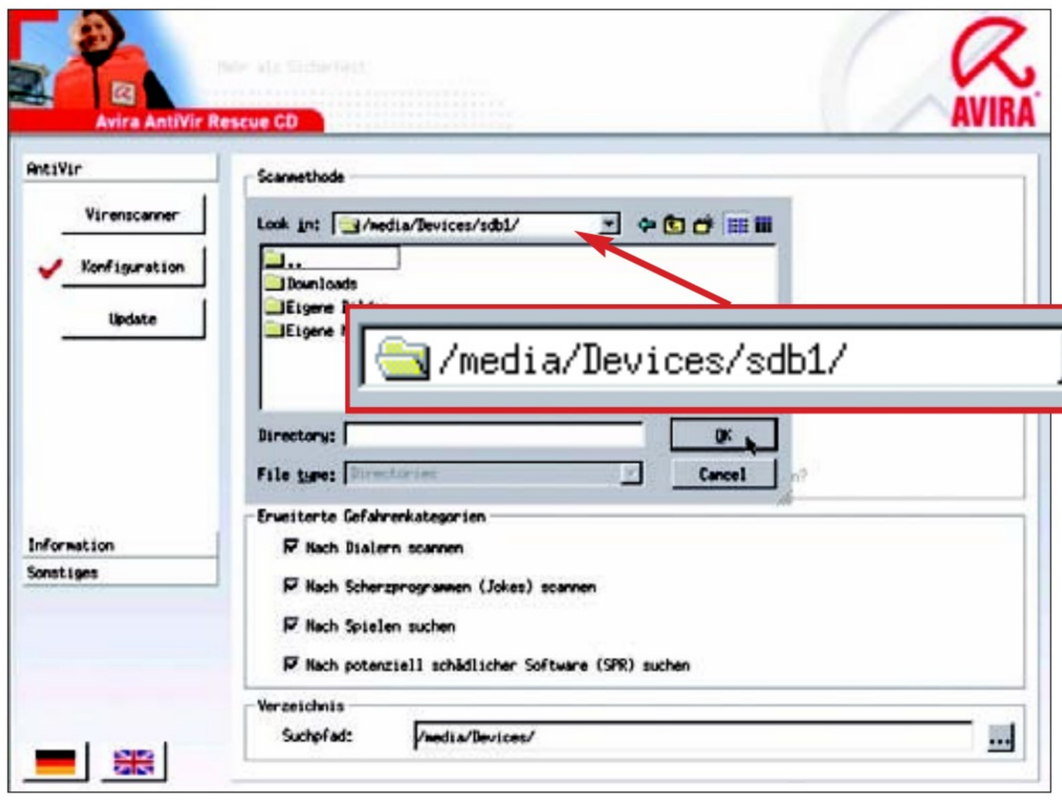
5. Virencheck II

Nach dem Check mit der Kaspersky-CD legen Sie das Avira Antivir Rescue System ein. Starten Sie Ihren PC davon. Ein zusätzlicher Durchgang mit einer zweiten Antiviren-CD erhöht die Chance, Viren aufzuspüren.

Sobald das Boot-Menü der Antiviren-CD erscheint, drücken Sie die Eingabetaste. Nun startet das Antivirensystem. Wenn die Oberfläche fertig geladen ist, aktualisieren Sie die Virensignaturen. Wählen Sie „Update, Ja“ aus.

Klicken Sie danach auf „Konfiguration“ und anschließend unten rechts auf die Schaltfläche mit den drei Punkten. Wählen Sie nun Ihre USB-Platte aus. Wie bei Kaspersky ist sie meist als „sdb1“ eingebunden (Bild E). Bestätigen Sie mit „OK“ und wechseln Sie dann zum „Virenscanner“. Klicken Sie auf „Scanner starten“.

Im Gegensatz zur Kaspersky Rescue Disk 10 ist es mit der Antiviren-CD von Avira nicht möglich, das Suchprotokoll auf dem Stick zu speichern.



Avira Antivir Rescue System 3.7.16: Im Konfigurationsfenster legen Sie fest, dass die Antiviren-CD nur Ihre USB-Platte auf Viren prüfen soll (Bild E)

PC säubern und neu aufsetzen

Führen Sie die folgenden Schritte erst aus, wenn Sie alle wichtigen Daten von Ihrem PC gerettet haben. Eine Wiederherstellung der Dateien ist später nicht mehr möglich.

6. Festplatte überschreiben

Darik's Boot and Nuke 2.2.6 Beta überschreibt die komplette Festplatte und ver- ▶

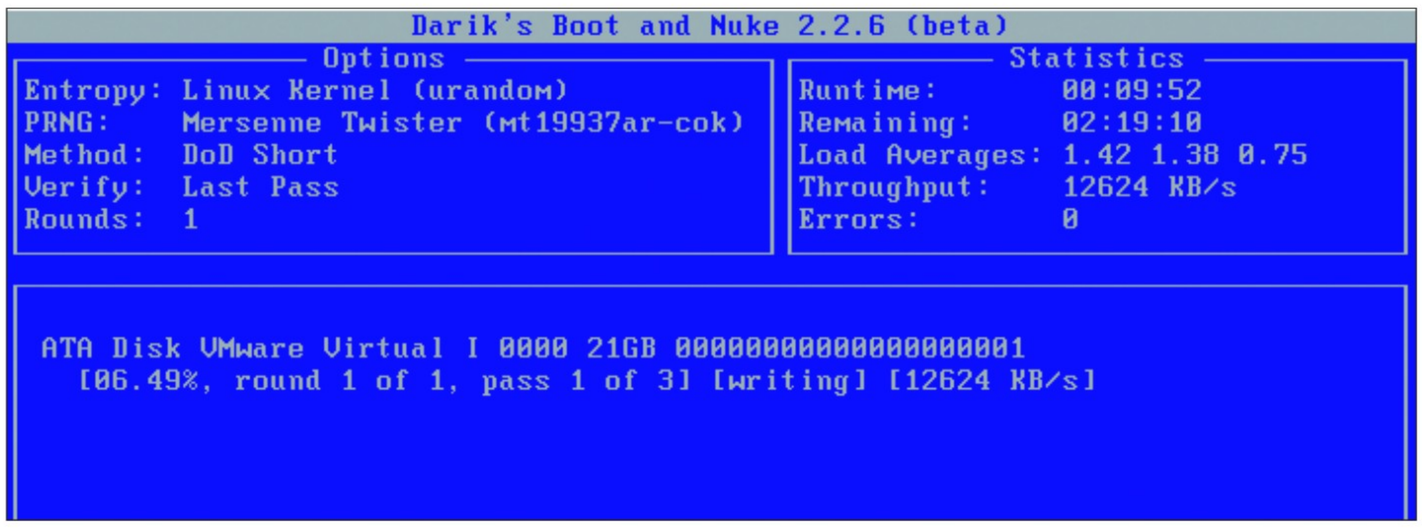
www.boot-und-werk.de

nichtet dabei alle noch vorhandenen Reste von Computerviren.

Wichtig dabei ist, dass Sie wirklich die komplette Festplatte und nicht nur einzelne Partitionen überschreiben. Erstens überleben so keine Viren etwa auf einer Datenpartition, und zweitens überschreibt das Tool nur dann auch den MBR (Master Boot Record) der Festplatte. Im MBR verbergen sich besonders fiese Boot-Viren.

Legen Sie die Live-CD mit Darik's Boot and Nuke ein und starten Sie Ihren PC neu. Falls die USB-Platte mit Ihren gesicherten Daten noch angeschlossen ist, entfernen Sie sie jetzt.

Nach kurzer Zeit erscheint die Startseite des Tools. Tippen Sie den Befehl **autonuke** ein und bestätigen Sie mit der Eingabetaste. Darik's Boot and Nuke überschreibt nun die komplette Festplatte drei Mal (Bild F). Beim ersten Durchgang schreibt das Tool lauter Einsen, beim zweiten Mal nur noch Nullen und beim dritten Durchgang dann zufällige Datenfolgen.



Darik's Boot and Nuke 2.2.6 Beta: Die Live-CD überschreibt alle Daten auf der Festplatte und vernichtet so auch hartnäckige Viren (Bild F)

7. Windows installieren

Nachdem Sie mit Darik's Boot and Nuke die Festplatte komplett überschrieben haben, installieren Sie nun Windows neu. Entfernen Sie aber vorher noch das Netzwerkkabel, damit nicht ein Wurm Ihren PC über das Netzwerk infiziert, bevor alle Sicherheits-Patches eingespielt sind.

Legen Sie Ihre Windows-CD oder das Recovery-Medium ein, das Ihrem PC beim Kauf beilag, und booten Sie Ihren PC davon. Folgen Sie dann dem Installationsassistenten.

8. Windows aktualisieren

Frisch installierte Windows-Versionen sind voller Sicherheitslücken. Aktualisieren Sie deshalb nach dem Windows-Setup als Erstes das Betriebssystem.

Kopieren Sie die in Schritt 1 mit dem com! Update-Pack-Builder erstellte EXE-Datei auf die Festplatte Ihres Computers und klicken Sie doppelt darauf. Klicken Sie auf „Weiter" und danach auf „Automatisch (empfohlen)". Starten Sie das Update mit einem erneuten Klick auf „Weiter".

9. Virenscanner installieren

Installieren Sie nun einen Virenscanner. Entweder besitzen Sie bereits einen kostenpflichtigen Scanner oder Sie verwenden Avast Free Edition 6.0, den Sie bereits in Schritt 2 heruntergeladen und auf einen USB-Stick, eine CD oder eine DVD kopiert haben.

10. PC ans Internet anschließen

Erst jetzt, nachdem Sie Windows aktualisiert und einen Virenscanner installiert haben, schließen Sie das Netzwerkkabel wieder an und verbinden Ihren PC mit dem Internet.

Jetzt ist auch der ideale Zeitpunkt, um Ihre Daten von der USB-Platte wieder zurückzuspielen und Ihre Lieblingsprogramme zu installieren. Falls noch Hardware-Treiber fehlen, sollten Sie diese nun auch herunterladen und installieren. ■

Andreas Th. Fischer
sonderheft@com-magazin.de

So geht's: Antiviren-CDs aktualisieren

Für die Suche nach Viren benötigen sowohl die Kaspersky Rescue Disk 10 als auch das Avira Antivir Rescue System 3.7.16 aktuelle Signaturen. Die auf den CDs mitgelieferten Signaturen sind nämlich veraltet.

Das Update der Signaturen über das Internet funktioniert mit einem aktuellen DSL-Router problemlos, es sei denn, in dem Router ist DHCP (Dynamic Host Control Protocol) deaktiviert. Mit DHCP erhält jeder Computer automatisch eine IP-Adresse, die er zum Download der Signaturen benötigt.

Ein Problem kann außerdem auftreten, wenn Ihr PC per WLAN mit dem Router verbunden ist. Die Antiviren-CDs enthalten nur eine Auswahl der gängigsten WLAN-Treiber. Falls ein Update der Signaturen per WLAN nicht möglich ist (Bild H), schließen Sie Ihren Computer vorübergehend per Netzwerkkabel an den Router an.

Fehlgeschlagenes Update: Zum Aktualisieren der Virensignaturen ist eine Online-Verbindung nötig (Bild H)

Weitere Infos

- www.malte-wetz.de/wiki/pmwiki.php/De/VirenEntfernen
  Tipps zum Bereinigen eines PCs

wiwobooks2.0

Mehr News!

Tipp-Newsletter

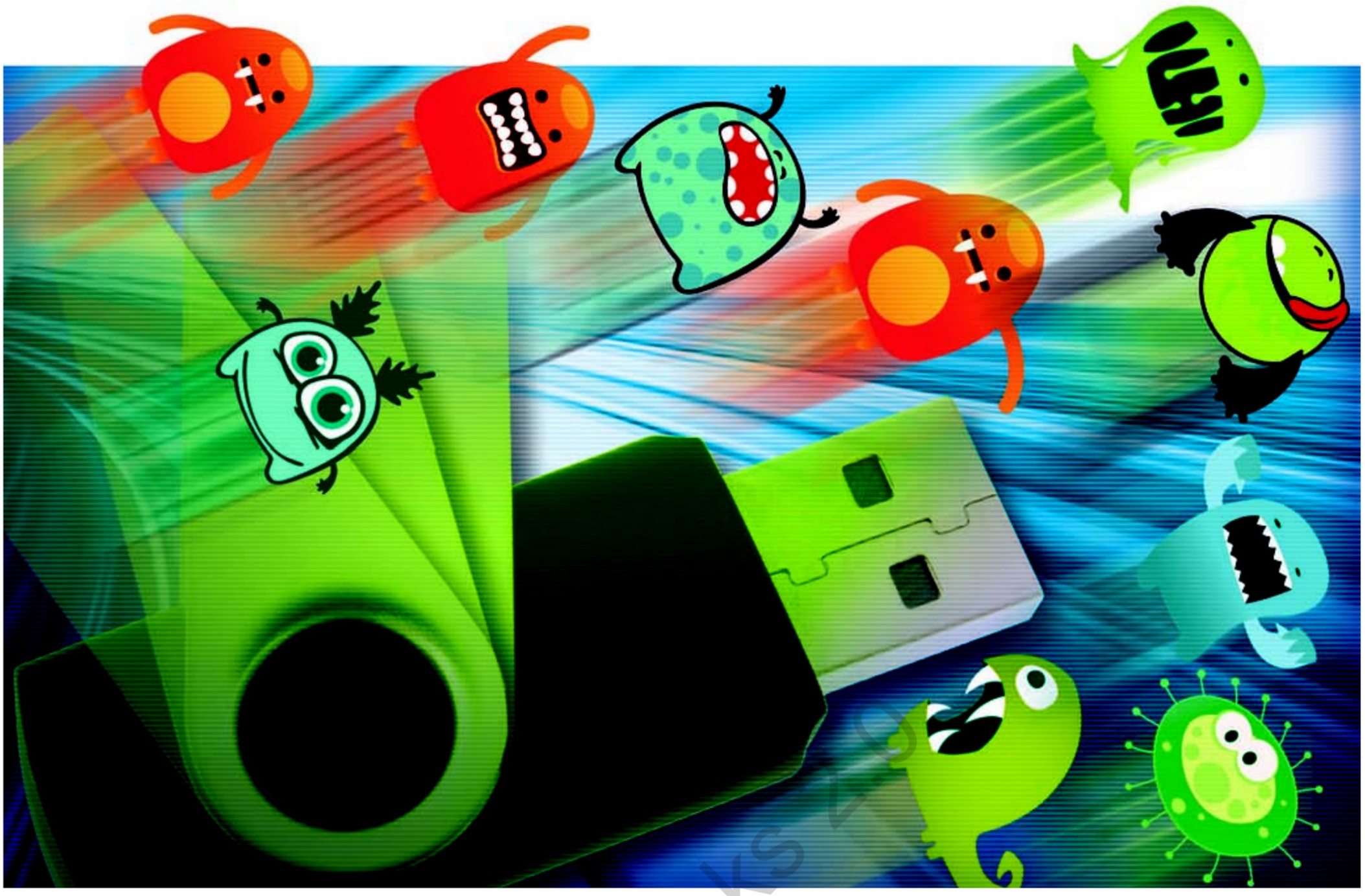
Donnerstags: Experten-Tipps zu Windows XP, Vista und 7, Firefox, Open Source, USB-Sticks, virtuelle PCs, Live-Systeme …

Sicherheits-Newsletter

Dienstags: Aktuelle Sicherheitslücken, wichtige System-Updates, Rückruf-Aktionen, neue Service Packs …

Jetzt kostenlos bestellen unter:

www.com-magazin.de/newsletter



Virenschleuder USB

WiWeBooks

Nach dem Internet sind USB-Sticks und -Festplatten die zweite große Infektionsquelle für Windows-PCs. So schützen Sie Ihren Computer vor USB-Viren.

Fast jede dritte Infektion mit einem Computervirus erfolgt über den USB-Anschluss. Früher setzten Kriminelle vor allem automatisch startende USB-Würmer ein. Microsoft hat jedoch die dabei genutzten Hintertüren in Windows mittlerweile geschlossen. Die Banden denken sich deswegen immer neue Tricks aus, damit der Anwender eine vermeintlich harmlose Datei auf dem Stick selbst startet.

Ein Beispiel für diese neue Art von Viren ist USB Switchblade. Der Schädling verwendet einen besonders fiesen Trick: Er erzeugt einen neuen Eintrag in dem Menü, das Windows automatisch öffnet, wenn ein USB-Stick angeschlossen wird. Dieser Eintrag sieht fast genauso aus wie das gewohnte Feld „Ordner öffnen, um Dateien anzuzeigen“ (Bild A).

Wählt der Anwender den gefälschten Eintrag aus, startet er statt des Windows-Explorers den Schädling. USB Switchblade klaut dann Seriennummern und verschickt sie heimlich über das Internet.

Der Artikel beschreibt, mit welchen Tricks die Kriminellen heute arbeiten und wie Sie Ihren PC vor USB-Viren schützen. Alle benötigten Tools finden Sie auf Heft-DVD sowie kostenlos im Internet.

Kompakt

- ***Der Artikel erklärt, wie USB-Viren funktionieren und wie Sie Ihren PC davor schützen.***
- ***Die Tools funktionieren auf jedem USB-Stick. Es gibt sie auf Heft-DVD oder kostenlos im Internet.***

USB-Viren

USB-Würmer sind Schädlinge, die sich automatisch über den USB-Anschluss verbreiten. Von noch größerer Bedeutung sind heute jedoch USB-Viren, die eine Aktion des Nutzers erfordern, etwa

Inhalt

Virenschleuder USB

- **USB-Viren**
  - So funktionieren USB-Viren S. 41
  - Automatisch startende Würmer S. 41
  - Windows-Lücken S. 42
  - U3-Sticks S. 42
  - Nutzer täuschen S. 42
- **Schutz vor USB-Viren**
  - Windows-Patch S. 42
  - Dateinamen komplett anzeigen S. 43
  - System aktualisieren S. 43
  - USB Wächter 0.7.1.130 S. 43

So geht's: USB Wächter 0.7.1.130 S. 41
Jeder dritte Virus kommt vom Stick S. 42
Software-Übersicht S. 42
Tipp: Schreibschutz für USB-Sticks S. 43

das Doppelklicken auf eine harmlos aussehende, aber verseuchte Datei.

So funktionieren USB-Viren

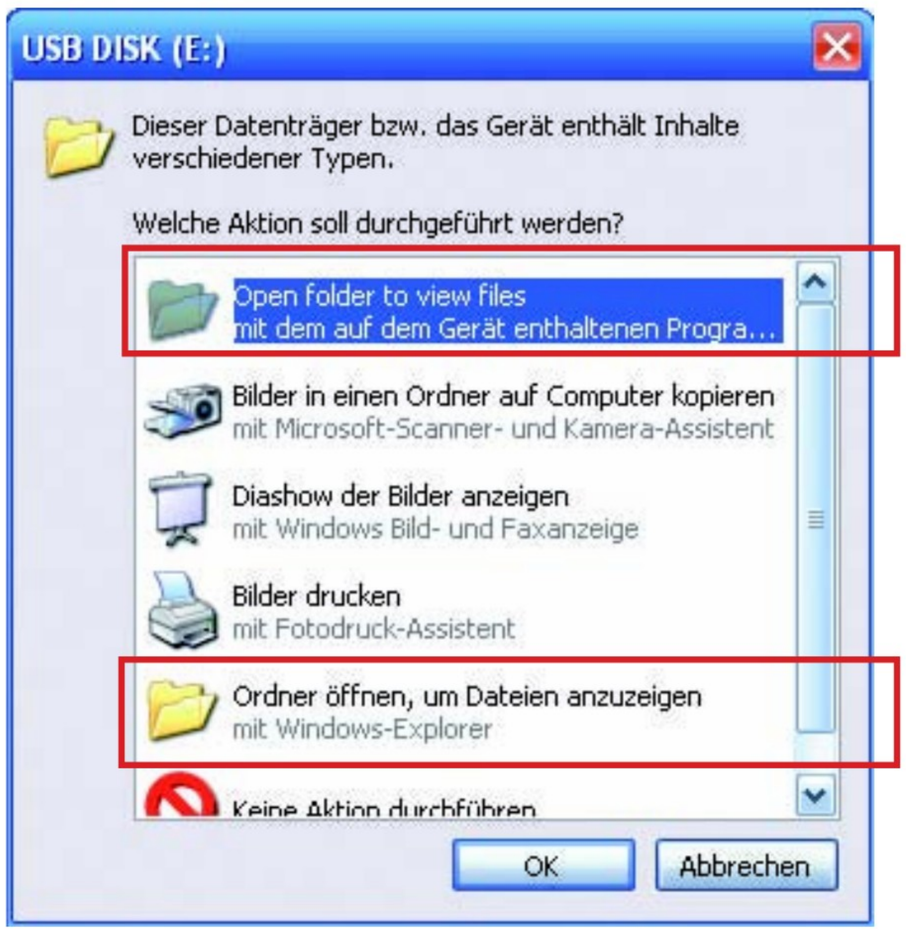
Die Funktionsweise ist recht simpel: Der Schädling befindet sich auf einem USB-Stick, den beispielsweise ein Kollege mitbringt.

Sobald der Stick an den PC angeschlossen wird, startet Windows automatisch den Virus. Dieser kopiert sich auf alle Festplatten des Computers und sorgt dafür, dass er bei jedem erneuten PC-Start automatisch aktiviert wird.

Sobald dann ein anderer USB-Stick an den Computer angeschlossen wird, kopiert sich der Wurm auch auf diesen Datenträger und infiziert so langsam, aber sicher immer mehr Rechner.

Die gute Nachricht: Bis auf ungepatchte Versionen von Windows XP sind mittlerweile alle Windows-Varianten gegen diese automatische Verbreitung von USB-Würmern geschützt.

Trotzdem ist die Gefahr nicht gebannt. Neben der automatischen Verbreitung gibt es noch andere Tricks, um Schädlinge über den USB-Anschluss einzuschleusen.



USB Switchblade: Unten sehen Sie den Original-Eintrag im USB-Menü, oben den vom Schädling nachgeahmten Eintrag (Bild A)

Automatisch startende Würmer

Die älteste Methode ist das bereits beschriebene automatische Starten einer ausführbaren Datei, sobald ein USB-Stick oder eine USB-Festplatte an den PC angeschlossen wird. Hier platzieren die Kriminellen eine Datei namens „autorun.inf" auf dem Datenträger, die etwa diesen Inhalt haben kann:

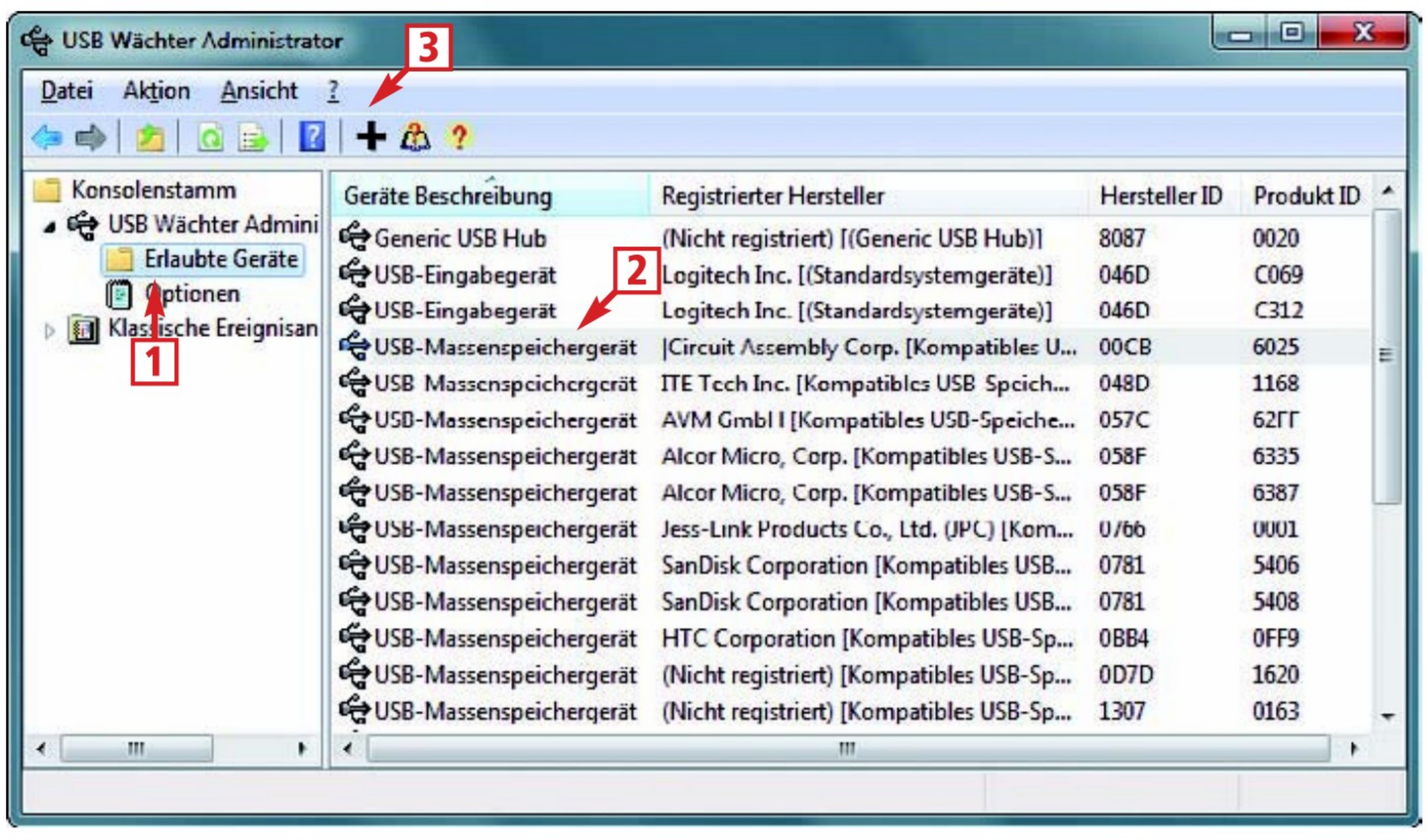
```
1 [autorun]
2 open=autorun.exe
```

Außerdem befindet sich auf dem verseuchten Stick die Datei „autorun.exe", die den Schädling enthält. ▶

wiwobooks 2.0

So geht's: USB Wächter 0.7.1.130

USB Wächter 0.7.1.130 sperrt fremde USB-Sticks und -Festplatten an Ihrem PC (kostenlos, www.trinit-soft.de/usb-waechter und auf DVD). Das Tool verhindert so, dass Dateien auf diesen USB-Sticks geöffnet oder kopiert werden können.



1 Erlaubte Geräte
Klicken Sie hier, um alle zugelassenen USB-Geräte anzuzeigen.

2 USB-Massenspeichergerät
Jeder Eintrag in diesem Bereich ist ein freigegebener USB-Stick oder eine USB-Festplatte.

3 Pluszeichen
Klicken Sie auf den Button, um einen Assistenten zu starten, der neue USB-Hardware freischaltet.

Frühere Versionen von Windows haben die Datei automatisch gestartet. Bereits in Windows XP und Vista hat Microsoft dieser Methode jedoch einen Riegel vorgeschoben. Das Update KB967715 (kostenlos, http://support.microsoft.com/kb/967715) deaktiviert alle Autorun-Funktionen (Bild B). Windows 7 ist von Haus aus sicher gegen automatisch startende USB-Viren.

Windows-Lücken

Immer wieder werden auch neue Lücken in Windows bekannt, die sich von USB-Viren ausnutzen lassen.

So war es mit manipulierten Verknüpfungen möglich, Dateien auf einem infizierten USB-Stick automatisch auszuführen. Patches, die diese LNK-Lücke schließen, finden Sie unter www.microsoft.com/technet/security/bulletin/MS10-046.mspx.

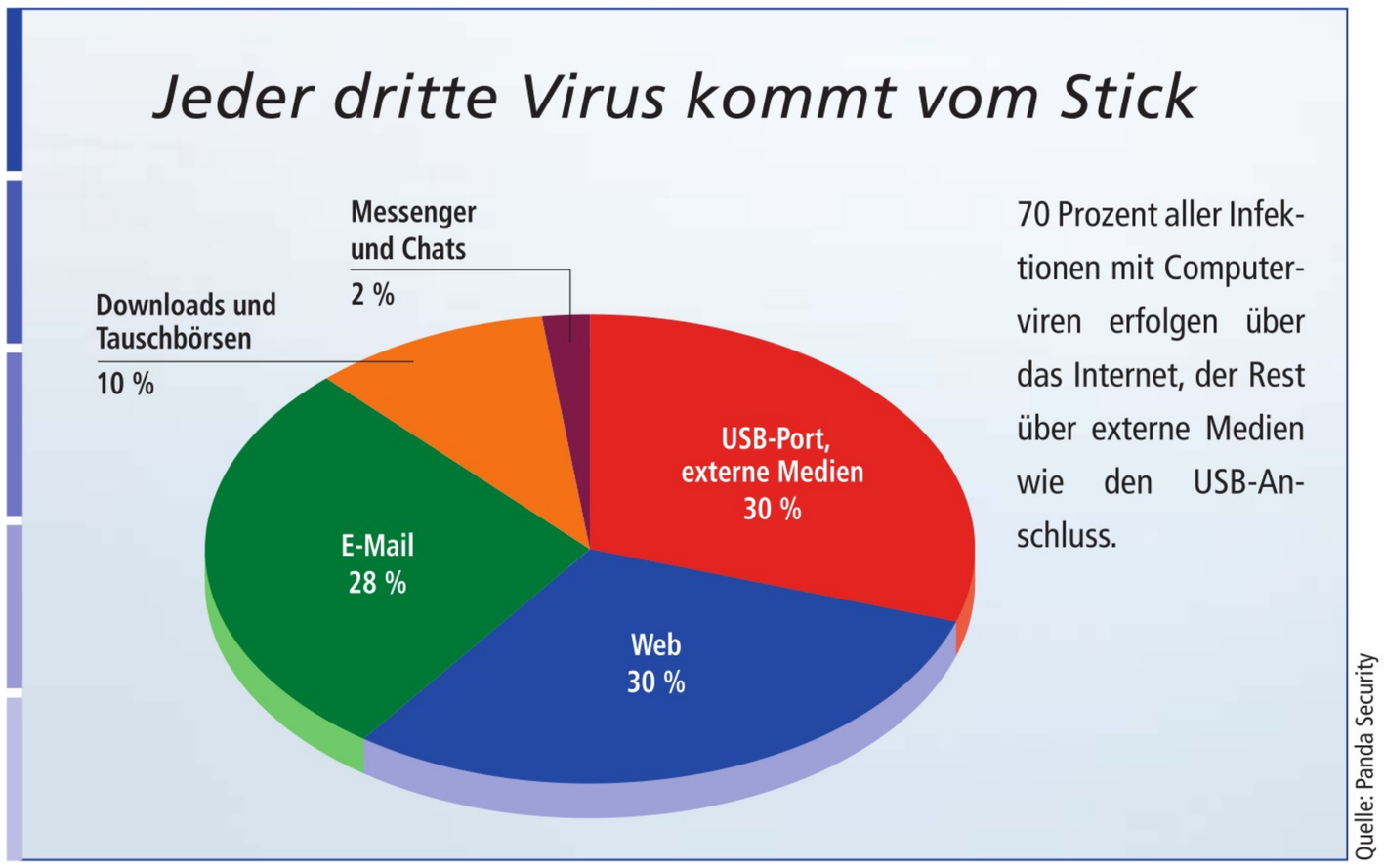
U3-Sticks

Ein weiterer Trick zum Einschleusen von USB-Viren funktioniert nur mit U3-Sticks, die ein virtuelles CD-ROM-Laufwerk automatisch einbinden.

Ausführbare Dateien in diesem Laufwerk startet Windows XP automatisch, also auch Viren. U3-Sticks waren aber kein Verkaufserfolg und sind nur noch relativ selten anzutreffen. Windows 7 war von dieser Lücke nie betroffen. Auch Vista ist bereits durch die Benutzerkontensteuerung geschützt – sofern der Nutzer sie nicht deaktiviert hat.

Nutzer täuschen

Die vierte und letzte Möglichkeit ist die derzeit gefährlichste: Hierbei präparieren die Angreifer den Stick mit gefälschten Menüeinträgen oder Dateien, die beim Anwender Interesse wecken sollen, sie zu öffnen. Das kann etwa eine Datei „Strandfoto.exe“ sein, die neben einem Urlaubsbild einen Schädling enthält, oder die Datei „Gehaltsdaten.pdf“, die über eine Lücke im Adobe Reader einen Schädling einschleust.



Schutz vor USB-Viren

Folgende Tipps schützen Ihren Computer vor USB-Würmern, die automatisch starten, und vor USB-Viren, die den Nutzer mit Täuschungen hereinlegen wollen.

Windows-Update: Statten Sie Windows XP und Vista mit diesem Patch aus, damit USB-Würmer nicht mehr automatisch starten können (Bild B)

Windows-Patch

Gegen das automatische Ausführen eines USB-Wurms sind alle Windows-Versionen geschützt. Bei XP und Vista muss dafür jedoch das Update KB967715 eingespielt sein (kostenlos, http://support.microsoft.com/kb/967715).

So finden sie heraus, ob Ihr Windows diesen Patch bereits enthält: Rufen Sie „Start, Systemsteuerung, Software“ auf. Setzen Sie dann das Häkchen vor „Updates anzeigen“. Suchen Sie nun nach dem Eintrag „Update für Windows XP (KB967715)“. Wenn der Eintrag nicht vorhanden ist, laden Sie den Patch von http://support.microsoft.com/kb/967715 herunter und installieren ihn mit einem Doppelklick. Ein Neustart des PCs ist danach nicht nötig.

Software-Übersicht

Programm	Quelle	Seite
KB967715 (Patch für Windows XP und Vista)	http://support.microsoft.com/kb/967715	42
Personal Software Inspector 2.0 (Updater)	http://secunia.com/vulnerability_scanning/personal	43
USB-Schreibschutz (REG-Dateien)	www.com-magazin.de/ergaenzungen	43
USB Wächter 0.7.1.130 (USB-Tool)	www.trinit-soft.de/usb-waechter	43

Alle -Programme finden Sie auf Heft-DVD in der Rubrik „Windows, Virenschleuder USB“.

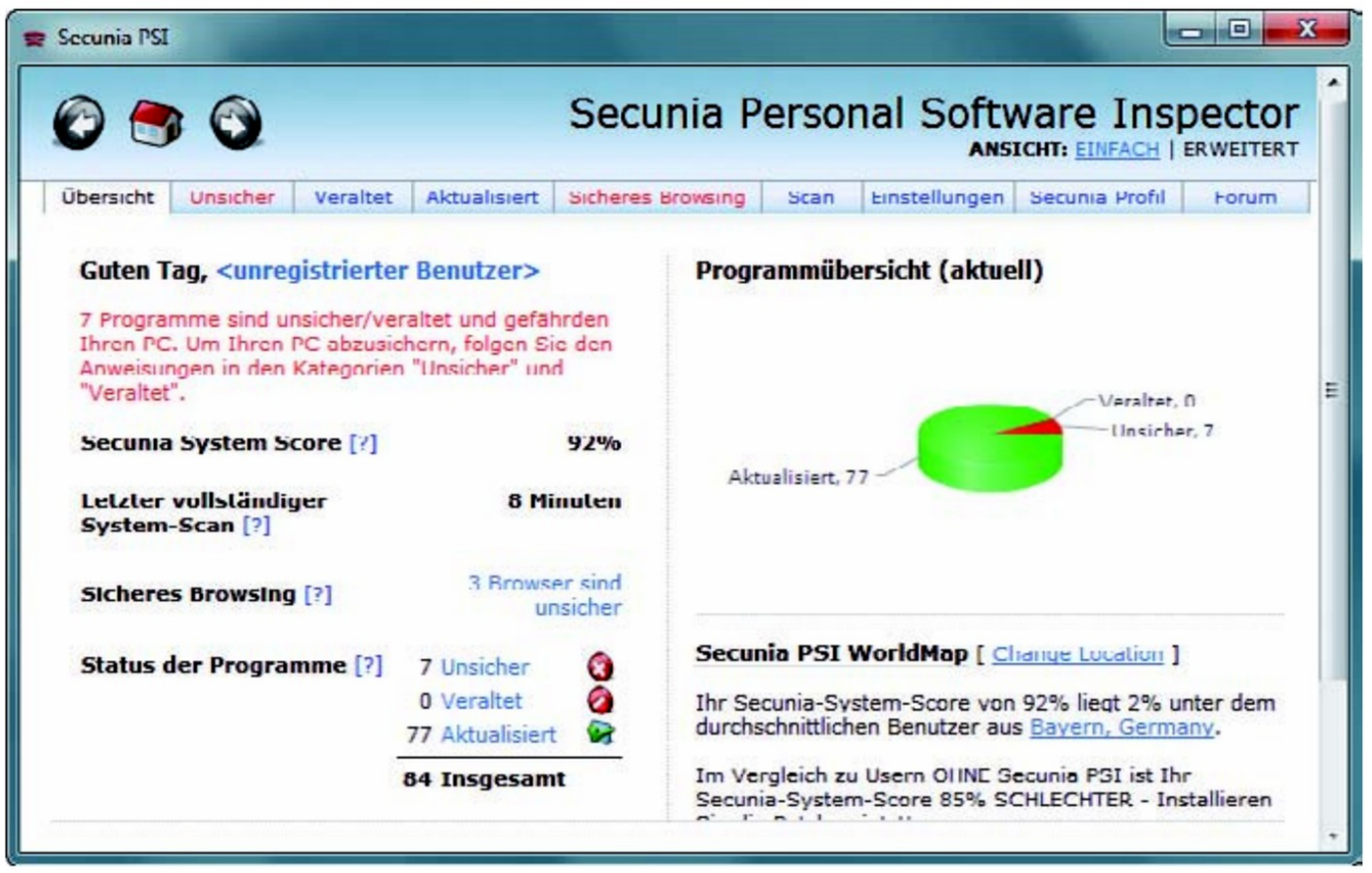
Windows 2.0

Dateinamen komplett anzeigen

Auch wenn es schon vielfach erwähnt wurde: Lassen Sie sich im Windows-Explorer unbedingt die Dateiendungen anzeigen. Nur so erkennen Sie eine ausführbare Datei sofort, die sich zu tarnen versucht.

System aktualisieren

Zur Absicherung eines Systems gehört auch das regelmäßige Aktualisieren von Windows und der installierten Anwendungen. Nur so verhindern Sie etwa, dass sich beim Öffnen einer verseuchten PDF-Datei ein Schädling einschleicht. Am einfachsten halten Sie Ihren PC mit dem Personal Software Inspector 2.0 aktuell (kostenlos, http://secunia.com/vulnerability_scanning/personal und auf) (Bild C).



Personal Software Inspector 2.0: Das Update-Tool aktualisiert auf Ihrem PC installierte Software und schließt so Lücken, über die sich USB-Viren einschleichen (Bild C)

USB Wächter 0.7.1.130

USB Wächter 0.7.1.130 erlaubt nur noch USB-Sticks an Ihrem PC, die Sie freigeben (kostenlos, www.trinit-soft.de/usb-waechter und auf). Bei nicht freigegebenen USB-Geräten verhindert das Tool die Installation des passenden Treibers.

Nach der Installation nimmt USB Wächter automatisch alle bislang an Ihrem PC angeschlossenen Sticks in die Liste der erlaubten Sticks auf. Am besten löschen Sie zuerst alle „USB-Massenspeichergeräte“ aus der Liste und fügen danach Ihre USB-Sticks hinzu. Wählen Sie zu entfernende Einträge mit der Maus aus und drücken Sie [Entf].

Vorsicht: Entfernen Sie auf keinen Fall Einträge wie „Generic USB Hub“ oder „USB-Eingabegerät“. Sonst funktionieren anschließend eventuell Maus und Tastatur nicht mehr.

Um einen Stick zur Erlaubnisliste hinzuzufügen, klicken Sie auf das schwarze Plus-Symbol und dann in dem neuen Fenster auf „Weiter“. Stecken Sie jetzt den Stick an den PC an. Nach kurzer Zeit erscheint er in dem großen Feld. Setzen Sie das Häkchen vor seinem Namen und bestätigen Sie mit „Weiter“ sowie „Fertig stellen“. Eine detaillierte Beschreibung der Bedienoberfläche finden Sie im Kasten „So geht's: USB Wächter 0.7.1.130“ auf Seite 41. ■

Andreas Th. Fischer
sonderheft@com-magazin.de

Tipp: Schreibschutz für USB-Sticks

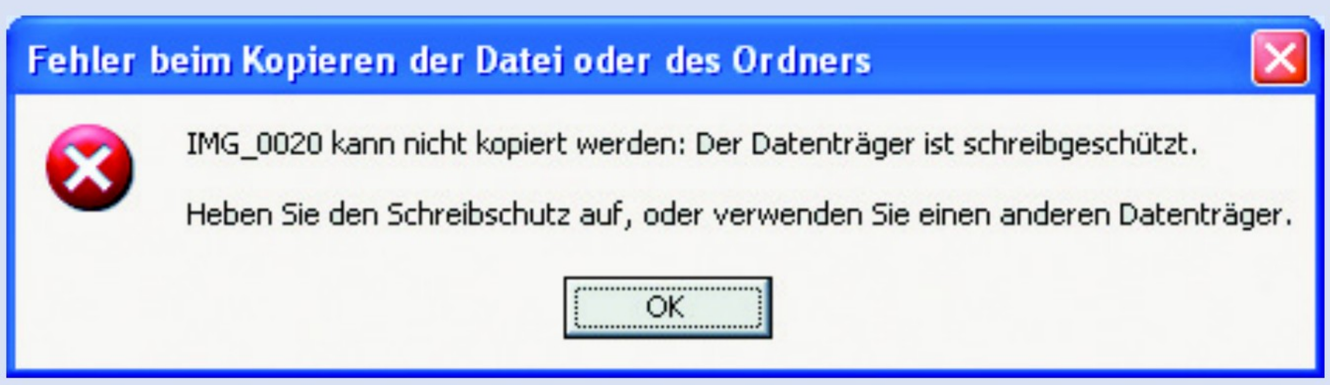
So verhindern Sie, dass jemand Daten von Ihrem PC klaut und auf seinem USB-Stick speichert.

Diese relativ brachiale Lösung schützt zwar Ihren PC nicht vor Viren, die über den USB-Stick eingeschleust werden. Dafür verhindert sie aber ein für allemal, dass Daten von Ihrem PC auf USB-Sticks gespeichert werden. Es handelt sich um einen generellen Schreibschutz für USB-Sticks und -Festplatten.

Letztendlich besteht dieser Schreibschutz nur aus zwei REG-Dateien: „Schreibschutz_an.reg“ schaltet den Schreibschutz ein, „Schreibschutz_aus.reg“ schaltet ihn wieder aus. Beide Dateien finden Sie auf Heft-DVD.

Eine REG-Datei enthält einen neuen Schlüssel für die Registrierungsdatenbank von Windows. Durch einen Doppelklick auf „schreibschutz_an.reg“ wird die Änderung in die Registrierungsdatenbank Ihres PCs geschrieben. Künftig lassen sich Daten von Sticks zwar lesen, beim Schreiben erscheint jedoch eine Fehlermeldung (Bild D).

Um den Schreibschutz wieder zu entfernen, führen Sie „Schreibschutz_aus.reg“ aus.



Schreibschutz für USB-Sticks: Eine REG-Datei verhindert, dass jemand ohne Ihre Erlaubnis von Ihrem PC aus Daten auf USB-Sticks kopiert (Bild D)

Weitere Infos

- http://four.cs.uni-bonn.de/fileadmin/user_upload/werner/cfdetector
  Webseite, die testet, ob Ihr PC mit dem USB-Wurm Conficker verseucht ist

winobooks 2.0

Hosts-Datei für Profis

So schützen Sie Ihren Computer mit der Hosts-Datei und einem kostenlosen Tool vor mehr als hunderttausend gefährlichen Internetadressen.

Die Hosts-Datei, die auf jedem Windows-Rechner vorhanden ist, ist ein gutes Werkzeug, um den Zugriff auf gefährliche Webseiten zu verhindern und um Werbung zu blockieren.

Das müssen Sie wissen

Eigentlich ist die Hosts-Datei ein Relikt aus den Anfangszeiten des Internets. Warum sie trotzdem noch überaus wichtig ist, lesen Sie in den folgenden Abschnitten.

Kompakt

- *Die Hosts-Datei ist ein lokales Adressbuch für Internetadressen.*
- *Das kostenlose Tool Hostsman 3.2.73 nutzt die Hosts-Datei, um den Zugriff auf gefährliche URLs zu unterbinden.*

Was ist die Hosts-Datei?

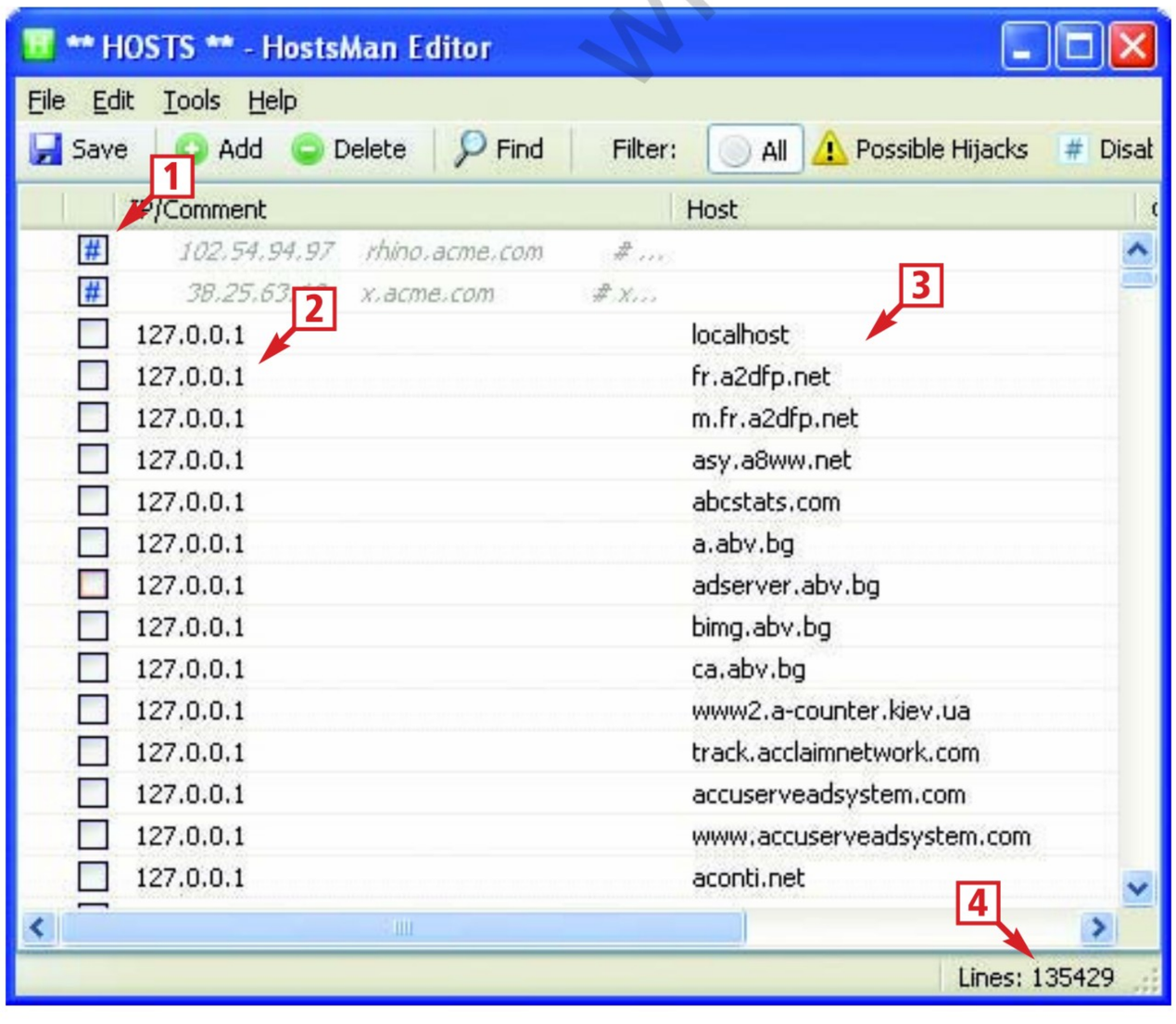
Die ersten Computer im Internet nutzten die Hosts-Datei als universelles Adressbuch. Auf jedem Rechner befand sich eine Hosts-Datei. Ein Computer, der mit einem anderen kommunizieren wollte, musste in seinem lokalen Adressbuch – der Hosts-Datei – nachsehen, um die richtige Adresse zu erfahren. Klar, dass dieses System schnell an seine Grenzen stieß.

Im Prinzip wurde die Hosts-Datei mit dem Domain Name System (DNS) überflüssig. Heutzutage speichern DNS-Server alle Internetadressen in gigantischen Datenbanken, die laufend aktualisiert werden.

www.books2.0

So geht's: Hostsman 3.2.73

Die Freeware Hostsman 3.2.73 schützt Ihren Computer mit Hilfe der Hosts-Datei vor gefährlichen Webseiten und vor Werbung (kostenlos, www.abelhadigital.com/hostsman und auf). Dazu holt sich Hostsman Sperrlisten von bekannten gefährlichen Seiten aus dem Internet und blockiert den Zugriff darauf.

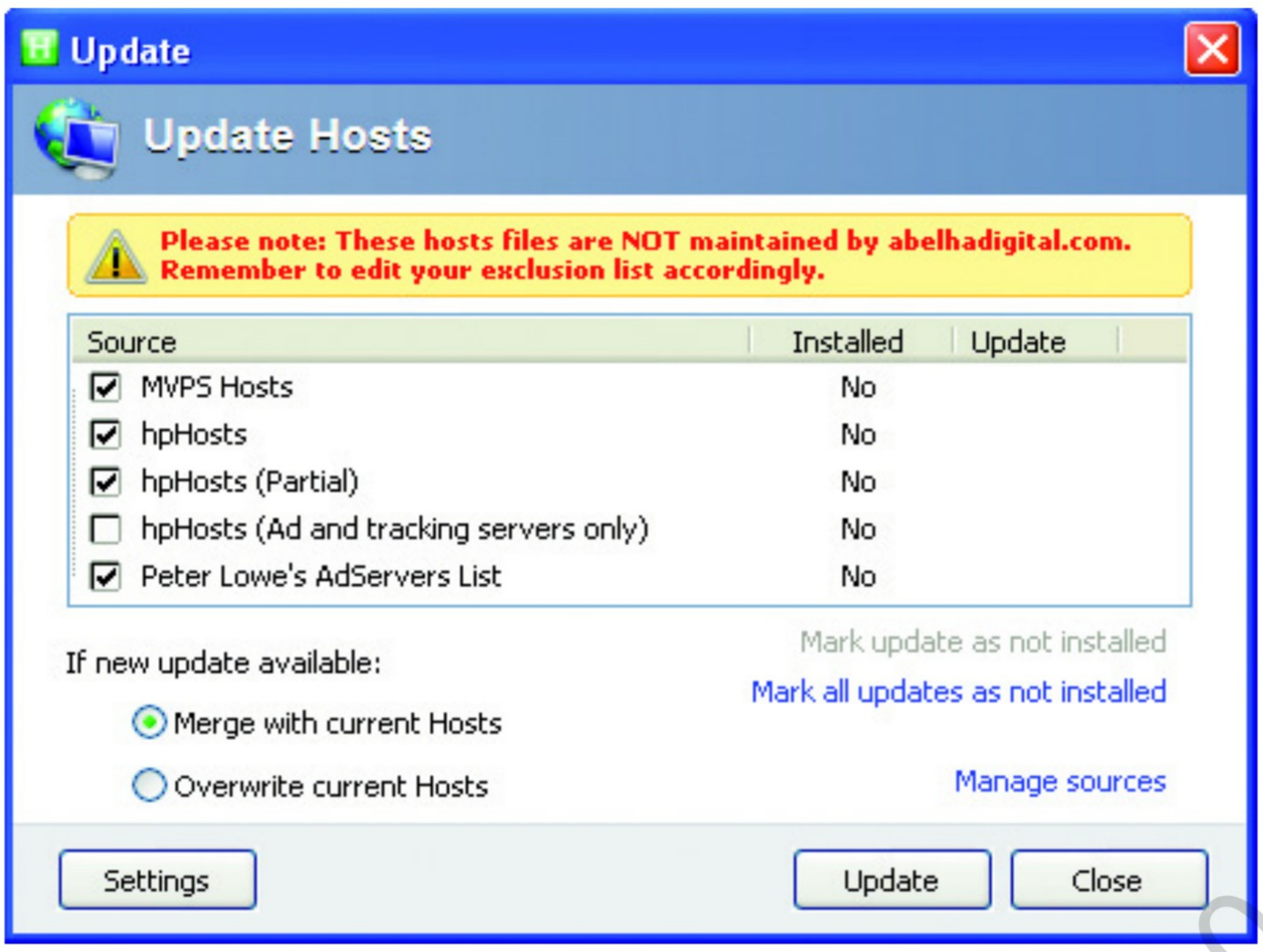


1 Rautezeichen
Kommentarzeilen beginnen mit dem Zeichen #.

2 127.0.0.1
Das ist die Adresse des lokalen PCs, auf den Anfragen umgeleitet werden.

3 Gefährliche URLs
Hier stehen die Adressen, die über Ihre Hosts-Datei geblockt werden.

4 Lines
Gesamtzahl aller in der Hosts-Datei aufgelisteten gefährlichen Webseiten.



Hostsman 3.2.73: Das Tool verwendet die Hosts-Datei, um den Zugriff auf gefährliche Webseiten zu verhindern. Dazu lädt es Sperrlisten wie „MVPS Hosts" und „hpHosts" herunter (Bild A)

Aber auch heute noch befindet sich auf jedem Windows-PC eine Hosts-Datei. Bevor Windows einen DNS-Server beispielsweise nach der richtigen IP-Adresse von Microsoft fragt, sieht es zuerst in der lokalen Hosts-Datei nach. Befindet sich dort ein Eintrag zu der gewünschten Adresse, fragt Windows nicht mehr bei einem DNS-Server nach. Die Hosts-Datei hat also Vorrang vor dem DNS-Server.

Die Hosts-Datei ist sehr simpel aufgebaut. Zuerst kommt die IP-Adresse und danach die ausgeschriebene, von Menschen leichter zu verstehende Adresse, also zum Beispiel:

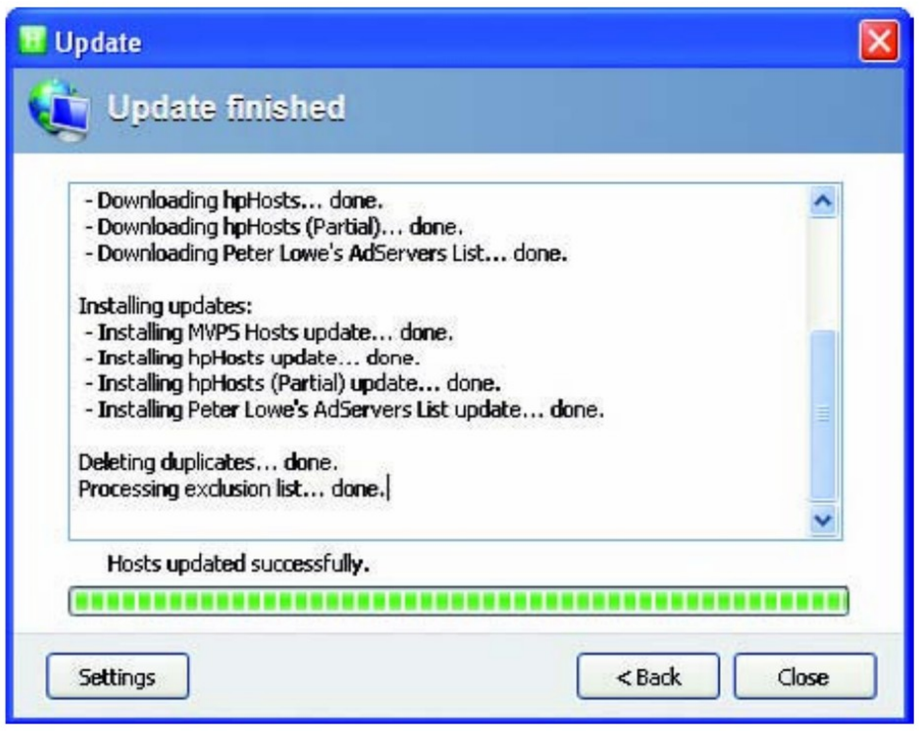
```
1 207.46.197.32·www.microsoft.de
```

Der Eintrag bedeutet, dass der Webserver von Microsoft unter der IP-Adresse 207.46.197.32 zu erreichen ist.

Die Hosts-Datei in einem frisch installierten Windows enthält – nach einem längeren Einleitungstext – meist nur den Eintrag

```
1 127.0.0.1·localhost
```

Bei der Entwicklung des Internetprotokolls wurde festgelegt, dass 127.0.0.1 immer die Adresse des lokalen PCs ist. Wenn Sie also `localhost` aufrufen, dann landet die Anfrage bei Ihrem PC. Weil dort meist kein Webserver läuft, sehen Sie nur eine Fehlermeldung.



PC-Schutz aktualisieren: Hostsman 3.2.73 lädt die von Ihnen ausgewählten Sperrlisten herunter, fügt die Listen zusammen und entfernt Duplikate (Bild B)

Auf DVD

Hostsman 3.2.73 finden Sie auf DVD in der Rubrik „Windows, Hosts-Datei".

Inhalt

Hosts-Datei für Profis

- **Das müssen Sie wissen**
  - Was ist die Hosts-Datei? S. 44
  - Wie schützt die Hosts-Datei vor gefährlichen Webseiten? S. 45
- **Hostsman 3.2.73**
  - Hostsman 3.2.73 installieren S. 46
  - Gefährliche Seiten blocken S. 46
  - Weitere Sperrlisten S. 47
  - Protokoll geblockter Seiten S. 47

So geht's: Hostsman 3.2.73 S. 44
Pharming: Hosts-Datei missbraucht S. 46
Hosts-Datei: Direkt bearbeiten S. 47

Wie schützt die Hosts-Datei vor gefährlichen Webseiten?

Sie drehen dazu die normale Funktion der Hosts-Datei um: Statt einer Adresse die richtige IP-Nummer zuzuordnen, weisen Sie ihr eine falsche zu. Die gefährliche Webseite wird nie gefunden.

Konkret geht das zum Beispiel so – der folgende Eintrag in der Hosts-Datei verhindert jeden Besuch der Webseite www.rootkit.com von Ihrem PC aus:

```
1 127.0.0.1·www.rootkit.com
```

Windows sieht zuerst in der Hosts-Datei nach. Dort findet das Betriebssystem den Eintrag www.rootkit.com und fragt nicht mehr bei einem DNS-Server nach. Stattdessen leitet es die Anfrage zur IP-Adresse 127.0.0.1, also Ihrem eigenen PC, um. Statt der echten Webseite zeigt der Browser dann nur eine Fehlermeldung an.

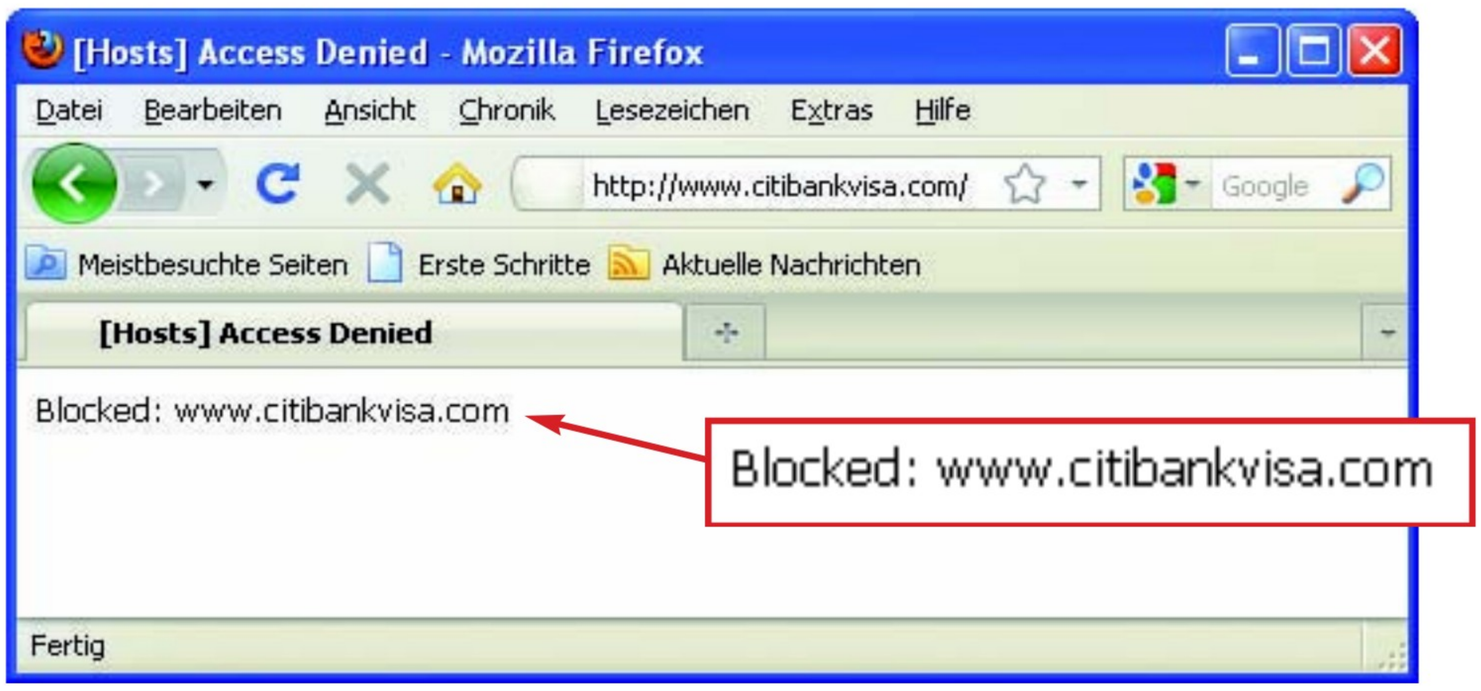
Natürlich kann niemand den Überblick über alle gefährlichen URLs behalten und diese in der Hosts-Datei eintragen. Deswegen gibt es spezielle Programme, die Ihre Hosts-Datei automatisch aktualisieren. Das beste Tool für diesen Zweck ist Hostsman 3.2.73 (kostenlos, www.abelhadigital.com/hostsman und auf DVD). ▶

www.books 2.0

Hostsman 3.2.73

Hostsman 3.2.73 bearbeitet die Hosts-Datei und fügt Sperrlisten ein. Das sind Verzeichnisse gefährlicher Webseiten, die dann künftig gesperrt werden.

Manuelle Korrekturen mit dem Texteditor von Windows, wie sie im Kasten „Hosts-Datei: Direkt bearbeiten“ auf Seite 47 beschrieben werden, sind dagegen erheblich zeitaufwendiger.



Blockiert: Hostsman 3.2.73 hat den Zugriff auf eine gefälschte Bank-Seite verhindert (Bild D)

Hostsman 3.2.73 installieren

In wenigen Schritten ist Hostsman 3.2.73 eingerichtet.

So geht's: Entpacken Sie das ZIP-Archiv „hm_3.2.73_installer.zip“ in einen Ordner auf Ihrer Festplatte. Klicken Sie dann doppelt auf die Datei „Hosts Man_Setup.exe“, um die Installation zu starten.

Bestätigen Sie das Willkommensfenster mit „Next“ und akzeptieren Sie dann mit „I accept the terms of the License Agreement“ sowie „Next“ die Lizenzbedingungen. Klicken Sie anschließend noch dreimal auf „Next“ und starten Sie die eigentliche Installation von Hostsman im Dialog „Additional Options“ mit „Install“.

Zuletzt schließen Sie die Installation mit „Next“ und „Finish“ ab. Hostsman ist jetzt einsatzbereit.

Gefährliche Seiten blocken

Hostsman lädt Sperrlisten aus dem Internet herunter und integriert sie in Ihre Hosts-Datei. Diese Listen werden von Freiwilligen erstellt und laufend gepflegt.

So geht's: Starten Sie Hostsman und klicken Sie auf „Hosts, Check for Updates …“. Ein neues Fenster öffnet sich, in dem Sie Sperrlisten auswählen, die in Ihre Hosts-Datei integriert werden sollen. Setzen Sie dazu einfach ein Häkchen vor diese Listen (Bild A).

MVPS Hosts ist auf gefährliche Seiten spezialisiert und blockiert Webseiten, die Schädlinge sowie Adware auf Ihrem PC einschleusen wollen.

HpHosts enthält ebenfalls Seiten, die Schädlinge verbreiten. Außerdem blockiert HpHosts nervige Werbung sowie Seiten, die Ihr Surfverhalten protokollieren. Der Eintrag „hpHosts“ im Update-Fenster ist die Hauptliste, die nicht so häufig aktualisiert wird. „hpHosts (Partial)“ ist erheblich kleiner und enthält lediglich die Aktualisierungen seit dem letzten großen Update. „hpHosts (Ad and tracking servers only)“ enthält nur die Werbeseiten und muss nicht ausgewählt werden, wenn bereits der Eintrag „hpHosts“ markiert wurde.

Peter Lowe's AdServers List ist eine weitere, auf das Blockieren unerwünschter Werbung spezialisierte Sperrliste.

Zuletzt klicken Sie auf „Update“, um die ausgewählten Sperrlisten herunterzuladen und in Ihre Hosts-Datei zu integrieren. Das Tool entfernt anschließend automatisch doppelt vorhandene Einträge (Bild B).

Pharming: Hosts-Datei missbraucht

So wie Sie die Hosts-Datei dazu verwenden können, Ihren PC vor gefährlichen Seiten zu schützen, wird sie von Kriminellen auch missbraucht. Das nennt man Pharming.

Ein Virus kann mit Hilfe der Hosts-Datei den Besuch der Webseiten bekannter Antivirenhersteller verhindern (Bild C). Wegen folgendem Eintrag würde Windows beispielsweise jeden Zugriff auf die Symantec-Webseite blockieren:

```
1 127.0.0.1·www.symantec.de
```

Oder der Schädling trägt die Adressen der Webseiten von Banken, Auktionsplattformen und Online-Shops in die Hosts-Datei ein und verknüpft sie mit den IP-Adressen gefälschter Seiten. Statt auf der richtigen Seite landet der Surfer dann auf der Kopie. Das Fatale an diesem Trick ist, dass in der Adressleiste des Browsers trotzdem die richtige Adresse steht. Überprüfen Sie deshalb den Inhalt Ihrer Hosts-Datei, wenn die Webseiten von Sicherheitsanbietern unerreichbar sind.

Unter Vista und Windows 7 wird die Hosts-Datei durch das Betriebssystem geschützt. Wenn ein Trojaner versucht, sie zu manipulieren, meldet sich die Benutzerkontensteuerung und erbittet Ihre Zustimmung. Unter XP oder bei abgeschalteter Benutzerkontensteuerung ist eine heimliche Veränderung der Hosts-Datei durch einen Schädling jedoch jederzeit möglich.

Missbrauchte Hosts-Datei: Kriminelle manipulieren die Hosts-Datei und unterbinden so etwa den Besuch der Symantec-Seite (Bild C)

www.wowbooks 2.0

Weitere Sperrlisten

Neben den bereits in Hostsman integrierten Sperrlisten gibt es noch weitere Quellen im Internet, die Sie mit wenig Aufwand in Ihre Hosts-Datei einfügen.

Dazu zählt die **Malwaredomainlist** (www.malwaredomainlist.com), die brandneue URLs von gefährlichen Seiten sammelt und eine der wichtigsten Listen bietet. Auf lästige Werbeserver ist **Cameleon** (http://sysctl.org/cameleon) spezialisiert, während **Hostsfile.org** (www.hostsfile.org) vor allem pornografische und Zocker-Adressen, aber auch viele Adserver-Adressen enthält.

So geht's: Öffnen Sie Hostsman und rufen Sie „Hosts, Check for Updates …" sowie „Manage sources" auf. Klicken Sie auf „Add Source" und tragen Sie in das obere Feld `Malwaredomainlist` ein und ins Feld darunter `http://www.malwaredomainlist.com/hostslist/hosts.txt`. Bestätigen Sie mit „OK, Close" und klicken Sie auf den Button „Update".

Fügen Sie anschließend noch Cameleon hinzu. Das Vorgehen ist das gleiche wie bei der Malwaredomainlist. Tragen Sie ins obere Feld `Cameleon` ein und ins untere Feld `http://sysctl.org/cameleon/hosts.win`.

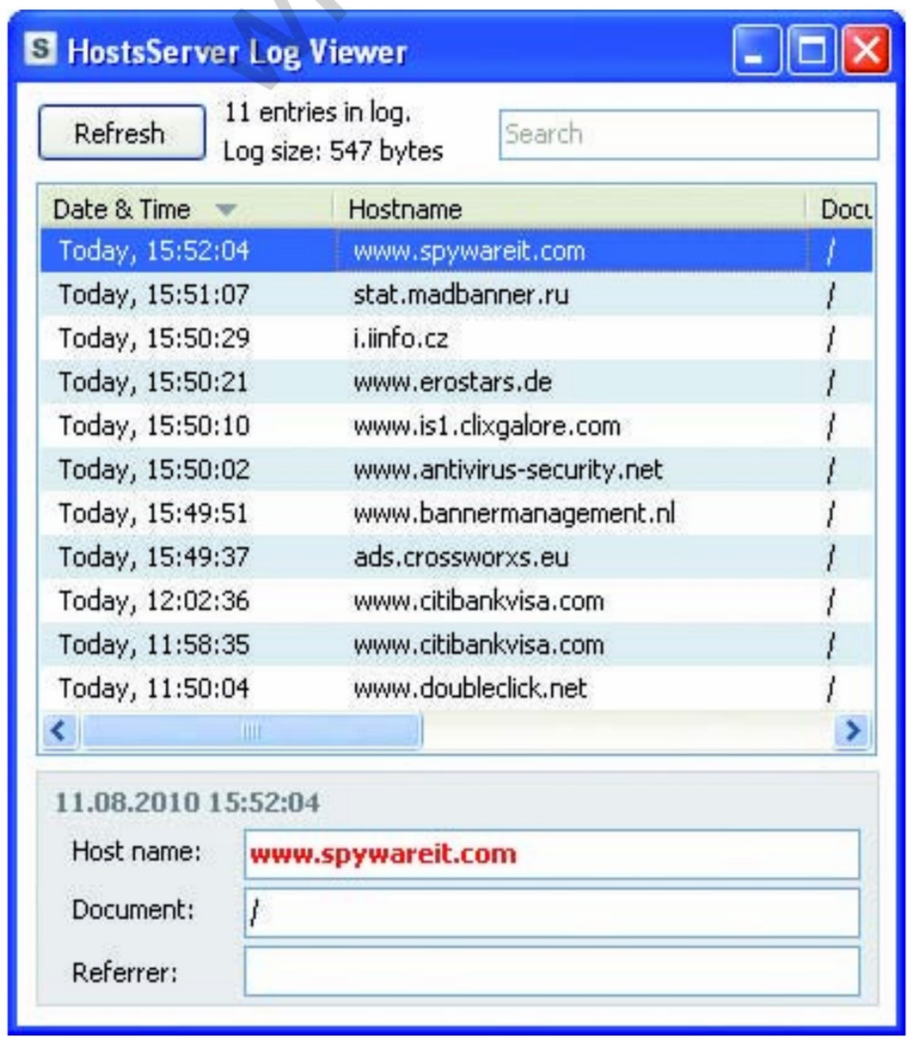
Hostsfile.org fügen Sie hinzu, indem Sie in das obere Feld `Hostsfile.org` und ins untere Feld `http://hostsfile.org/Downloads/hosts.txt` eintragen.

Protokoll geblockter Seiten

Wenn eine Seite mit Hilfe der Hosts-Datei auf den lokalen Rechner umgeleitet wird, dann sehen Sie lediglich eine Fehlermeldung, dass die Seite nicht erreichbar ist.

Das kann leicht mit einer normalen Fehlermeldung verwechselt werden, wenn eine Webseite einmal nicht erreichbar ist.

Hostsman verfügt deswegen über einen integrierten Webserver, der auf Ihrem lokalen PC läuft. Dieser kleine Webserver weist ausdrücklich darauf hin, dass eine Seite geblockt wurde. Außerdem protokolliert er auch gleich sämtliche geblockten Seiten.



Protokolldatei: Hostsman 3.2.73 erstellt eine Liste aller Internetadressen, deren Aufruf von Ihrem PC verhindert wurde (Bild E)

So richten Sie den Webserver ein: Öffnen Sie das Kontrollfenster für den Hosts-Server mit „Tools, HostsServer, Control Panel …" und starten Sie den Server mit einem Klick auf „Start Server". Ab sofort erhalten Sie beim versehentlichen Ansurfen einer geblockten Seite einen Hinweis im Browser (Bild D).

Damit der Hosts-Server in Zukunft automatisch gestartet wird, klicken Sie im „HostsServer Control Panel" auf „Preferences". Setzen Sie unter „General" ein Häkchen vor „Start HostsServer automatically".

Ein Klick auf „View Log" im „HostsServer Control Panel" zeigt alle bislang geblockten Seiten an (Bild E). ■

Andreas Th. Fischer
sonderheft@com-magazin.de

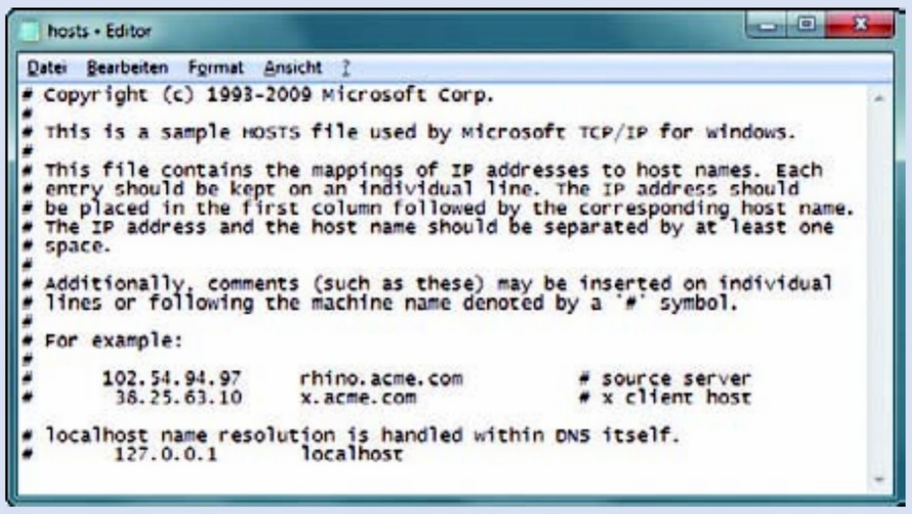
Hosts-Datei: Direkt bearbeiten

Kleinere Änderungen an der Hosts-Datei lassen sich auch mit dem integrierten Texteditor von Windows erledigen.

Unter Vista und Windows 7 lässt sich die Hosts-Datei nur als Administrator bearbeiten. Rufen Sie dazu „Start, Alle Programme, Zubehör" auf und klicken Sie mit der rechten Maustaste auf „Editor". Wählen Sie „Als Administrator ausführen" und bestätigen Sie die Abfrage der Benutzerkontensteuerung mit „Ja".

Rufen Sie nun „Datei, Öffnen …" auf und navigieren Sie zum Ordner „C:\Windows\System32\drivers\etc". Wählen Sie unten rechts bei „Textdateien (*.txt)" den Eintrag „Alle Dateien (*.*)" aus und klicken Sie danach doppelt auf die Datei „hosts" (Bild F).

Unter XP bearbeiten Sie die Hosts-Datei genauso, allerdings ist hier der Schritt „Als Administrator ausführen" nicht nötig.



Hosts-Datei bearbeiten: Unter Vista und Windows 7 geht dies nur mit Admin-Rechten (Bild F)

Weitere Infos

- www.elektronik-kompendium.de/sites/net/0901121.htm
  Hintergründe zur Entstehung der Hosts-Datei
- www.com-magazin.de/tipps/2141
  So schützt man die Hosts-Datei

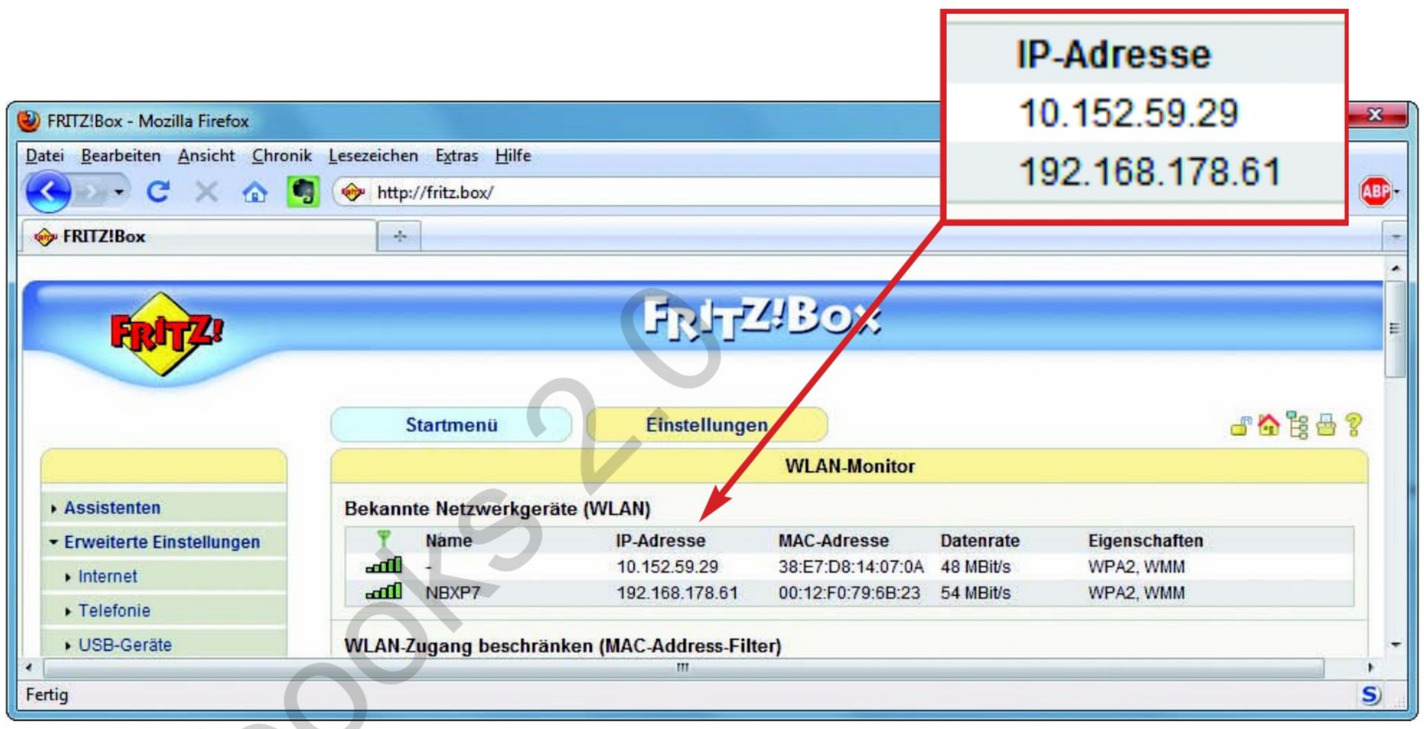
WIWOBOOKS 2.0

Wer surft in meinem WLAN?

Jedes WLAN funkt auch über die Wände Ihrer Wohnung hinaus. Nutzen Eindringlinge die große Reichweite aus und surfen heimlich über Ihre Internetleitung?

Wer sein WLAN absichtlich oder unabsichtlich für jeden offen lässt, riskiert viel Ärger. So kann ein Eindringling etwa illegal Raubkopien tauschen. Fliegt dies auf, wird dafür jedoch zunächst der Besitzer des WLANs haftbar gemacht. Die Juristen nennen dies Störerhaftung. Der Besitzer muss dann beweisen, dass nicht er derjenige war, der die Raubkopien geladen oder verbreitet hat.

Die meisten WLANs sind heute bereits weitgehend sicher konfiguriert. Aber machen Sie besser die Probe aufs Exempel: Der Artikel beschreibt, wie Sie Eindringlinge aufspüren und in wenigen einfachen Schritten Ihr WLAN abschotten.



Router-Check: Viele WLAN-Router, etwa die Fritzbox, zeigen auf einen Blick, welche Computer gerade am Funknetz angemeldet sind (Bild A)

WLAN prüfen

Vier Checks helfen Ihnen dabei, festzustellen, ob jemand Ihr WLAN ohne Ihr Einverständnis nutzt.

1. Router-Check

Der einfachste und schnellste Sicherheits-Check ist ein Blick in die Konfigurationsoberfläche Ihres DSL-Routers. Die meisten Modelle listen dort genau auf, welche Computer sich bislang angemeldet haben beziehungsweise gerade angemeldet sind und im Internet surfen.

So geht's: Rufen Sie die Konfigurationsoberfläche Ihres DSL-Routers auf. Fast alle aktuellen Modelle werden über den Browser verwaltet. Das Verwaltungsmenü der Fritzbox erreichen Sie zum Beispiel, indem Sie im Browser `http://fritz.box` eintippen.

Hinweis: Je nach Firmware-Version Ihrer Fritzbox können die Bezeichnungen leicht variieren.

Bereits auf der Übersichtsseite zeigt die Fritzbox hinter „WLAN" an, wie viele WLAN-Geräte gerade angemeldet sind. Klicken Sie auf „WLAN", um eine detaillierte Übersicht über die angemeldeten Computer zu erhalten (Bild A). Hier sehen Sie aber nur, welche Endgeräte momentan aktiv sind.

Wer etwa vergangene Nacht angemeldet war, erfahren Sie über „Startmenü, Ereignisse, WLAN". Hier protokolliert die Fritzbox alle Vorkommnisse. Also auch, wann welcher Computer angemeldet war und wann er sich wieder abgemeldet hat. Zu jedem Eintrag notiert die Fritzbox den Namen des Computers sowie seine IP- und seine MAC-Adresse. Letztere ist die weltweit eindeutige Hardware-Adresse des in einem Computer eingebauten WLAN-Adapters.

Die Fritzbox speichert diese Daten mehrere Wochen. Wie Sie sie auswerten, zeigt der nebenstehende Kasten „So geht's: Router-Protokoll auswerten".

Haben Sie einen anderen Router als eine Fritzbox und sind Sie sich nicht si-

Auf DVD

Rogue Scanner 2.6.0 finden Sie auf in der Rubrik „Internet, WLAN".

Kompakt

- *Vier Checks klären, ob jemand Ihr WLAN heimlich mitnutzt.*
- *Die Fritzbox zeichnet auf Wunsch den fremden Datenverkehr auf.*

Wiwobooks 2.0

Inhalt

Wer surft in meinem WLAN?

- **WLAN prüfen**
  - 1. Router-Check S. 48
  - 2. Ping-Check S. 49
  - 3. IP-Check S. 50
  - 4. Sniffing-Check S. 50
- **WLAN schützen**
  - Router-Passwort ändern S. 51
  - Richtig verschlüsseln S. 51
  - WLAN-Schlüssel S. 51
  - Funknetzname ändern S. 51
  - Filtern von MAC-Adressen S. 51
- So geht's: Router-Protokoll auswerten S. 49

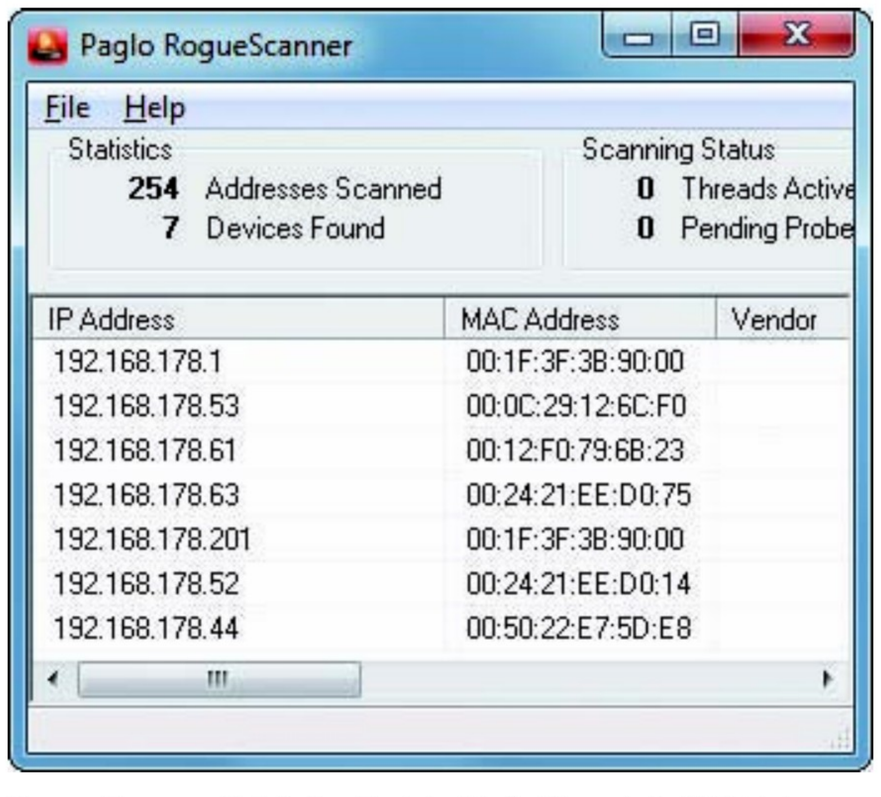
cher, unter welcher Adresse er erreichbar ist, öffnen Sie die Windows-Eingabeaufforderung mit [Windows R] und **cmd**. Tippen Sie **ipconfig** ein. Bei „Ethernet-Adapter Drahtlose Netzwerkverbindung" beziehungsweise „Drahtlosnetzwerkverbindung" finden Sie die IP-Adresse des Routers hinter „Standardgateway". Geben Sie diese Adresse im Browser ein, um die Konfigurationsoberfläche zu öffnen.

2. Ping-Check

Falls Ihr Router keine Informationen über gerade angemeldete WLAN-Geräte anzeigt, verwenden Sie das Netzwerk-Tool Rogue Scanner 2.6.0 (kostenlos, http://sourceforge.net/projects/roguescanner und auf). Rogue Scanner spürt Rechner im lokalen Netzwerk und im WLAN auf.

So geht's: Installieren Sie Rogue Scanner. Nach dem Setup startet das Tool automatisch. Im Fenster „Configuration" wählen Sie den WLAN-Adapter aus, mit dem Ihr Computer mit dem Netzwerk verbunden ist.

Ein Klick auf „OK" öffnet das Tool, das sofort mit der Suche nach Computern in Ihrem Netzwerk startet. Zu jedem gefundenen PC sehen Sie jeweils die IP- und die MAC-Adresse (Bild B).



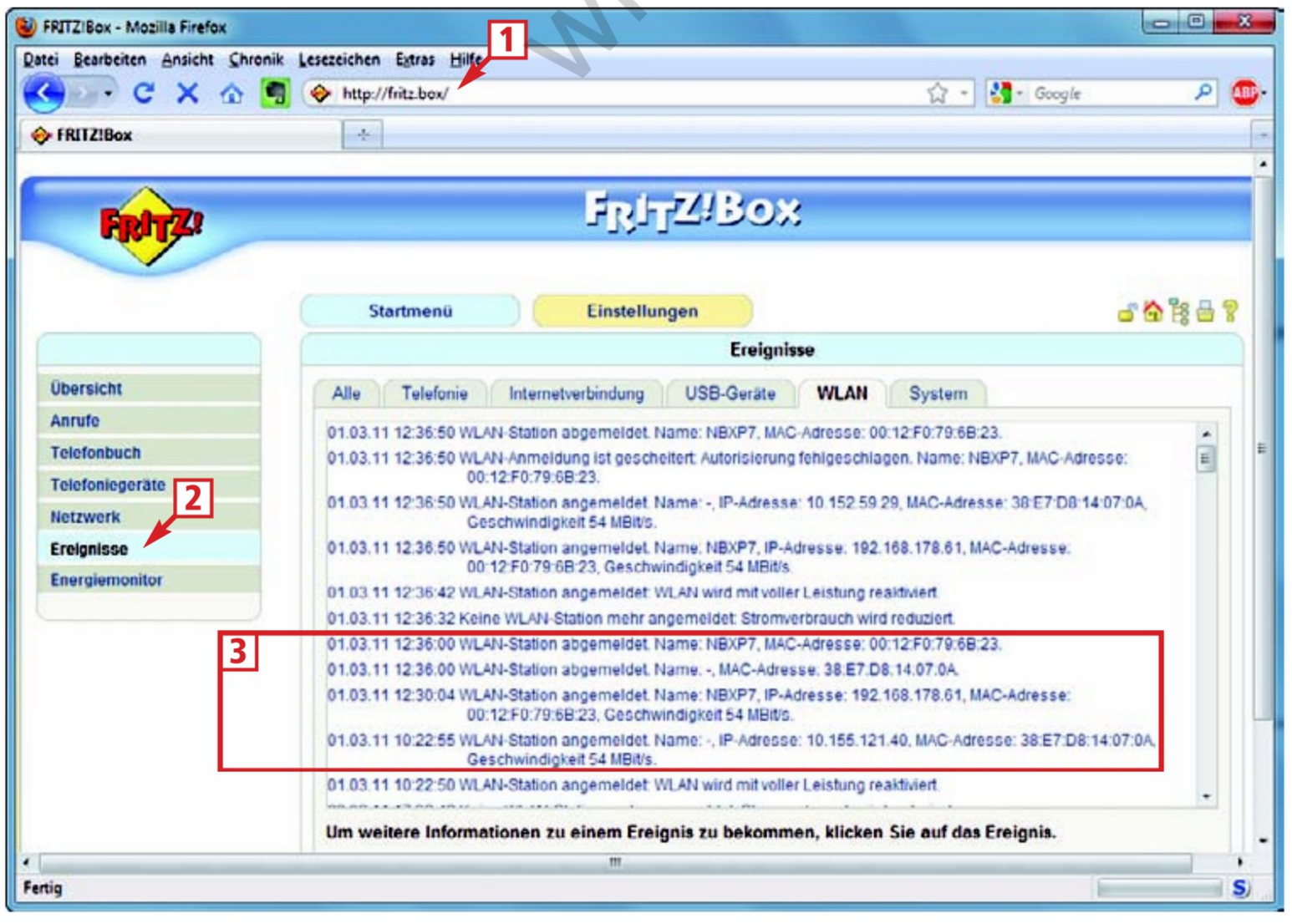
Rogue Scanner 2.6.0: Das Tool deckt die IP- und die MAC-Adressen aller Computer auf, die gerade Ihr WLAN nutzen (Bild B)

Rogue Scanner zeigt nicht nur fremde Rechner an, sondern auch Ihre eigenen PCs. Öffnen Sie deshalb auf jedem Computer ein Fenster der Windows-Eingabeaufforderung mit [Windows R] und **cmd**. Tippen Sie **ipconfig** ein. Bei „Ethernet-Adapter LAN-Verbin- ▶

wiwobooks 2.0

So geht's: Router-Protokoll auswerten

Aktuelle Router, wie hier die Fritzbox, speichern akribisch, welche Computer sich zu welchem Zeitpunkt an Ihrem WLAN an- und abgemeldet haben.

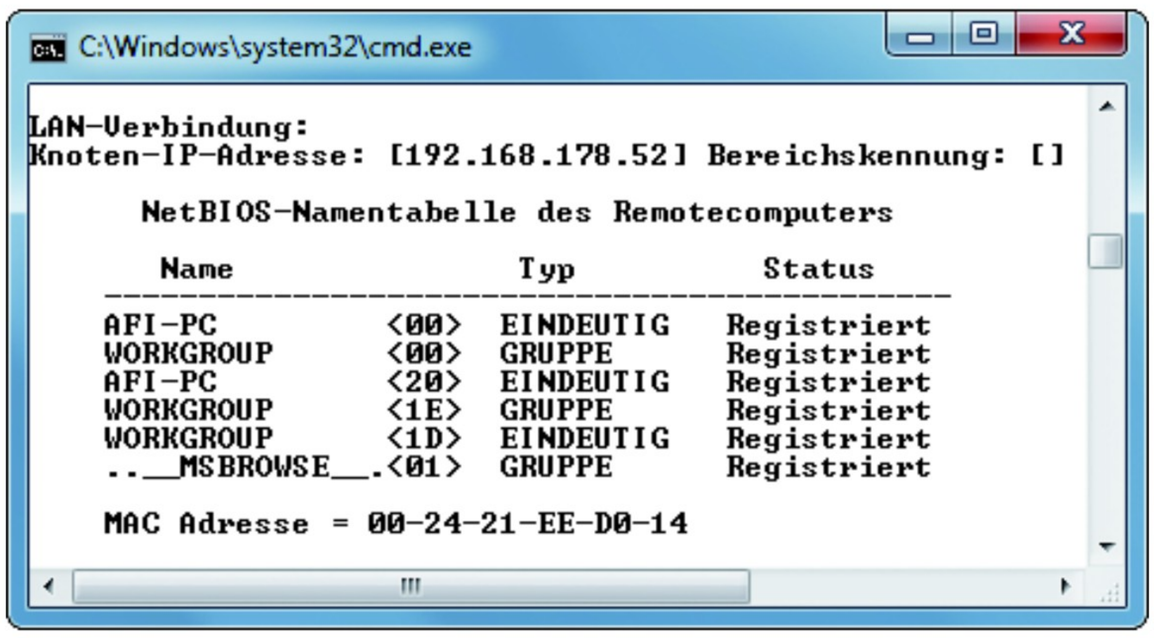


1 Adressfeld
Die Steuerung Ihrer Fritzbox erreichen Sie über die Adresse `http://fritz.box`.

2 Ereignisse
Hier finden Sie alle Protokolle, die Ihre Fritzbox automatisch erstellt.

3 WLAN
Akribisch speichert die Fritzbox Datum, Uhrzeit, Name und IP-Adresse jedes WLAN-Nutzers.

dung“ beziehungsweise „Ethernet-Adapter Drahtlose Netzwerkverbindung“ sehen Sie nun hinter „IPv4-Adresse“ die IP-Adresse Ihres Computers. Vergleichen Sie diese Information mit den IP-Adressen im Fenster von Rogue Scanner. Finden Sie eine unbekannte Adresse, haben Sie einen Eindringling aufgespürt.



IP-Check: Der Kommandozeilenbefehl **nbtstat** findet zu einer IP-Adresse heraus, wie der Name des fremden Computers lautet (Bild C)

3. IP-Check

Allein die IP-Adresse sagt noch nicht viel über einen PC aus. Mehr erfahren Sie über ihn mit dem Kommandozeilenbefehl **nbtstat**. Er zeigt den Rechnernamen und die Arbeitsgruppe.

So geht's: Öffnen Sie mit [Windows R] und **cmd** ein Fenster der Eingabeaufforderung und tippen Sie den Befehl **nbtstat·-A·<IP-Adresse>** ein. Statt **<IP-Adresse>** verwenden Sie die zuvor ermittelte IP-Adresse.

In der Spalte „Name“ erfahren Sie anschließend den PC-Namen sowie seine Arbeitsgruppe (Bild C). Mehr lässt sich über einen fremden PC nur mit einem Netzwerk-Sniffer herausfinden.

4. Sniffing-Check

Der letzte und gründlichste Check gibt Ihnen einen Einblick in die Daten, die über Ihr WLAN gesendet werden. Der Check funktioniert allerdings nur mit einer Fritzbox. Fast jede aktuelle Fritzbox verfügt über einen eingebauten Sniffer. Der Begriff leitet sich vom englischen to sniff, schnüffeln, ab und steht für ein Tool, das Daten sammelt.

Die Daten lassen sich dann mit Wireshark 1.4.4 auswerten (kostenlos, www.wireshark.org).

So geht's: Öffnen Sie den Browser und rufen Sie **http://fritz.box/html/capture.html** auf. Geben Sie das Passwort für den Router ein und bestätigen Sie mit „Anmelden“.

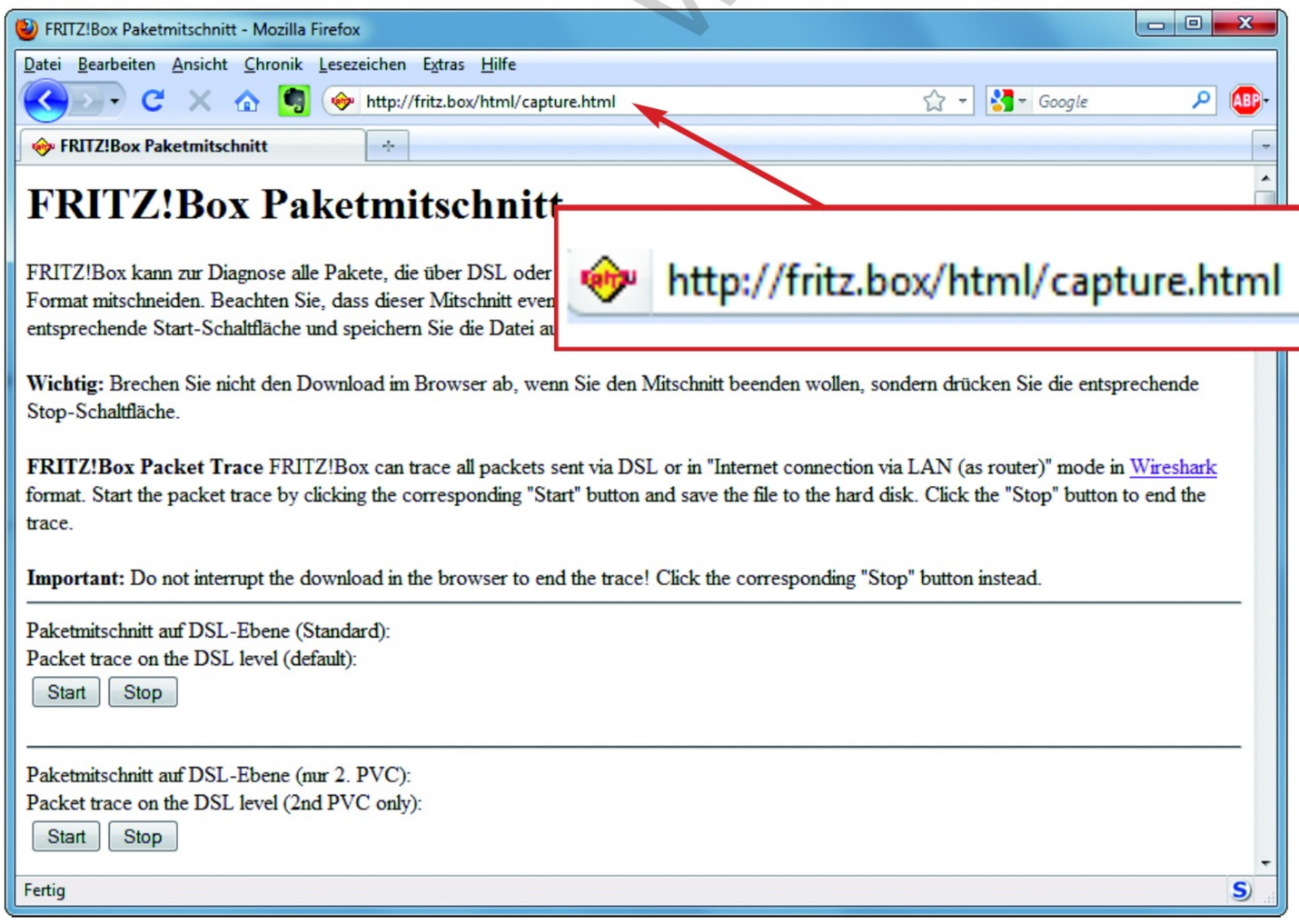
Sie sehen nun die Seite „FRITZ!Box Paketmitschnitt“ (Bild D). Scrollen Sie bis „Paketmitschnitt WLAN (wifi0)“ und klicken Sie dort auf „Start“. Ein „Speichern“-Dialog öffnet sich. Bestätigen Sie mit „OK“, legen Sie den Speicherort fest und klicken Sie auf „Speichern“. Das Mitschneiden aller übertragenen Daten beginnt. Beenden Sie die Protokollierung nach ein paar Minuten mit einem Klick auf „Stop“.

Am von Ihnen angegebenen Speicherort liegt nun eine Datei mit der Endung „.eth“. Um sie auszuwerten, benötigen Sie das Tool Wireshark. Sie finden es unter www.wireshark.org/download.html. Laden Sie das Tool herunter und installieren und starten Sie es anschließend. Ziehen Sie danach die zuvor gespeicherte ETH-Datei mit der Maus in das Wireshark-Fenster.

Sie sehen nun eine Übersicht über alle gesendeten und empfangenen Datenpakete. Interessante Pakete zu finden, ist jedoch nicht ganz einfach. Sortieren Sie die Pakete nach ihrer Quelle. Klicken Sie dazu auf „Source“.

Einträge, bei denen unter „Destination“ der Begriff „Broadcast“ steht, können Sie ignorieren. Dabei handelt es sich um Statusmeldungen sämtlicher WLAN-Router in der näheren Umgebung.

Klicken Sie nun im oberen Feld auf eines der Datenpakete und sehen Sie sich den Inhalt im untersten Feld an. Links sehen Sie hexadezimale Spalten und rechts die Auswertung in für Menschen lesbarer Darstellung. Prüfen Sie den Inhalt und drücken Sie dann die Taste [Abwärtspfeil], um zum nächsten Paket zu kommen. Wiederholen Sie dies, bis Sie ein interessantes Paket gefunden haben. So erfahren Sie etwa, wenn jemand über Ihr WLAN eine bestimmte Webseite aufgerufen hat.



Sniffing-Check: Praktisch jede Fritzbox schneidet auf Wunsch alle übertragenen Datenpakete mit. Sie starten den Mitschnitt über die versteckte Seite **http://fritz.box/html/capture.html** (Bild D)

WinBooks 2.0

WLAN schützen

Im Folgenden finden Sie die wichtigsten Sicherheits-Tipps, um Ihr WLAN zu schützen und um Eindringlinge auszusperren. Falls Sie einen Fremdsurfer entdeckt haben, ändern Sie unbedingt alle Passwörter und wechseln Sie zum Protokoll WPA2.

Router-Passwort ändern

Ein Passwort für die Konfigurationsoberfläche Ihres WLAN-Routers verhindert, dass jemand, der in Ihr WLAN eingedrungen ist, die Einstellungen heimlich verändert.

Viele aktuelle Router, die von Providern mit einem neuen DSL-Anschluss verteilt werden, haben bereits ein individuelles Passwort. Meist steht es auf der Unterseite des Geräts. In der Regel reicht dies für Privatpersonen aus und muss nicht geändert werden.

Richtig verschlüsseln

Prüfen Sie, ob Ihr Router das Verschlüsselungsprotokoll WPA2 (Wifi Protected Access) verwendet und ändern Sie die Einstellung gegebenenfalls in WPA2. Anders als WEP (Wireless Equivalent Privacy) lässt sich dieses Protokoll nicht durch Belauschen der übertragenen Datenpakete knacken.

Bei der Fritzbox finden sich die Optionen unter „Einstellungen, WLAN, Sicherheit“.

WLAN-Schlüssel

Der WLAN-Schlüssel sollte mindestens zehn Zeichen lang sein und nicht in einem Wörterbuch stehen. Theoretisch darf er sogar bis zu 63 Zeichen lang sein.

Viele Router sind bereits mit einem individuellen WLAN-Schlüssel versehen, der auf der Unterseite steht. Diese können meist weitergenutzt werden.

Funknetzname ändern

Alle WLAN-Router bieten eine Funktion, den Funknetznamen zu ändern. Echte Sicherheit bringt dies aber nicht, weil Hacker-Tools ein WLAN auch bei unterdrücktem Namen aufspüren.

Filtern von MAC-Adressen

Ein Filter für MAC-Adressen soll verhindern, dass sich fremde PCs ohne Ihre Erlaubnis an Ihrem WLAN anmelden. Dieser Schutz lässt sich jedoch umgehen, da ein Angreifer die MAC-Adressen Ihres PCs aus dem Datenstrom ausfiltern und fälschen kann. ■

Andreas Th. Fischer
sonderheft@com-magazin.de

Weitere Infos

- www.schwarz-surfen.de/storerhaftung
  Ausführliche Infos zum Thema Störerhaftung

www.ebooks2.0

Konten-Diebstahl im WLAN

Die Firefox-Erweiterung Firesheep macht das Spionieren zum Kinderspiel. Per Mausklick lassen sich fremde Benutzerkonten kapern. Zwei weitere Firefox-Erweiterungen schützen davor.

In fremden Facebook-Konten stöbern, E-Mails mit falschem Absender verschicken oder vom Konto des Nachbarn aus twittern: All diese Arten von Identitätsdiebstahl ermöglicht die Firefox-Erweiterung Firesheep 0.1.1 (kostenlos, http://codebutler.github.com/firesheep). Die Bedienung ist dabei so einfach, dass selbst Laien in wenigen Sekunden fremde Benutzerkonten kapern und sich mit falschen Identitäten durchs Netz bewegen können.

Dieser Artikel erklärt, wie der Datenklau funktioniert und wie Sie sich davor schützen.

Firesheep 0.1.1: Die Firefox-Erweiterung übernimmt in offenen WLANs per Mausklick fremde Benutzerkonten. Die Spalte links zeigt, welche Konten gerade in der Nähe sind und sich kapern lassen (Bild A)

So funktioniert der Datenklau

Die Firefox-Erweiterung Firesheep fängt die Datenübertragung in offenen WLAN-Netzen ab, wie sie in vielen Cafés und Hotels sowie auf Flughäfen anzutreffen sind. Dazu benötigt Firesheep auch den Netzwerktreiber Winpcap (kostenlos, www.winpcap.org/install/default.htm).

Die Erweiterung zeigt nach dem Start eine Liste der Konten, die Sie per Mausklick übernehmen können (Bild A). Sie belauscht den HTTP-Verkehr über Port 80 und gelangt so an die Login-Daten etwa von Facebook und Twitter. So einfach es mit Firesheep auch sein mag: Das Einloggen in einen fremden Account ist in Deutschland verboten.

Möglich wird dieser Hack durch die Klartextübertragung der Login-Daten, die die entsprechende Webseite mit einem Cookie beantwortet. Dieses Session-Cookie greift sich Firesheep und ermöglicht so die Übernahme des Benutzerkontos. Firesheep hat etliche Abhör-Vorlagen für Cookies von großen sozialen Netzwerken oder Einkaufsportalen. Da sich diese Vorlagen aber leicht ändern lassen, ist prinzipiell jede Webseite betroffen, die Login-Daten unverschlüsselt übermittelt.

Aber was haben Cookies damit zu tun? Und warum werden überhaupt Cookies verwendet?

Auf DVD

Sie finden Blacksheep 1.7 und HTTPS Everywhere 0.9.4 auf in der Rubrik „Internet, Firesheep".

Das Gegenmittel: So warnt die Firefox-Erweiterung Blacksheep 1.7, wenn sie den Versuch einer feindlichen Übernahme entdeckt (Bild B)

www.books24.de

Das hat in erster Linie mit Komfort und Bequemlichkeit zu tun. Wenn Sie eine Webseite aufrufen, dann sendet Ihr Browser per HTTP Daten an einen Webserver. Wenn Sie das nächste Mal die gleiche Webseite aufrufen, erkennt der Server Sie nicht wieder. Mit Cookies dagegen werden Sie einmal nach Benutzername und Passwort gefragt und erhalten das Cookie quasi als Eintrittskarte. Später müssen Sie dann nur die Eintrittskarte vorzeigen, werden aber nicht mehr nach Login und Passwort gefragt. Somit kann sich jeder einloggen, der das Cookie besitzt.

So schützen Sie sich

Es gibt zwei Schutzmechanismen gegen Firesheep: Der eine jagt Firesheep, der andere sorgt dafür, dass Webseiten, wenn möglich, das verschlüsselte Protokoll HTTPS verwenden.

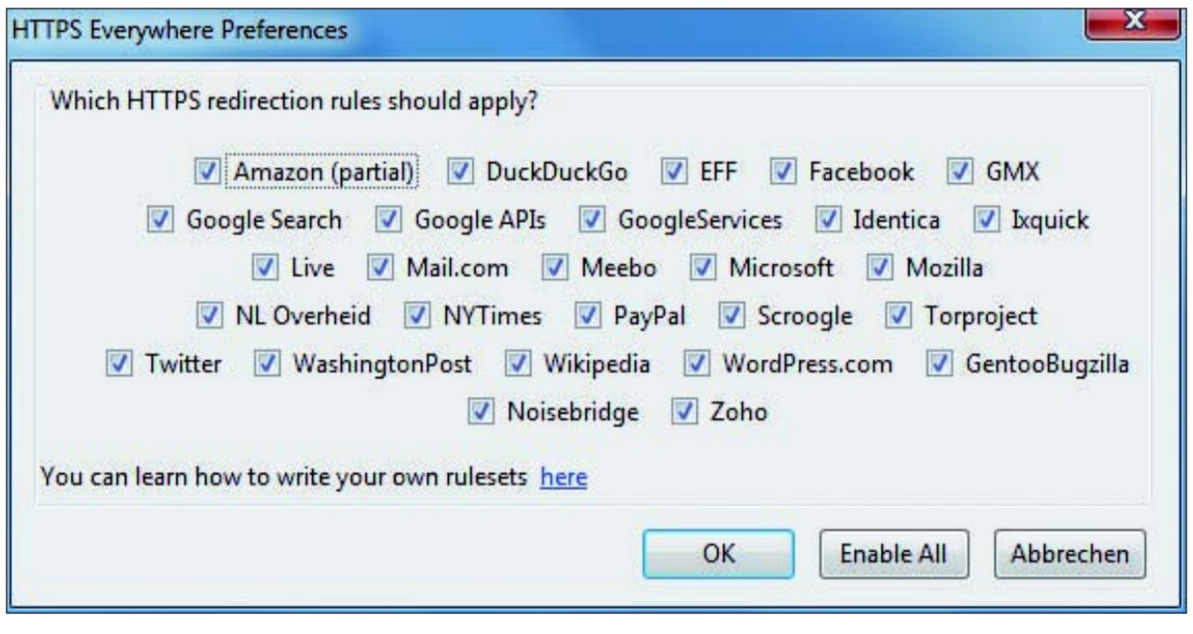
Blacksheep 1.7

In offenen WLAN-Netzen droht seit der Programmierung von Firesheep die Gefahr, dass Cookies und damit Kontoinformationen abgefangen werden.

Die Firefox-Erweiterung Blacksheep 1.7 durchsucht das Netzwerk und schlägt Alarm, wenn sie Firesheep im Einsatz findet (kostenlos, http://research.zscaler.com/2010/11/blacksheep-tool-to-detect-firesheep.html und auf).

Wie Firesheep setzt auch die Erweiterung Blacksheep den Netzwerktreiber Winpcap voraus.

Um Firesheep aufzuspüren, generiert Blacksheep in festgesetzten Intervallen gefälschte Daten, die Logins simulieren. Wenn Firesheep nun diese Daten abgreift und selbst ein Login versucht, dann blendet Blacksheep eine Warnung ein (Bild B).



HTTPS Everywhere 0.9.4: Die Firefox-Erweiterung sorgt dafür, dass Verbindungen zu Seiten wie Facebook und Paypal stets HTTPS-verschlüsselt sind (Bild C)

Noch besser: Blacksheep zeigt sogar die IP-Adresse des Spions an.

Firesheep und Blacksheep lassen sich nicht in der gleichen Firefox-Instanz einsetzen.

HTTPS Everywhere 0.9.4

Es gibt sichere Wege, im Web Daten auszutauschen: Das entsprechende Protokoll heißt HTTPS. Das steht für Hypertext Transfer Protocol Secure. Die Daten, die damit übertragen werden, sind verschlüsselt und nicht ohne Weiteres zu belauschen. Standardmäßig kommt aber meistens das unverschlüsselte Protokoll HTTP zum Einsatz, auch wenn HTTPS möglich wäre. Google mit verschlüsseltem Datentransfer etwa erreichen Sie nur über die Adresse https://encrypted.google.com.

Die Firefox-Erweiterung HTTPS Everywhere 0.9.4 bringt den Browser dazu, falls möglich, automatisch die sichere HTTPS-Verbindung zu wählen (kostenlos, www.eff.org/https-everywhere und auf). Dies funktioniert auf über 30 Webseiten wie Google, GMX und Wikipedia. Facebook, Paypal, Twitter und eine ganze Reihe anderer Dienste lassen sich ebenfalls mit dieser Erweiterung in offenen WLAN-Netzen sicher verwenden (Bild C).

Weitere Webseiten lassen sich manuell hinzufügen. Wie das geht, beschreibt die Seite www.eff.org/https-everywhere/rulesets.

Ob eine Internetverbindung verschlüsselt ist, erkennen Sie an der blauen Markierung im Adressfeld des Browsers (Bild D). ■

Sicher surfen: Wenn Sie mit einer verschlüsselten Verbindung surfen, dann zeigt Firefox dies mit einer blauen Markierung im Adressfeld an (Bild D)

Andreas Dumont
sonderheft@com-magazin.de

Weitere Infos

- www.youtube.com/watch?v=JHKtsuATAh0
  Das Youtube-Video zeigt Firesheep im Einsatz

www.pcbooks2.0

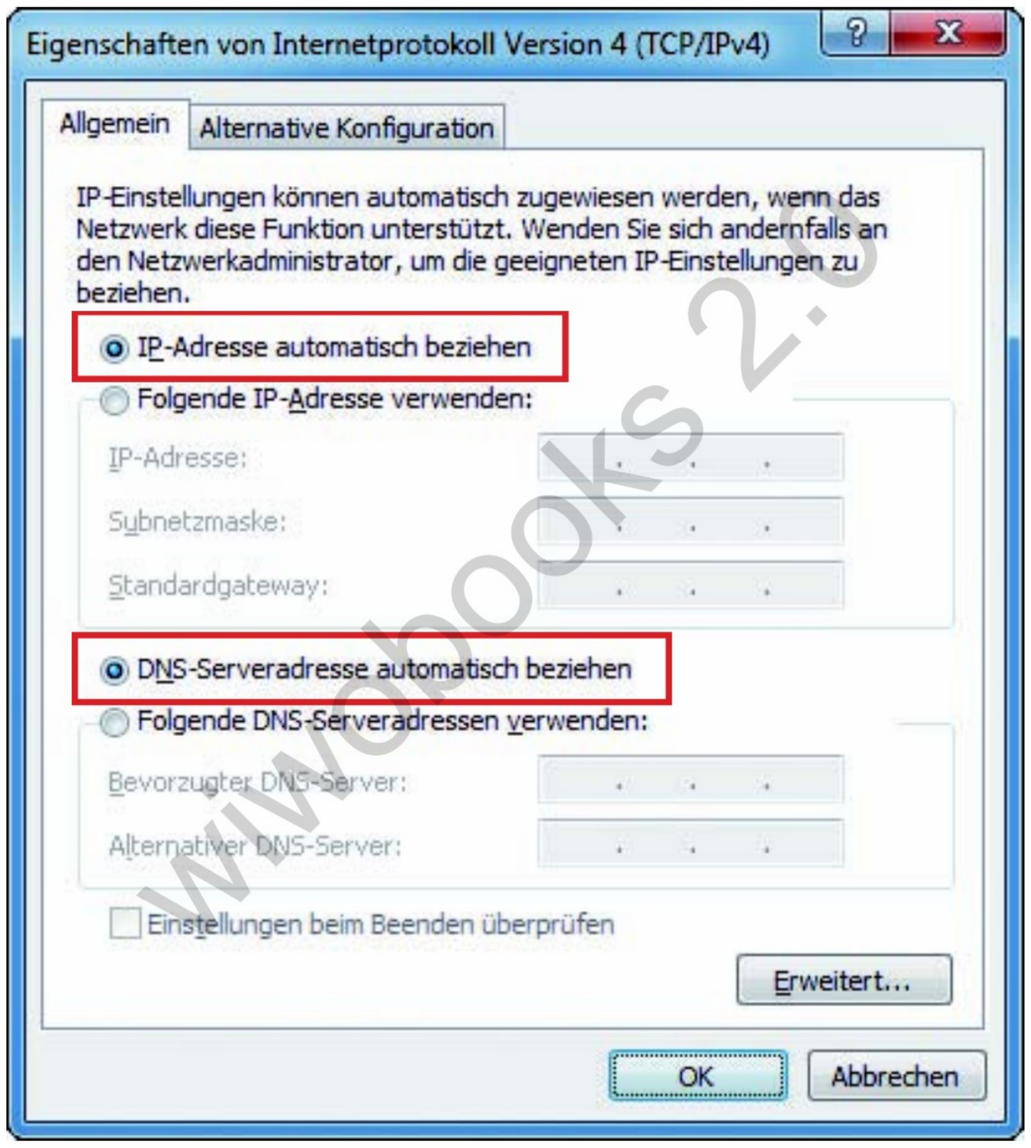
Mit dem Notebook in fremden Netzen

Mit jedem aktuellen Notebook können Sie öffentliche WLANs nutzen und im Internet surfen. Wenn man das Notebook vorher aber nicht richtig einstellt, dann ist das so, als würde man nackt U-Bahn fahren.

Ob am Flughafen, am Bahnhof oder im Hotel: An immer mehr Orten stehen öffentliche Funknetze zur Verfügung, Hotspots genannt. Damit können Sie unterwegs per Notebook oder Netbook das Internet nutzen.

So praktisch öffentliche WLANs auch sind – sie zu nutzen ist ein Risiko: Die meisten Hotspots verwenden nämlich keine Verschlüsselung. So kann jeder andere Nutzer die Datenpakete mitlesen und sehen, welche Webseiten Sie öffnen und was in Ihren E-Mails steht.

Die folgenden Tipps zeigen, wie Sie die Vorteile von Hotspots nutzen – und zwar sicher. So konfigurieren Sie Ihr Windows 7 und die Anwendungen.



IP-Adressen konfigurieren: In öffentlichen Funknetzen werden IP-Adressen meist per DHCP automatisch vergeben. Konfigurieren Sie hierfür den WLAN-Adapter wie in diesem Screenshot (Bild A)

WLAN

Dieser Abschnitt beschreibt, wie Sie eine Funkverbindung zu einem Hotspot herstellen. Öffentliche Funknetze vergeben die IP-Adressen meist per DHCP (Dynamic Host Configuration Protocol). Dabei weist der WLAN-Router dem Notebook automatisch die notwendigen Adressen wie eine IP-Adresse zu.

Auf DVD

Die Software Tor Browser Bundle 1.3.20 finden Sie auf in der Rubrik „Internet, Notebook im Netz“.

Konfiguration

In Windows sind nur wenige Klicks nötig, um ein Notebook mit einem WLAN zu verbinden.

Windows 7 zeigt automatisch alle empfangbaren Funknetze an. Stellen Sie die Verbindung zu einem Funknetz her.

So geht's: Klicken Sie rechts unten in der Taskleiste im System-Tray auf das WLAN-Symbol. Sie erkennen das Symbol an den fünf senkrechten Balken. Ein kleines Fenster öffnet sich, das alle WLANs in der Umgebung anzeigt. Markieren Sie das Funknetz, zu dem Sie eine Verbindung aufbauen wollen. Klicken Sie auf „Verbinden“.

Wenn das WLAN eine Verschlüsselung nutzt, erscheint das Fenster „Geben Sie einen Netzwerksicherheitsschlüssel ein“. Geben Sie den Netzwerkschlüssel ein, den Sie vom Hotspot-Betreiber erhalten haben, und bestätigen Sie mit „OK“.

Windows stellt nun automatisch eine Verbindung zu dem Funknetz her, das Sie ausgewählt haben. In der Regel sind dazu keine weiteren Einstellungen notwendig. Wenn Sie vom

Kompakt

- *Aktuelle Notebooks sind mit WLAN ausgestattet. Damit lassen sich öffentliche Funknetze nutzen.*
- *Die Tipps zeigen, wie Sie Ihren Rechner in einem öffentlichen WLAN vor fremden Blicken schützen.*

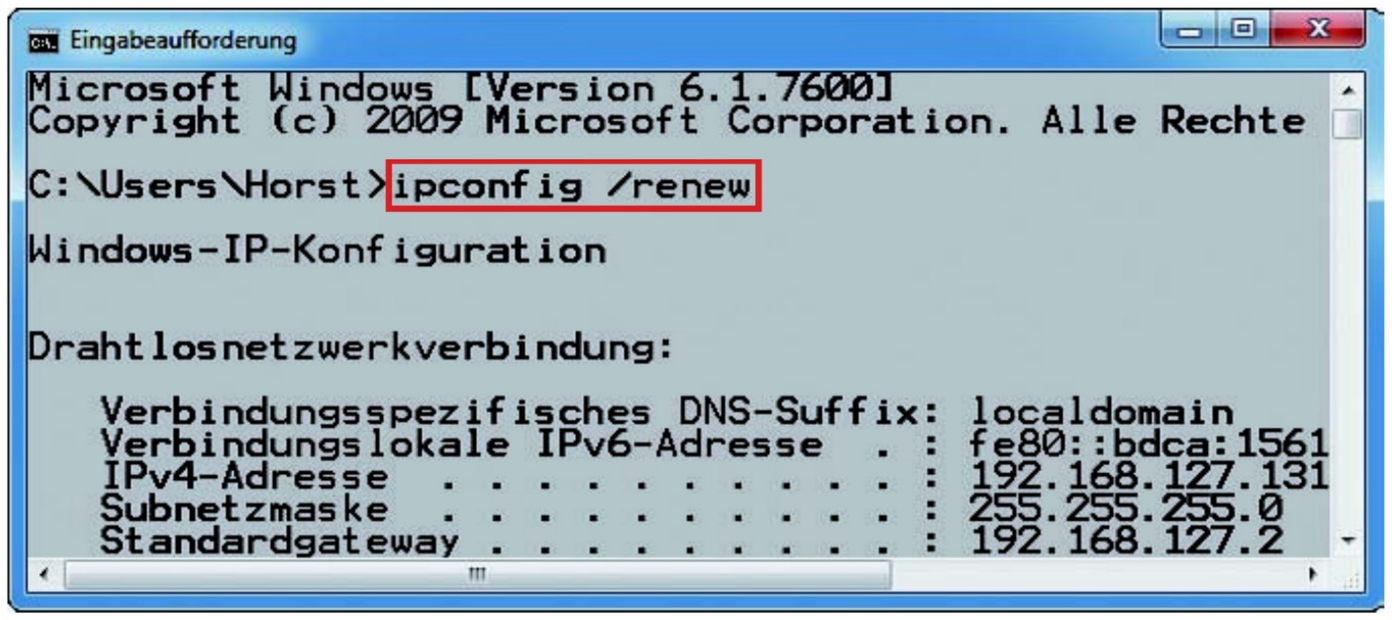
www.obooks 2.0

Inhalt

Notebook in fremden Netzen

- **WLAN**
  - Konfiguration S. 54
  - IP-Adressen S. 55
  - DHCP-Lease S. 56
- **Netzwerkstandort**
  - Konfiguration S. 56
  - Freigaben S. 56
  - Administrative Freigaben S. 56
- **Bluetooth**
  - Schalter und Tastenkombination S. 57
  - Geräte-Manager S. 57
- **MAC-Adressen**
  - Adresse ermitteln S. 58
  - Adressfilter einrichten S. 58
- **Verschlüsselung**
  - Sicher surfen S. 58

So geht's: Tor Browser Bundle 1.3.20 S. 55



Neue IP-Adressen anfordern: Bei Verbindungsproblemen im WLAN-Hotspot erhalten Sie mit diesem Kommandozeilenbefehl automatisch neue IP-Adressen zugewiesen (Bild B)

IP-Adressen

Die meisten öffentlichen WLANs vergeben die IP-Adressen automatisch.

Nur wenn die IP-Adressen richtig konfiguriert sind, kommt eine Verbindung zwischen Ihrem Net- oder Notebook und dem Internet zustande. Die meisten WLANs nutzen das Dynamic Host Configuration Protocol DHCP. Damit konfiguriert der Router im Funknetz automatisch die notwendigen IP-Adressen Ihres Rechners.

So geht's: Wählen Sie in der Systemsteuerung „Netzwerk und Internet, Netzwerk- und Freigabecenter". Klicken Sie links auf „Adaptereinstellungen ändern". Klicken Sie mit der rechten Maustaste auf den Eintrag für den WLAN-Adapter und wählen Sie „Eigenschaften". Das Fenster „Eigenschaften für Drahtlosnetzwerk" öffnet sich. Markieren Sie unter „Diese Verbindung (…)" den Eintrag „Internetprotokoll Version 4 (TCP/IPv4)" und klicken Sie auf die Schaltfläche „Eigenschaften".

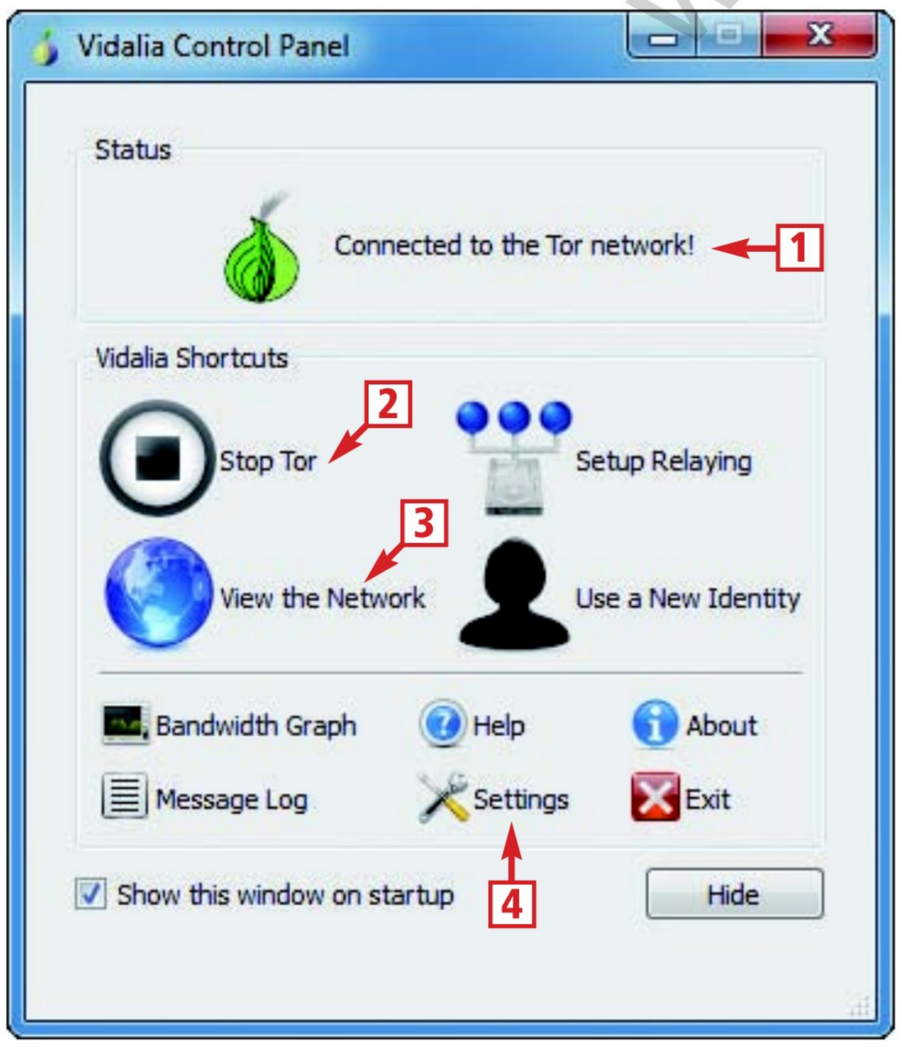
In der Regel vergeben öffentliche Funknetze die IP-Adressen automatisch über DHCP. In diesem Fall markieren Sie auf der Registerkarte „Allgemein" die beiden Einstellungen „IP-Adresse automatisch beziehen" und „DNS-Serveradresse automatisch beziehen" (Bild A).

Wenn Sie vom Betreiber des WLAN-Hotspots IP-Adressen erhalten haben, geben Sie diese im Dialogfenster ein. Markieren Sie „Folgende IP-Adresse verwenden" und „Folgende DNS-Serveradressen verwenden". Geben Sie die IP-Adressen ein und klicken Sie auf „OK". ▶

WLAN-Betreiber eine IP-Adresse erhalten oder in den Netzwerkeinstellungen manuell eine Adresse vergeben haben, dann konfigurieren Sie die IP-Adressen wie im folgenden Abschnitt beschrieben.

So geht's: Tor Browser Bundle 1.3.20

Das Tor Browser Bundle 1.3.20 basiert auf Firefox (kostenlos, www.torproject.org und auf). Es leitet Ihre Anfragen an Webseiten über mehrere anonyme Server. Dabei verschlüsselt es die Anfragen und schützt sie so vor fremden Blicken im öffentlichen WLAN.



1 Status
Wenn eine grüne Zwiebel und der Text „Connected (…)" angezeigt wird, surfen Sie anonym und sicher.

2 Stop Tor
Beendet die Verbindung zum Tor-Netzwerk. Danach surfen Sie nicht mehr sicher.

3 View the Network
Zeigt anhand einer Weltkarte, über welche Server Ihre Anfragen umgeleitet werden.

4 Settings
Dieses Symbol öffnet ein weiteres Fenster mit Profi-Einstellungen.

www.wobooks.2.0

DHCP-Lease

Bei Verbindungsproblemen im Funknetz fordern Sie einfach neue IP-Adressen an.

Der DHCP-Server vergibt die IP-Adressen an die Rechner jeweils für eine bestimmte Zeit. Manchmal kommt es aber zu Verbindungsproblemen – und mit den zugewiesenen Adressen lässt sich keine Verbindung aufbauen. Fordern Sie in diesem Fall einfach neue IP-Adressen an.

So geht's: Öffnen Sie die Kommandozeile mit [Windows R] und `cmd`. Geben Sie auf der Kommandozeile den Befehl `ipconfig·/renew` ein und bestätigen Sie mit der Eingabetaste (Bild B). Windows fordert daraufhin automatisch vom DHCP-Server im Funknetz neue IP-Adressen an.

Netzwerkstandort

Schützen Sie Ihren Rechner vor Angreifern aus dem Netzwerk: Dazu konfigurieren Sie den Rechner für ein öffentliches Netzwerk und beenden Sie Freigaben.

Konfiguration

Wählen Sie in öffentlichen Netzen stets den Netzwerkstandort „Öffentliches Netzwerk".

Windows 7 nutzt erstmals sogenannte Netzwerkstandorte. Anhand des gewählten Netzwerkstandorts konfiguriert Windows dann das Netzwerk und legt zum Beispiel fest, ob Ihr Rechner im Netzwerk sichtbar ist und ob Dateien freigegeben werden. Dabei passt Windows auch gleich die Einstellungen der integrierten Firewall an.

Netzwerkstandort: Wenn Sie den Standort „Öffentliches Netzwerk" auswählen, ist Ihr Notebook für andere Rechner im Netzwerk unsichtbar (Bild C)

Bei der ersten Verbindung mit einem neuen Netzwerk erscheint ein Fenster zur Auswahl des Netzwerkstandorts (Bild C). In öffentlichen Funknetzen sollten Sie stets „Öffentliches Netzwerk" wählen. Damit riegelt Windows Ihren Rechner gegenüber anderen Rechnern und Geräten im Netzwerk ab.

Dabei sind die Netzwerkerkennung sowie die Freigabe von Dateien und Druckern abgeschaltet. Die Windows-Firewall blockiert unbekannte eingehende Datenpakete. Sie verwirft auch Datenpakete zur Netzwerkerkennung.

Der Standort des Netzwerks lässt sich übrigens auch nachträglich ändern. Wählen Sie dazu in der Systemsteuerung „Netzwerk und Internet, Netzwerk- und Freigabecenter". Klicken Sie unter „Aktive Netzwerke anzeigen" auf die Bezeichnung des aktuellen Netzwerkstandorts. Es erscheint das Fenster „Netzwerkadresse festlegen", in dem Sie für das aktuelle Netzwerk einen neuen Standort bestimmen.

Freigaben

Mit der Freigabeübersicht in Windows 7 haben Sie alle freigegebenen Dateien im Blick.

Wenn man häufig Ordner im Netzwerk freigibt, dann kann es schon einmal vorkommen, dass man nicht mehr weiß, was man so alles freigegeben hat. In diesem Fall hilft die Freigabeübersicht.

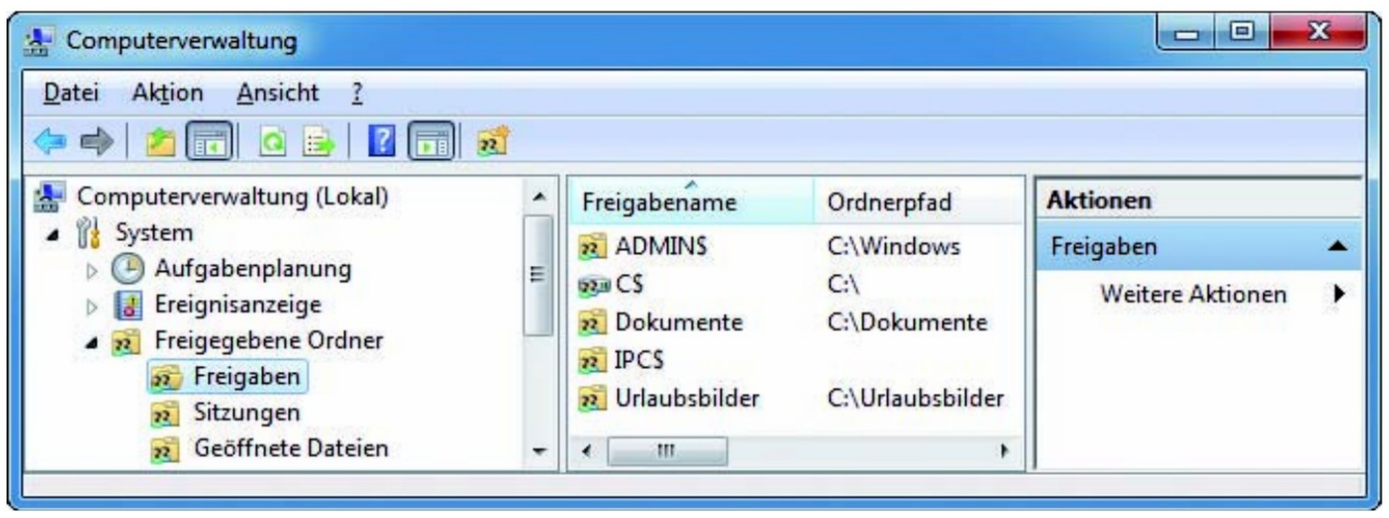
So geht's: Wählen Sie „Start", klicken Sie mit der rechten Maustaste auf „Computer" und wählen Sie „Verwalten". Es öffnet sich das neue Fenster „Computerverwaltung". Markieren Sie in der linken Baumstruktur den Eintrag „Freigegebene Ordner, Freigaben". Im mittleren Fensterbereich erhalten Sie eine Übersicht über alle Freigaben auf dem Rechner (Bild D).

Wenn Sie eine Freigabe entfernen möchten, klicken Sie mit der rechten Maustaste auf den Eintrag. Wählen Sie im Kontextmenü „Freigabe aufheben" und bestätigen Sie mit „Ja".

Administrative Freigaben

Windows legt automatisch versteckte Freigaben an, etwa für das Laufwerk „C:".

Windows 7 legt für Verwaltungszwecke auf dem Rechner automatisch mehrere versteckte Freigaben an, zum Beispiel „C$" für das Laufwerk „C:". Diese Freigaben benötigen Sie aber nicht. Aus Si-



Freigaben im Überblick: Windows 7 zeigt in der „Computerverwaltung" an, welche Ordner und Dateien auf Ihrem Rechner freigegeben sind (Bild D)

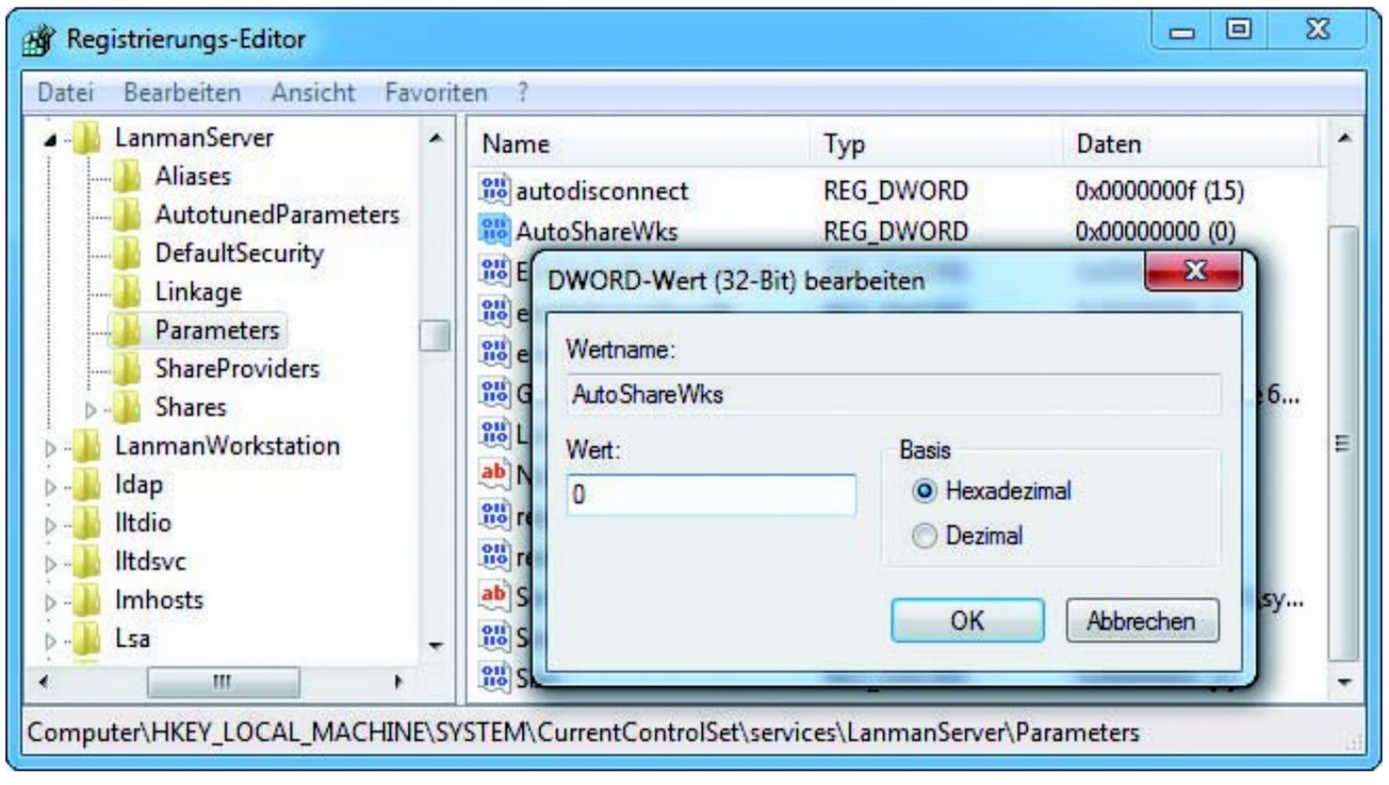
www.books 2.0

cherheitsgründen sollten Sie diese deaktivieren.

Freigaben, deren Freigabename mit einem Dollarzeichen „$“ endet, sind unsichtbar. Das bedeutet, dass diese Freigaben nicht in der Netzwerkübersicht anderer Rechner erscheinen. Diese Freigaben sind aber dennoch ein Sicherheitsrisiko: Denn durch Eingeben der Adresse im Windows-Explorer haben andere Nutzer über das Netzwerk trotzdem Zugriff darauf.

So geht's: Die administrativen Freigaben lassen sich zwar wie im vorherigen Abschnitt beschrieben abschalten – allerdings nur temporär: Windows legt sie beim nächsten Start erneut an.

Ein Registry-Hack sorgt dafür, dass die versteckten Freigaben für Verwaltungszwecke dauerhaft deaktiviert werden. Öffnen Sie den Registrierungs-Editor mit [Windows R] und `regedit`. Markieren Sie den Schlüssel „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters“. Erstellen Sie mit „Bearbeiten, Neu, DWORD-Wert (…)“ den Parameter `AutoShareWks`. Klicken Sie doppelt auf den Eintrag und geben Sie als Wert `0` ein (Bild E).



Administrative Freigaben abschalten: Windows legt standardmäßig versteckte Freigaben an. Das ist unsicher. Diese Registry-Manipulation entfernt die versteckten Freigaben (Bild E)

Bluetooth

Je mehr Möglichkeiten Sie Angreifern geben, auf Ihr System zuzugreifen, desto größer ist die Gefahr, dass das jemand ausnutzt. Deshalb sollten Sie die Bluetooth-Funktion abschalten. Sie brauchen Bluetooth nicht, um über WLAN zu surfen.

Schalter und Tastenkombination

Viele Geräte haben einen Schalter, der Bluetooth und WLAN gleichzeitig abschaltet.

Die meisten Net- und Notebooks haben am Gehäuse einen Schalter, mit dem Sie die Bluetooth-Funktion abschalten können. Statt eines Schalters kommt in vielen Fällen auch eine spezielle Tastenkombination der Form [Fn X] zum Einsatz.

So geht's: Im Handbuch Ihres Netbooks oder Notebooks können Sie nachlesen, welcher Schalter am Gehäuse beziehungsweise welche Tastenkombination die Bluetooth-Funktion ausschaltet.

Wenn Ihr Gerät nur einen Schalter oder eine Tastenkombination unterstützt, die WLAN und Bluetooth jeweils gleichzeitig aktiviert, lesen Sie im folgenden Abschnitt, wie Sie nur Bluetooth abschalten.

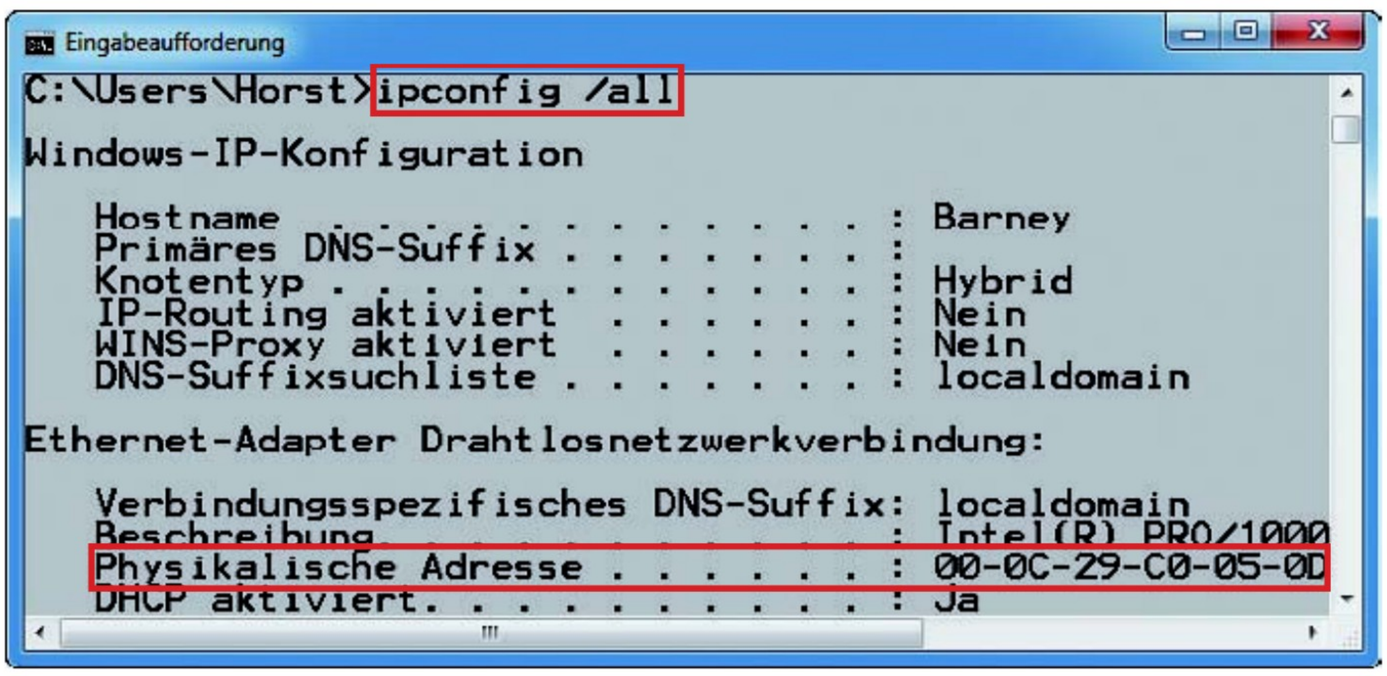
Geräte-Manager

Falls sich Bluetooth nicht unabhängig von WLAN deaktivieren lässt, erledigen Sie das im Geräte-Manager.

Wenn Sie Bluetooth nicht benötigen, schalten Sie diese Funktion ab. Das bietet mehr Sicherheit.

So geht's: Öffnen Sie den Geräte-Manager von Windows. Drücken Sie dazu [Windows Pause] und klicken Sie im linken Fensterbereich auf „Geräte-Manager“. Klicken Sie unter „Bluetooth-Funkgeräte“ mit der rechten Maustaste auf den Bluetooth-Adapter. Wählen Sie im Kontextmenü „Deaktivieren“ und bestätigen Sie mit „Ja“.

Wenn Sie Bluetooth später einmal benutzen möchten, aktivieren Sie es wieder im Geräte-Manager: Klicken Sie mit der rechten Maustaste darauf und wählen Sie „Aktivieren“.

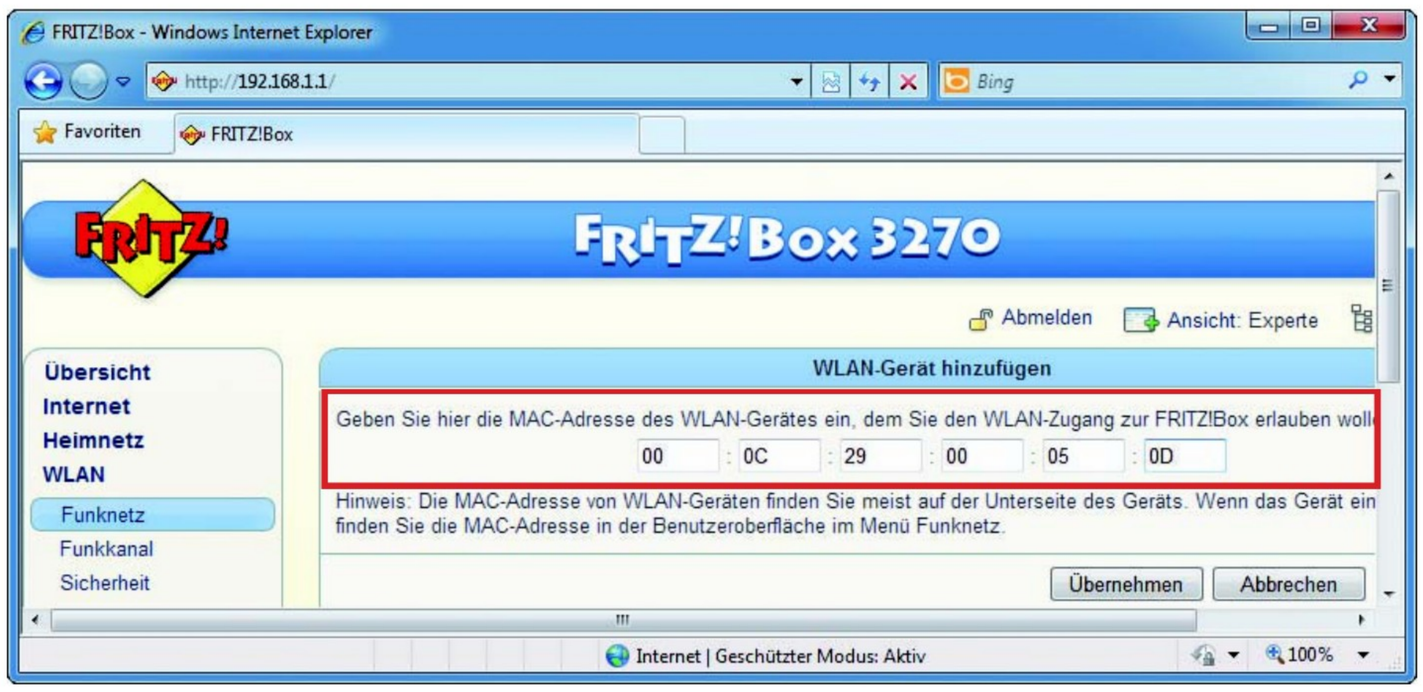


MAC-Adresse: Die eindeutige Adresse Ihres WLAN-Adapters zeigt dieser Kommandozeilenbefehl (Bild F)

MAC-Adressen

Die MAC-Adresse (Media Access Control) ist eine Adresse, die einen Netzwerkadapter eindeutig identifiziert. ▶

winwobooks 2.0



MAC-Adressfilter in der Fritzbox: In diesem Dialogfenster teilen Sie die MAC-Adresse Ihres Notebooks der Fritzbox eines Freundes mit, um von seinem Funknetz surfen zu können (Bild G)

Viele Funknetze bringen eine zusätzliche Zugangskontrolle mit: den MAC-Adressfilter.

Adresse ermitteln

Die MAC-Adresse des WLAN-Adapters in Ihrem Notebook ermittelt ein Kommandozeilenbefehl.

Viele Funknetze nutzen einen MAC-Adressfilter zur Zugangskontrolle. In diesem Fall müssen Sie dem Betreiber des Funknetzes die MAC-Adresse Ihres Net- oder Notebooks mitteilen. Ermitteln Sie die Adresse auf Ihrem Rechner.

So geht's: Zuerst öffnen Sie die Kommandozeile mit der Tastenkombination [Windows R] und `cmd`. Geben Sie auf der Kommandozeile den Befehl `ipconfig·/all` ein und bestätigen Sie mit der Eingabetaste.

Sie erhalten zu jedem Netzwerkadapter im Net- oder Notebook umfangreiche Informationen. Unter „Physikalische Adresse" finden Sie jeweils die MAC-Adresse. Dabei handelt es sich um eine Hexadezimaladresse der Form „00-0C-29-C0-05-0D" (Bild F).

Adressfilter einrichten

Wenn Sie die Fritzbox eines Bekannten mit Ihrer MAC-Adresse füttern, können Sie sein Funknetz nutzen.

Die Fritzbox hat ebenfalls einen MAC-Adressfilter, mit dem sich der Zugang zum WLAN zusätzlich zur Verschlüsselung sichern lässt. Erweitern Sie in der Fritzbox einfach die Liste der erlaubten MAC-Adressen um die Adresse Ihres Net- oder Notebooks. Dann können Sie sich mit Ihrem Rechner zum Beispiel in das Funknetz eines Bekannten einklinken.

So geht's: Öffnen Sie zunächst die Konfigurationsoberfläche der Fritzbox auf einem Rechner im Netzwerk des Bekannten.

Wechseln Sie in der Konfiguration der Fritzbox in der linken Navigation auf „WLAN, Funknetz". Klicken Sie unter „Bekannte WLAN-Geräte" auf die Schaltfläche „WLAN-Gerät hinzufügen". Jetzt geben Sie im nächsten Dialogfenster die MAC-Adresse Ihres Net- oder Notebooks ein und bestätigen Sie mit „Übernehmen" (Bild G).

Sicher surfen mit Tor: Wenn Sie diesen grünen Hinweis sehen, dann surfen Sie anonym (Bild H)

Verschlüsselung

Die meisten öffentlichen Funknetze verschlüsseln die übertragenen Datenpakete nicht. Das vereinfacht zwar den Zugang zum WLAN – ist aber ein Sicherheitsrisiko.

Sicher surfen

Surfen Sie nur verschlüsselt, damit niemand Ihren Datenverkehr mitschneiden kann.

Die Software Tor Browser Bundle 1.3.20 (kostenlos, www.torproject.org und auf) enthält einen Firefox-Browser, mit dem man sicher surfen kann.

Er verschlüsselt den Datenverkehr von Ihrem Net- oder Notebook zum Tor-Server sowie zwischen den Servern. Zudem surfen Sie mit Tor anonym und hinterlassen so keine Spuren.

So geht's: Das Tor Browser Bundle ist ein Sofort-Tool. Das bedeutet, dass das Bundle auf Ihrem Rechner keine Installation erfordert.

Entpacken Sie die Datei „tor-browser-1.3.20_en-US.exe" mit einem Doppelklick auf Ihrem Rechner. Speichern Sie die entpackten Dateien im neuen Verzeichnis `C:\Tor`. Navigieren Sie dann im Windows-Explorer in das neue Verzeichnis und starten Sie Tor mit einem Doppelklick auf die Datei „Start Tor Browser.exe".

Das neue Fenster „Vidalia Control Panel" öffnet sich. Dabei handelt es sich um das Tool, das dafür sorgt, dass Ihre Daten verschlüsselt und anonym übertragen werden.

Wenn eine Verbindung hergestellt ist, öffnet sich ein portabler Firefox. Damit surfen Sie sicher und anonym. Das erkennen Sie daran, dass im Firefox-Browser rechts unten in Grün der Hinweis „Tor Enabled" steht (Bild H). ■

Konstantin Pfliegl
sonderheft@com-magazin.de

Weitere Infos

- http://support.microsoft.com/kb/967445/de
  Anleitung zur WLAN-Einrichtung in Windows 7

Wlwobooks2.0

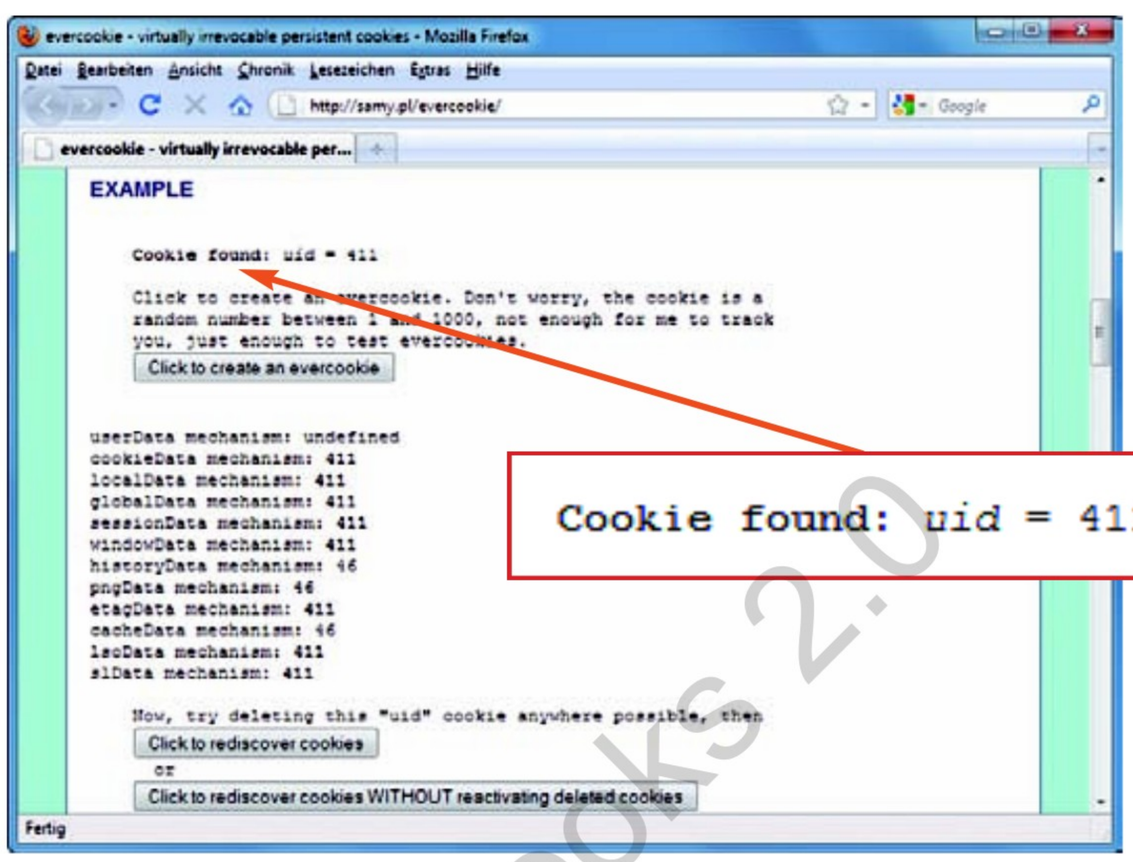
Zombie-Cookies

Eine neue Art von Cookies ist einfach nicht totzukriegen. Wenn diese Cookies erst einmal auf Ihrem PC sind, dann bleiben sie für immer dort.

Samy Kamkar hat ein Cookie erfunden, das Sie garantiert nie wieder loswerden. Das sogenannte Evercookie widersteht jedem Löschversuch.

Bislang wird das Cookie noch nicht von Websites eingesetzt. Kamkar demonstriert die Technik lediglich in einem Projekt auf seiner Seite http://samy.pl/evercookie.

Dort können Sie selbst auf Ihrem PC ein harmloses Evercookie platzieren und anschließend versuchen, es wieder zu entfernen. Sie werden es nicht schaffen.



Evercookies: Diese neuartigen Cookies lassen sich nie wieder löschen. Sie könnten jeden PC anhand einer ID identifizieren. Im Beispiel heißt die ID „411“ (Bild A)

Die Evercookies dieses Projekts enthalten lediglich eine ID zwischen 1 und 1000 (Bild A). Theoretisch könnte ein Evercookie aber auch andere Informationen enthalten. Auch zehnstellige IDs wären möglich. Damit wäre dann jeder PC auf der Welt eindeutig identifizierbar.

Privater Modus: Der Browser-Modus zum Schutz der Privatsphäre schützt auch vor Evercookies (Bild B)

So funktionieren Zombie-Cookies

Evercookies, von manchen auch Zombie-Cookies genannt, kombinieren 13 Techniken, um Daten auf dem PC abzulegen. Wenn auch nur eine dieser Techniken alle Löschaktionen überlebt, dann lässt sich damit die Information des Cookies erneut auslesen. Die übrigen Speicherorte werden erneut befüllt. Das Cookie regeneriert sich gewissermaßen selbst.

Es nützt also nichts, im Browser alle Cookies, die Chronik und den Cache zu löschen. Ebenso wenig hilft es, den Browser zu wechseln, da das Cookie über Browser-Grenzen hinweg funktioniert.

Zu den Techniken, die in der Summe das Cookie unverwundbar machen, gehören einige Neuerungen aus HTML5. So erlauben es die Techniken Session Storage, Local Storage und Database Storage, dass eine Website Daten auf Ihrer Festplatte ablegt.

Weitere Techniken sind Local Shared Objects, auch unter dem Namen Flash-Cookies bekannt.

Zudem generieren Evercookies ein PNG-Bild, dessen RGB-Werte die zu speichernde ID sind. Diese PNG-Datei landet im Browser-Cache.

Derzeit ist das Evercookie nur ein Projekt, das zeigt, was möglich ist. Der Antivirenspezialist Kaspersky sagt dazu: lästig, aber nicht gefährlich.

Vermutlich ist es aber nur eine Frage der Zeit, bis sich kommerzielle Webseiten diese Open-Source-Technik zunutze machen, etwa um PCs eindeutig identifizieren zu können.

So schützen Sie sich

Da sich ein Evercookie nicht löschen lässt, können Sie nur verhindern, dass es überhaupt auf Ihren PC gelangt. Dazu genügt es, beim Surfen den privaten Modus einzuschalten (Bild B).

In Firefox wählen Sie „Extras, Privaten Modus starten“. Im Internet Explorer finden Sie den privaten Modus unter „Extras, InPrivate-Browsen“. ■

Weitere Infos

- http://samy.pl/evercookie
  Hier erklärt Samy Kamkar Evercookies (englisch)

www.wobooks 2.0

Der Trojaner Carberp

Der Trojaner Carberp hat das Potenzial, zu einem der gefährlichsten Schädlinge im Internet zu werden: Er ist aggressiv, mächtig und braucht nicht einmal Admin-Rechte.

Der Trojaner Carberp klinkt sich in den Browser ein, manipuliert besuchte Webseiten und klaut Login-Daten.

Diese Fähigkeit haben auch Trojaner wie Gozi und Zeus. Das Besondere an Carberp ist jedoch, dass er nichts macht, was Admin-Rechte benötigt. So umgeht er den Schutz durch die Benutzerkontensteuerung von Windows Vista und 7.

Bislang ist Carberp noch nicht weit verbreitet. Der Antivirenhersteller Trend Micro hat das „Schadenspotenzial" des neuen Trojaners jedoch auf die höchste Stufe gesetzt – zu Recht.

Wie gelangt Carberp auf den PC?

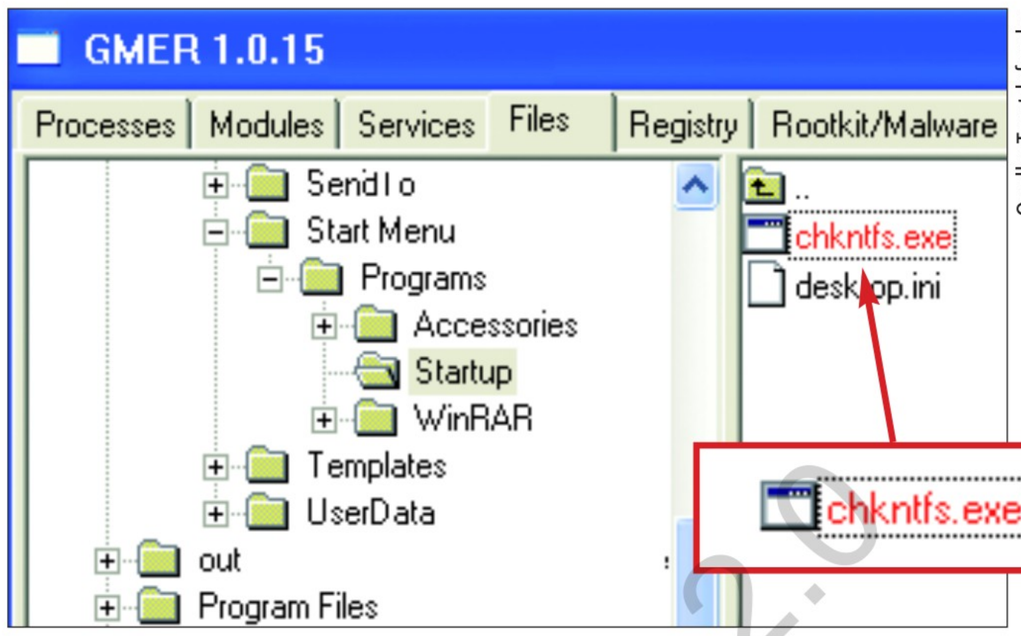
Bislang gefundene Carberp-Varianten schleichen sich über manipulierte Webseiten auf fremden PCs ein. Dabei setzen die Kriminellen Javascripts ein, die Lücken im Browser oder in installierten Plug-ins wie Flash und Java ausnutzen.

Nachdem der Schadcode einen PC erreicht hat, manipuliert Carberp den Windows-Explorer und injiziert Code. Danach erstellt der Virus mehrere Dateien mit unverfänglichen Namen wie „10.tmp" oder „~TM13.tmp".

Außerdem kopiert er sich in das Autostart-Verzeichnis des gerade angemeldeten Benutzers. Bislang bekannt gewordene Namen für diese Dateien sind „chkntfs.exe" und „syscron.exe".

Auf DVD

Tools gegen Carberp finden Sie auf in der Rubrik „Internet, Neuer Trojaner".



Quelle: Trustdefender

Carberp: Die versteckte Datei „chkntfs.exe" im Ordner „Startup" enthält den Trojaner Carberp. Die Datei lässt sich nur mit einem Spezial-Tool wie Gmer 1.0.15 sichtbar machen (Bild A)

Wie versteckt er sich auf dem PC?

Zum Verstecken verwendet Carberp Rootkits-Tricks, so dass der Schädling unter Windows komplett unsichtbar wird. Er manipuliert die Windows-Bibliothek „NTDLL.DLL" und die Komponenten „NtQueryDirectoryFile" sowie „NtResume Thread". Nur spezialisierte Tools wie Gmer 1.0.15 zeigen die verborgenen Dateien an (kostenlos, www.gmer.net) (Bild A).

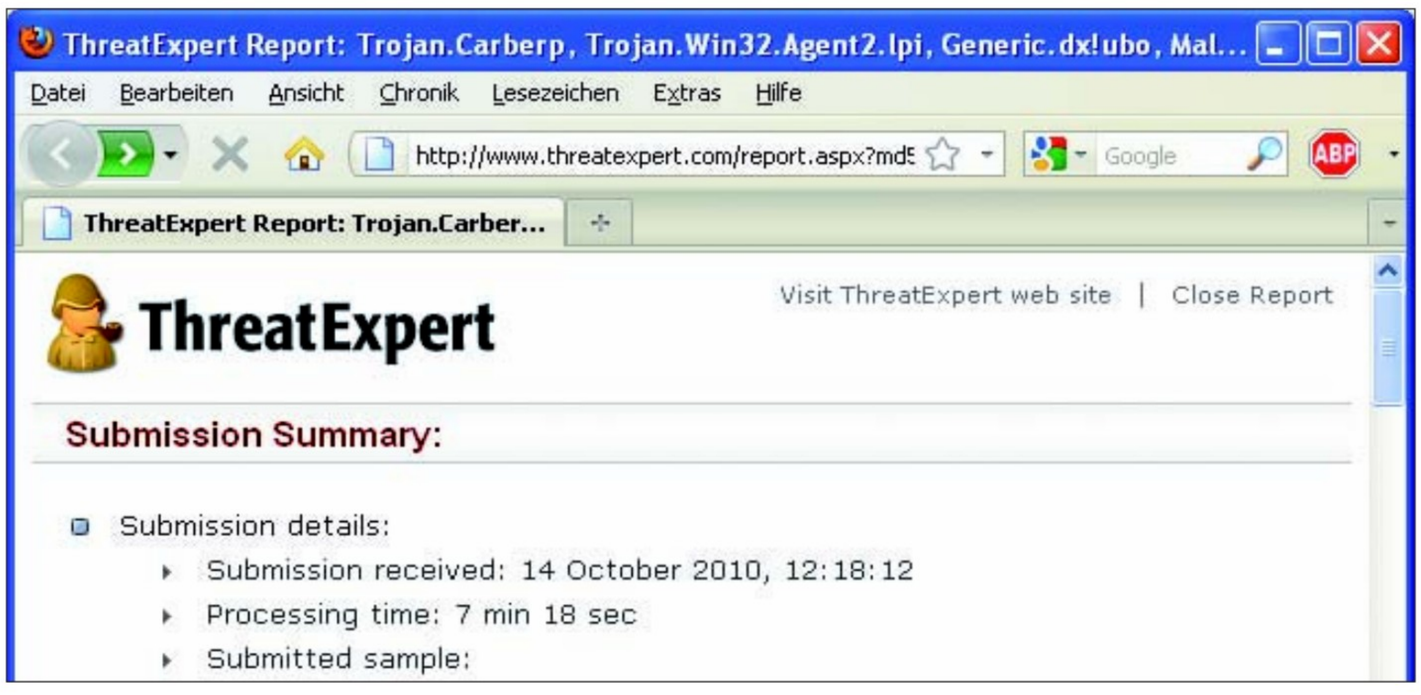
Wie aktualisiert er sich?

Nach der Infektion nimmt Carberp Kontakt mit einem C&C-Server (Command & Control) auf. Bekannt gewordene Server waren in China und der Ukraine registriert.

Zuerst holt sich Carberp eine eindeutige Identifizierungsnummer (ID) vom Kommandoserver. Anschließend erstellt er eine Liste aller aktiven Prozesse auf dem infizierten PC und kopiert sie auf den Server. Zuletzt lädt Carberp noch die Dateien „stopav.plug", „miniav.plug" und „passw.plug" herunter. „stopav.plug" dient zum Deaktivieren des Virenscanners, während „miniav.plug" konkurrierende Trojaner auf dem Rechner entfernt. „passw.plug" erlauscht Passwörter und Logins.

Wie wird Carberp gesteuert?

Die ersten Befehle erhält ein infizierter PC von seinem C&C-Server. Diese



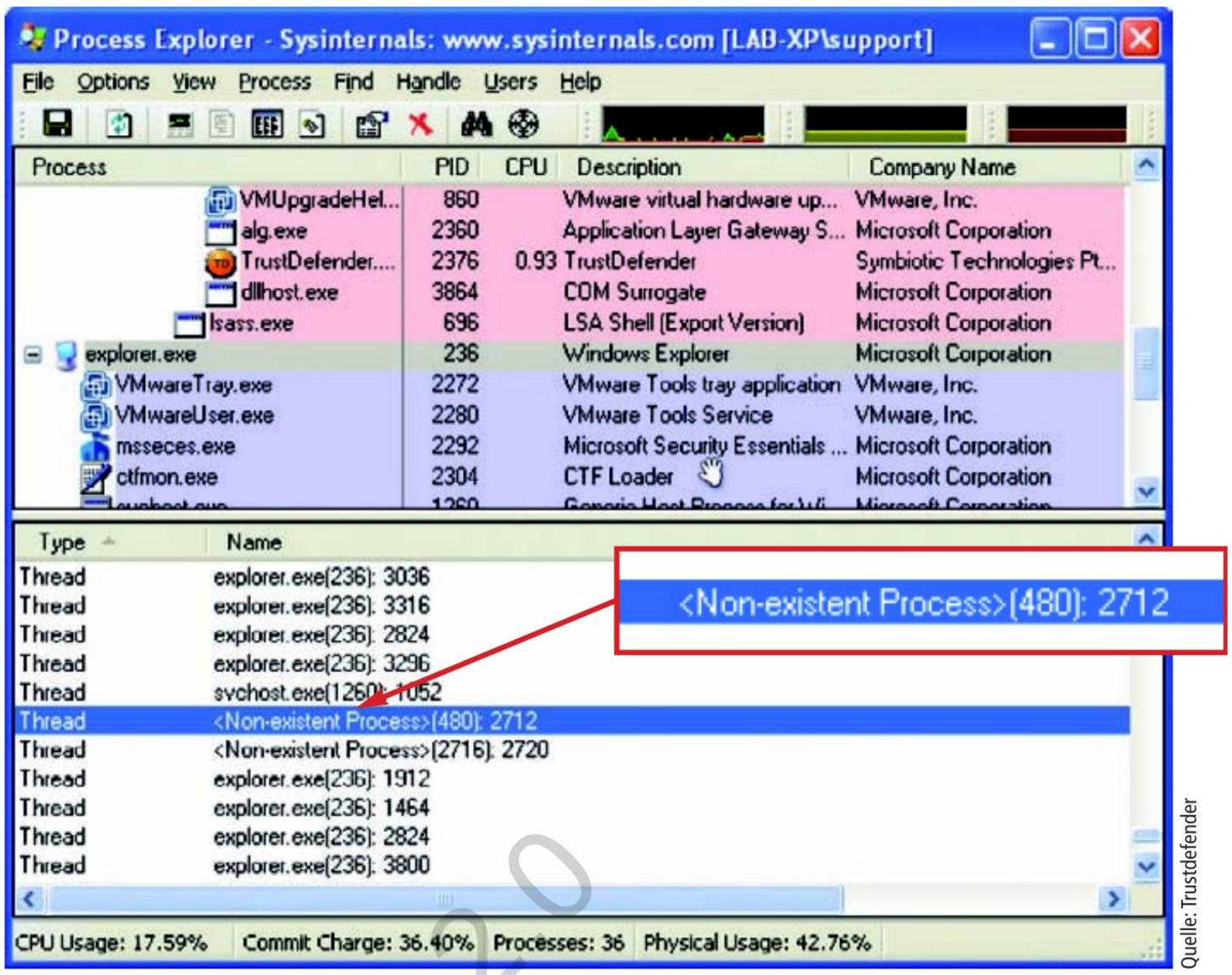
Threatexpert-Analyse: Sicherheitsexperten haben ein Exemplar von Carberp in einer abgeschotteten Sandbox ausgeführt und den Bericht online gestellt (Bild B).

www.wowbooks2.com

Steuerserver werden jedoch meist nach einiger Zeit enttarnt und deaktiviert.

Carberp versucht deswegen, den Port 80 in der Firewall zu öffnen. Welche Firewalls Carberp manipulieren kann, ist nicht bekannt. Es ist jedoch unwahrscheinlich, dass der Schädling auch Zugriff auf Router-Firewalls hat.

Der Sicherheitsspezialist Trustdefender hat Carberp in einer abgeschotteten Sandbox ausgeführt, die der Online-Dienst Threatexpert kostenlos anbietet (www.threatexpert.com) (Bild B). Dabei nahm der Schädling zuerst mit einem C&C-Server in China Kontakt auf. Bereits innerhalb des nur knapp sieben-einhalb Minuten dauernden Testzeitraums erfolgte dann ein Kontaktversuch auf den Port 80 der Sandbox – von einem Computer aus Bosnien aus. Die Bande ist international aktiv.



Quelle: Trustdefender

Process Explorer 14.01: Ein Thread, der zu einem angeblich nicht existierenden Prozess gehört, deutet auf eine Carberp-Infektion hin (Bild C)

Wie belauscht Carberp meinen Browser?

Carberp klinkt sich in die Systembibliothek „WININET.DLL“ ein, die viele zentrale Internetfunktionen von Windows enthält. Über diese DLL erhält der Schädling Zugriff auf den Datenstrom des Browsers. Außerdem greift Carberp auf die Firefox-Bibliothek „NSPR4 .DLL“ zu und erhält so die volle Kontrolle über die von Firefox übermittelten und dargestellten Daten.

Carberp filtert Passwörter und PINs aus und sendet sie mit der URL der besuchten Seite an den C&C-Server.

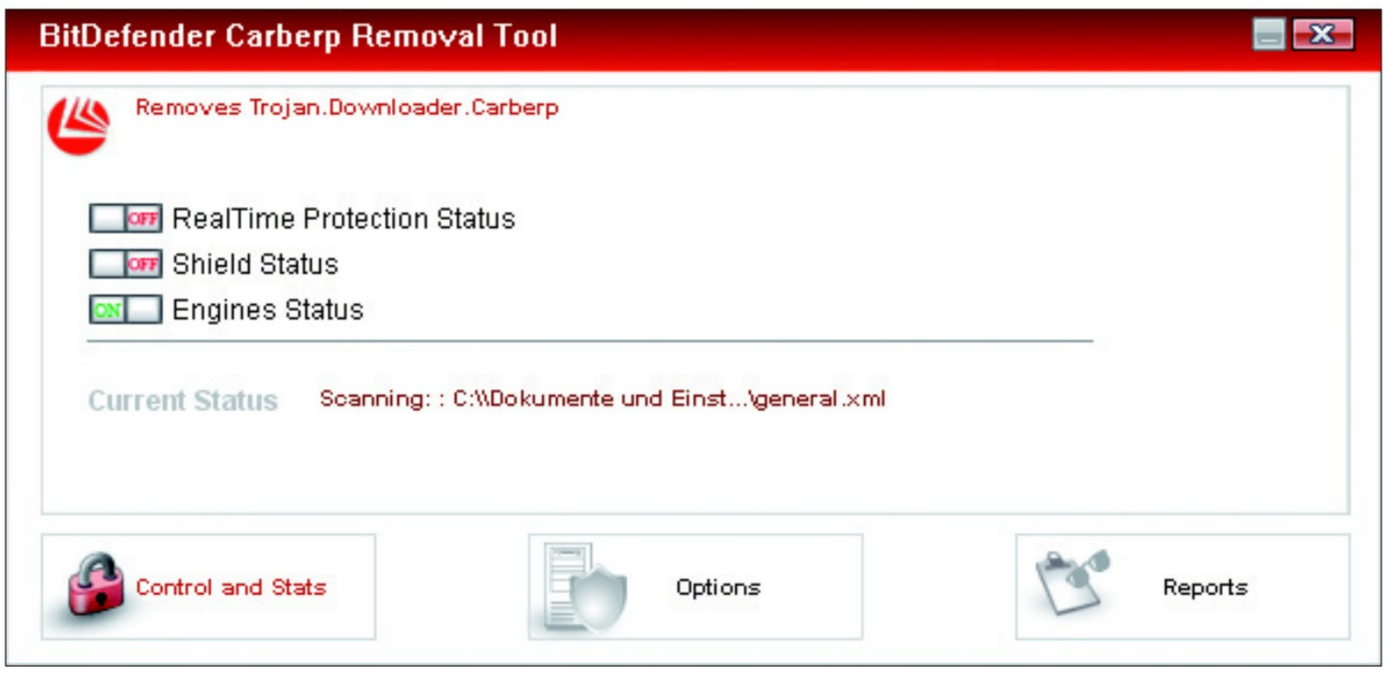
Wie manipuliert Carberp Webseiten, die ich besuche?

Der Trojaner, der durch die Manipulation mehrerer DLLs Zugriff auf den Browser hat, injiziert Javascripts auf bestimmten Webseiten. Bislang sind nur Scripts bekannt, die den Kriminellen beim Klau der Login-Daten helfen.

Wie spüre ich Carberp auf?

Das Tool Process Explorer 14.01 von Microsoft macht eine Carberp-Infektion sichtbar, indem es alle aktiven Prozesse anzeigt (kostenlos, http://technet.microsoft.com/de-de/sysinternals/bb896653.aspx und auf).

Scrollen Sie im oberen Feld von Process Explorer bis zu „explorer.exe“. Wählen Sie „View, Show Lower Pane“ aus, um das Detailfenster einzublenden. Scrollen Sie dann nach unten bis zu den „Thread“-Einträgen. Steht neben einem der „Thread“-Einträge der Hinweis auf einen „<Non-existent Process>“, ist Ihr PC laut Trustdefender mit Carberp infiziert (Bild C). Führen Sie in so einem Fall das Carberp Removal Tool von Bitdefender aus, das bisher aber nur die Variante Carberp.A erkennt und entfernt (kostenlos, www.malwarecity.com/community/index.php?app=downloads&showfile=16 und auf) (Bild D). ■



Carberp Removal Tool: Das kostenlose Werkzeug des Antivirenherstellers Bitdefender entfernt den neuen Trojaner vom PC, allerdings bisher nur die Variante Carberp.A (Bild D)

Andreas Th. Fischer
sonderheft@com-magazin.de

Weitere Infos

- www.trustdefender.com/blog
  Ausführliche Carberp-Analysen (englisch)

www.books2.0

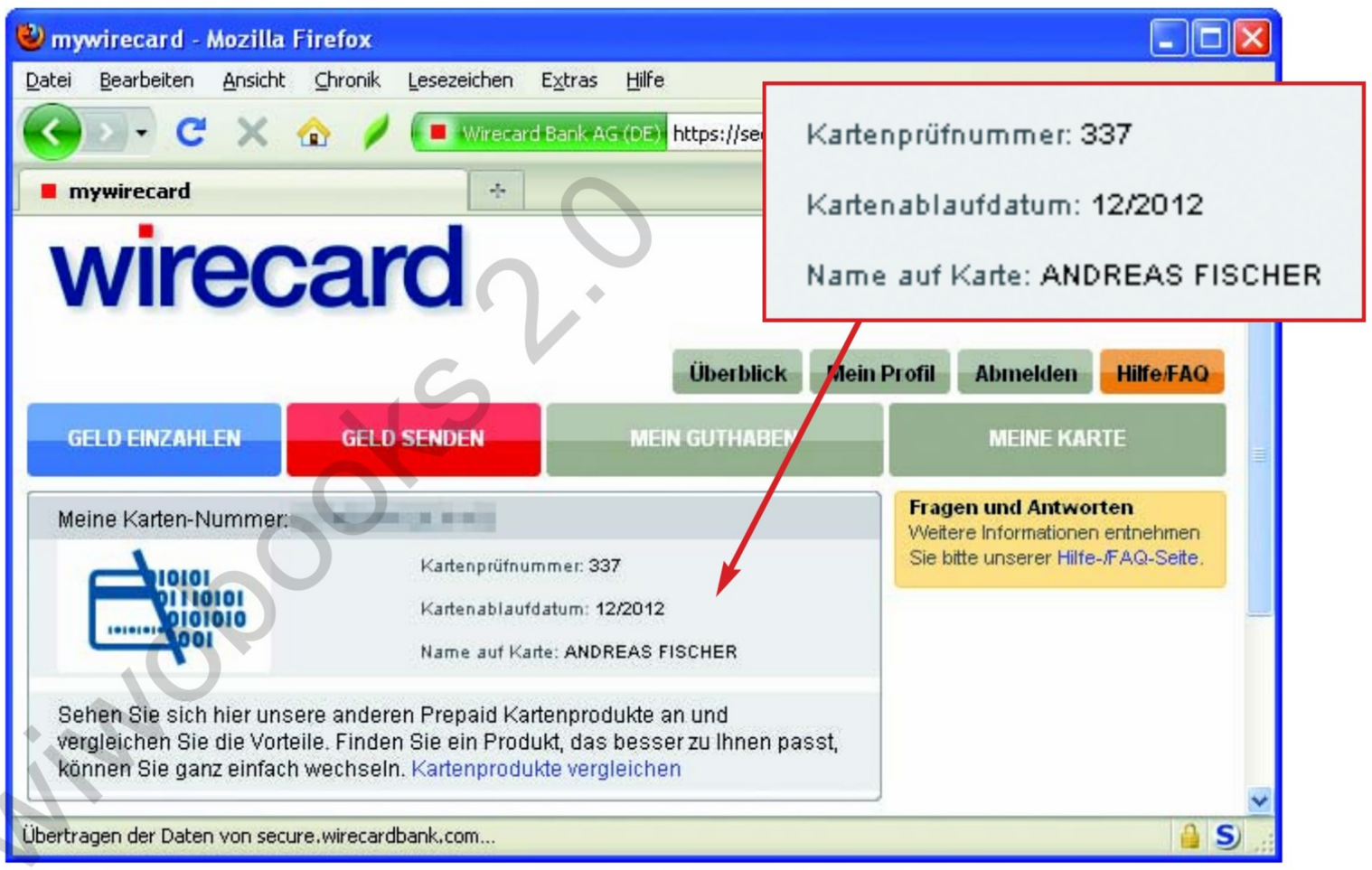
Sicher bezahlen im Internet

Fünf neue Bezahldienste wie Wirecard, Paysafecard und Ukash sollen das Einkaufen im Internet verbessern. Doch wie bequem und sicher sind sie wirklich?

Com! stellt fünf neuartige Bezahlsysteme im Internet vor: So gibt es jetzt virtuelle Kreditkarten, die jeder Online-Shop akzeptiert, der die Bezahlung per Mastercard erlaubt.

Andere Anbieter haben sich auf Prepaid-Systeme spezialisiert, die eine anonyme Bezahlung im Internet ermöglichen. Auch das Bezahlen von Kleinstbeträgen per SMS ist einfach und sicher geworden.

Schon länger verbreitete Systeme wie Paypal oder Click and Buy wurden bereits im Artikel „Bezahlen im Internet“ in com! 10/2009 beschrieben. Sie finden den Artikel als PDF-Datei in der Rubrik „Internet, Bezahlen im Internet“ auf Heft-DVD sowie kostenlos unter www.com-magazin.de/archiv.



Neue Bezahldienste: Die virtuelle Kreditkarte von Wirecard hat die gleichen Daten wie eine echte Kreditkarte, also etwa Kartenprüfnummer und Kartenablaufdatum, existiert aber nur im Browserfenster (Bild A)

1. Wirecard: Virtuelle Kreditkarte

Die Kreditkarte von Wirecard existiert nur virtuell im Internet. Sie bezahlen damit in Online-Shops, die Mastercard akzeptieren.

Um eine virtuelle Mastercard zu erhalten, ist eine Registrierung bei Wirecard notwendig (www.mywirecard.de). Dabei fragt das Unternehmen Daten wie Geburtsdatum, Adresse und Handy-Nummer ab. An Letztere schickt Wirecard dann eine Registrierungs-SMS, die einen Freischalt-Code enthält. Erst nach Eingabe dieses Codes wird der Account aktiviert.

Im nächsten Schritt laden Sie die virtuelle Kreditkarte mit Geld auf. Dies erfolgt über eine herkömmliche Banküberweisung oder über ein Terminal an einer Aufladestation.

Viele Tankstellen bieten diesen Dienst an. Eine Übersicht finden Sie unter https://secure.wirecardbank.com/mywirecard/StationFinder.html. Einzahlungen über eine Aufladestation sind – anders als bei einer Überweisung, die ein paar Tage benötigt – sofort verfügbar.

Sobald das erste Mal Geld auf Ihrem Wirecard-Konto eingegangen ist, wird Ihre virtuelle Kreditkarte freigeschaltet. Sie enthält alle üblichen Daten wie Karteninhaber, Kartennummer, Ablaufdatum und die dreistellige Kartenprüfnummer, die Sie bei einem Einkauf im Internet benötigen.

Besonderheiten: Die virtuelle Kreditkarte ist überall dort einsetzbar, wo Mastercard akzeptiert wird (Bild A). Damit eignet sich dieses System, um etwa in amerikanischen oder englischen Online-Shops einzukaufen.

Kompakt

- *Der Artikel stellt fünf neue, sichere Bezahlsysteme im Internet vor.*
- *Bezahlen Sie mit PIN-Codes, per SMS oder mit einer virtuellen Kreditkarte.*

www.pcpool.de

Inhalt

Sicher bezahlen im Internet

- 1. Wirecard: Virtuelle Kreditkarte S. 62
- 2. Paysafecard: Prepaid-System S. 63
- 3. Ukash: Kombisystem S. 64
- 4. Mbe4: Bezahlen per Handy S. 65
- 5. Iclear: Treuhandverfahren S. 65

Gebühren fallen nur beim Aufladen der Wirecard und beim Einkauf in einer anderen Währung an. Für Einzahlungen per Überweisung berechnet das Unternehmen einen Euro. Bei Einzahlungen an einer Aufladestation zieht Wirecard vier Prozent des eingezahlten Betrags als Gebühr ab, also beispielsweise vier Euro bei einer Einzahlung von 100 Euro. Für einen Einkauf in einer Fremdwährung, etwa in einem amerikanischen Shop, berechnet das Unternehmen eine Gebühr von 1,5 Prozent.

Die Registrierung einer Wirecard ist kostenlos. Gebühren für die Nutzung im Inland fallen keine an.

Die virtuelle Kreditkarte hat einen wichtigen Vorteil: Werden die Kreditkartendaten geklaut, ist der maximale Schaden auf den aktuell eingezahlten Betrag begrenzt.

Paysafecard: In einer Verkaufsstelle von Paysafecard erhalten Sie diese Bons. Den aufgedruckten PIN-Code geben Sie beim Bezahlen in einem Online-Shop an (Bild C)

2. Paysafecard: Prepaid-System

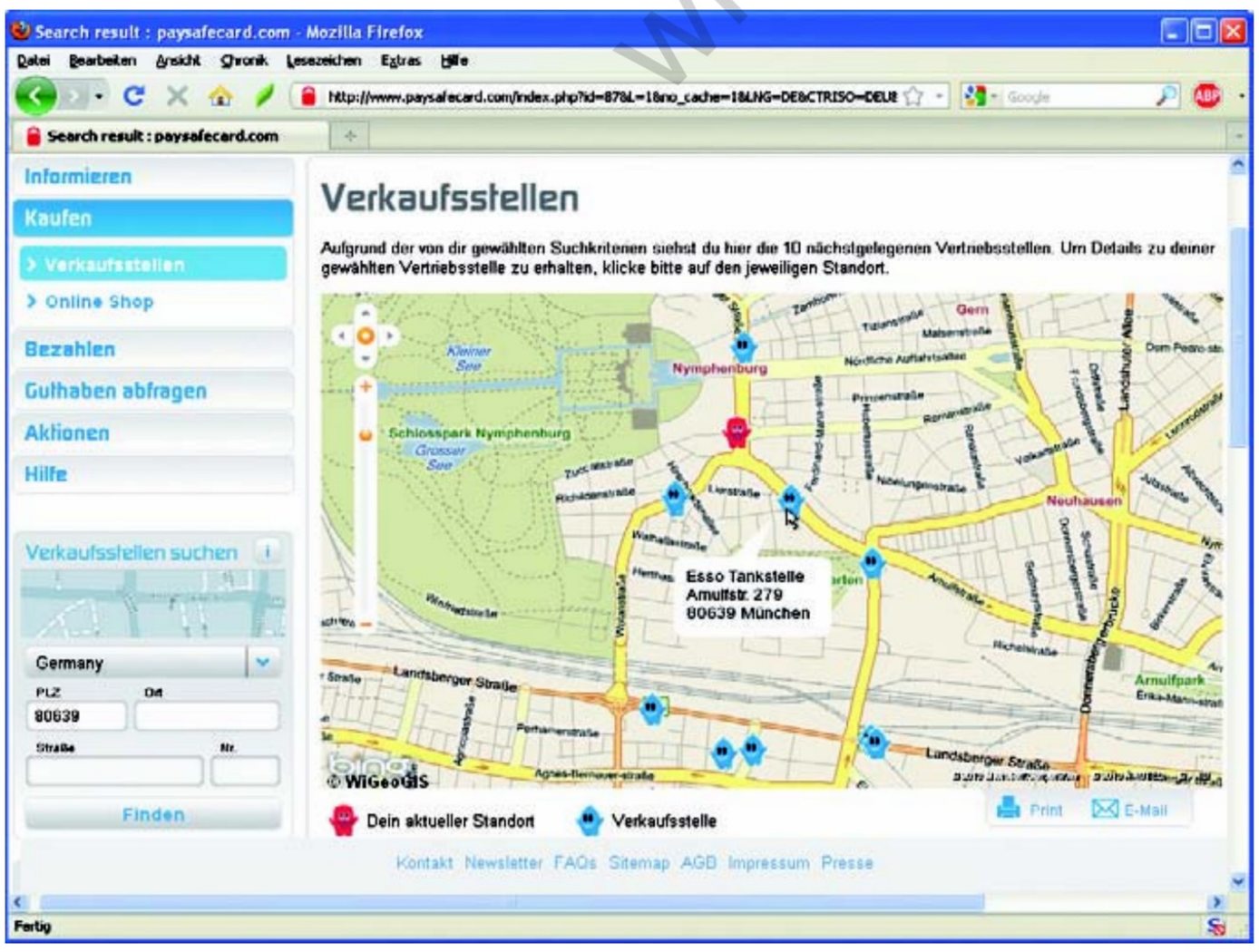
Paysafecard verkauft PIN-Codes an Tankstellen und Kiosken. Diese PIN-Codes lassen sich fast so anonym wie Bargeld einsetzen.

Paysafecard ist ein Prepaid-System, das nach Angaben des Anbieters an weltweit 300.000 Verkaufsstellen erhältlich ist (www.paysafecard.de).

Wo die nächste Verkaufsstelle liegt, erfahren Sie auf der Webseite www.paysafecard.com/de/kaufen/verkaufsstellen (Bild B). An der Kasse erhalten Sie dann einen Bon, der ähnlich wie ein Kassenbeleg aussieht (Bild C).

Auf dem Bon stehen einige allgemeine Hinweise und ein sechzehnstelliger PIN-Code, mit dem Sie in einem Online-Shop einkaufen, der Paysafecard als Zahlungsmittel unterstützt.

Besonderheiten: Derzeit unterstützen etwa 3500 Online-Shops das Paysafecard-System. Große und bekannte ▶



Verkaufsstellen finden: Die Webseite von Paysafecard zeigt auf einer Karte an, wo sich die nächsten zehn Verkaufsstellen befinden (Bild B)

wiwobooks 2.0

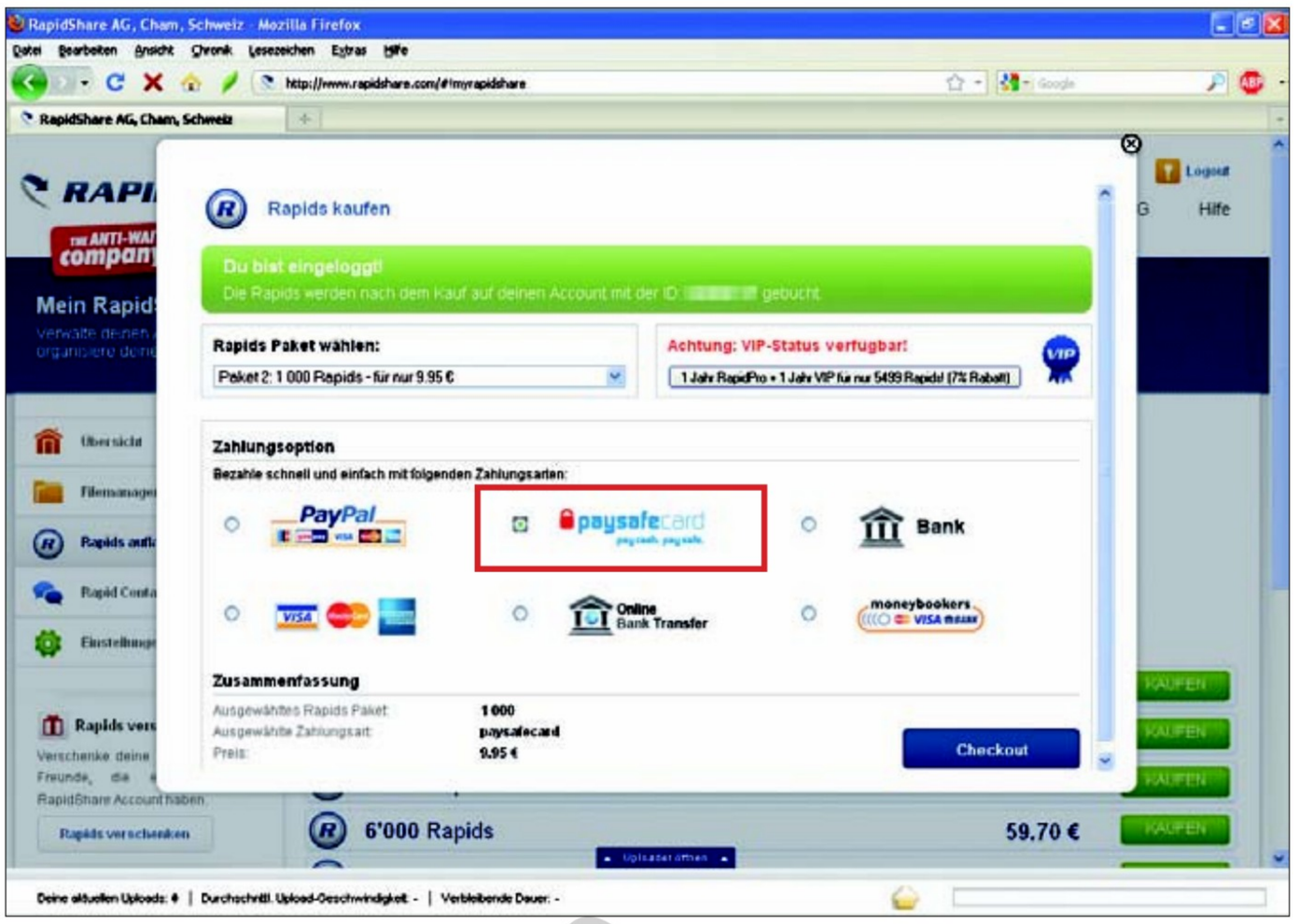
Anbieter sind aber nur wenige dabei. Immerhin wird Paysafecard von Rapidshare, Skype und Steam akzeptiert (Bild D). Außerdem ist es möglich, einen Bon in einen Amazon-Gutschein umzuwandeln. Dazu ist aber eine Registrierung auf der Webseite von Paysafecard nötig.

Der Wert eines Bons kann zwischen 10 und 100 Euro betragen. Sie müssen den Betrag nicht auf einmal ausgeben. Eine Stückelung ist erlaubt. Maximal zehn Bons lassen sich kombinieren, so dass auch Zahlungen bis zu 1000 Euro möglich sind.

24 Monate nach dem Kauf eines Bons oder aber 12 Monate nach der ersten Nutzung des Bons berechnet Paysafecard eine monatliche Gebühr von zwei Euro. Das heißt, der Wert des Bons reduziert sich jeden Monat um zwei Euro, bis das Guthaben aufgebraucht oder das Geld ausgegeben ist.

Wer den Bon an der Kasse mit Bargeld bezahlt, kann mit Paysafecard anonym im Internet einkaufen. So ist es etwa bei Rapidshare möglich, bei der Registrierung eine Wegwerf-Mail-Adresse anzugeben. Eine Identifizierung ist dann nur noch über die IP-Adresse möglich.

Im Prinzip ist Paysafecard genauso sicher wie Bargeld. Wer den PIN-Code hat, kann auch damit einkaufen.



Bezahlmethoden bei Rapidshare: Ein Premium-Account bei Rapidshare lässt sich weitgehend anonym mit Paysafecard bezahlen (Bild D)

3. Ukash: Kombisystem

Auch Ukash verkauft PIN-Codes. Diese Codes lassen sich in Online-Shops einsetzen oder in eine virtuelle Kreditkarte umwandeln.

Prinzipiell funktioniert das Ukash-System, sprich Jukäsch, (www.ukash.de) wie Paysafecard. Zuerst kaufen Sie zum Beispiel an einer Tankstelle in Ihrer Nähe einen Bon mit einem neunzehnstelligen PIN-Code. Bons gibt es im Wert zwischen 10 und 100 Euro.

Der PIN-Code lässt sich in einem der Online-Shops einsetzen, die Ukash unterstützen. Außerdem lässt sich der PIN-Code auf www.ukashneo.com in eine virtuelle Mastercard umwandeln. Dafür ist jedoch eine Online-Registrierung nötig.

Bezahlen per SMS: Geben Sie die TAN im Browser ein, um einen Einkauf zu bezahlen (Bild G)

Besonderheiten: Die genaue Zahl der Online-Shops, die Ukash unterstützen, ist nicht bekannt. Die Mehrheit stammt jedoch bislang aus dem Online-Spiele- und Wettsegment.

Außer Skype und Rapidshare sind bekannte Namen selten. Auf der Ukash-Website ist zum Beispiel auch noch kein einziger EDV-Shop gelistet, der das System unterstützt.

Dafür lässt sich ein Ukash-Bon in andere virtuelle Zahlungsmittel wie Webmoney (www.wmtransfer.com) oder Paybycash (www.paybycash.com) umwandeln (Bild E).

Außerdem bietet das Unternehmen virtuelle Mastercards im Wert zwischen 20 und 450 Euro an. Die virtuelle Mastercard funktioniert wie eine echte Kreditkarte, kann aber nur bis zum eingezahlten Betrag genutzt werden.

Die Maximalsumme für einen Einkauf mit Ukash liegt bei 750 Euro. Der Wert eines Bons lässt sich auch teilen. Anders als bei Paysafecard werden Ukash-Bons jedoch nach zwölf Monaten ungültig. Das Ablaufdatum steht auf dem Bon direkt über dem PIN-Code (Bild F).

Um Bons zu kombinieren oder zu teilen, ist eine Registrierung auf der Ukash-Webseite nötig, bei der aber nur die E-Mail-Adresse mit einer Aktivierungs-Mail überprüft wird. Ansonsten ist das System anonym nutzbar.

Anders ist das bei der virtuellen Mastercard, die Ukash anbietet. Hier ist eine ausführliche Registrierung nötig, bei der einige private Daten wie die Handy-Nummer abgefragt und überprüft werden.

wiwobooks 2.0

4. Mbe4: Bezahlen per Handy

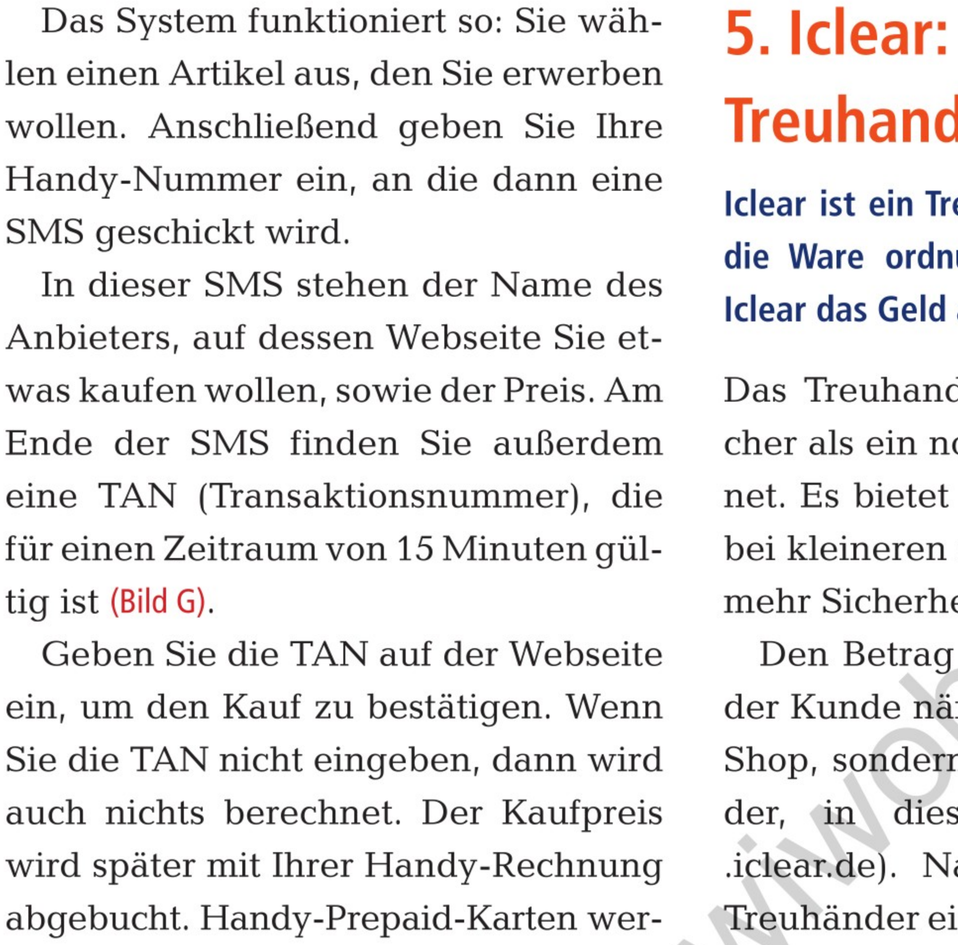
Bezahlen per SMS eignet sich besonders für kleine Beträge. Der zu zahlende Betrag wird mit der Handy-Rechnung abgebucht.

Digitale Produkte wie MP3-Musik oder Artikel aus Zeitschriften im PDF-Format eignen sich besonders gut für das Bezahlen per SMS. Eines der ersten Unternehmen, die das SMS-Bezahlsystem von Mbe4 (www.mbe4.de) nutzen, ist die Stiftung Warentest.

Das System funktioniert so: Sie wählen einen Artikel aus, den Sie erwerben wollen. Anschließend geben Sie Ihre Handy-Nummer ein, an die dann eine SMS geschickt wird.

In dieser SMS stehen der Name des Anbieters, auf dessen Webseite Sie etwas kaufen wollen, sowie der Preis. Am Ende der SMS finden Sie außerdem eine TAN (Transaktionsnummer), die für einen Zeitraum von 15 Minuten gültig ist (Bild G).

Geben Sie die TAN auf der Webseite ein, um den Kauf zu bestätigen. Wenn Sie die TAN nicht eingeben, dann wird auch nichts berechnet. Der Kaufpreis wird später mit Ihrer Handy-Rechnung abgebucht. Handy-Prepaid-Karten werden dagegen sofort belastet.



Ukash umtauschen: Ukash-Bons lassen sich in andere virtuelle Zahlungssysteme umtauschen (Bild E)

Besonderheiten: Bislang unterstützen noch relativ wenige Webseiten wie www.test.de das Bezahlen per SMS. Ein Konkurrenzsystem namens Mpass (www.mpass.de) verwenden unter anderem mehrere Kinos und Shops wie Mymuesli.com.

Gebühren fallen nicht an. Weil Sie eine Handy-Nummer angeben müssen, ist das System nicht anonym.

Auf jeden Fall ist das Bezahlen per SMS sicher – solange Sie Ihr Handy nicht aus der Hand geben.

5. Iclear: Treuhandverfahren

Iclear ist ein Treuhanddienst. Nur wenn Sie die Ware ordnungsgemäß erhalten, leitet Iclear das Geld an den Verkäufer weiter.

Das Treuhandverfahren ist umständlicher als ein normaler Einkauf im Internet. Es bietet dem Käufer aber gerade bei kleineren oder unbekannten Shops mehr Sicherheit.

Den Betrag für seinen Einkauf zahlt der Kunde nämlich nicht direkt an den Shop, sondern zuerst an den Treuhänder, in diesem Fall Iclear (www.iclear.de). Nachdem das Geld beim Treuhänder eingegangen ist, gibt Iclear dem Shop grünes Licht. Dieser versendet daraufhin die Ware direkt an den Kunden.

Erst nachdem die Widerrufsfrist des Käufers von 14 Tagen nach Erhalt der Ware abgelaufen ist, überweist Iclear das eingezahlte Geld an den Shop.

Besonderheiten: Das Treuhändersystem wird vor allem von kleineren Shops genutzt, die sonst oft Vorkasse verlangen.

Sowohl Kunde als auch Verkäufer profitieren von dem System: Versendet der Shop nicht, bliebe dem Käufer meist nur der langwierige Rechtsweg, um wieder an sein bereits bezahltes Geld zu gelangen.

Beim Treuhandverfahren geht das Geld dagegen zuerst an den Treuhänder. Dieser informiert dann den Verkäufer über den Eingang des Geldes. Nun wird die Ware versendet.

Gibt es Probleme beim Versand, erhält der Kunde sein Geld vom Treuhänder zurück. Auf der anderen Seite schützt das Verfahren auch den Verkäufer vor Zahlungsausfällen.

Gebühren für die Nutzung des Treuhandverfahrens fallen für den Käufer keine an. Allenfalls erhöht sich die Wartezeit auf sein Produkt durch die Zwischenstufe etwas.

Das Verfahren ist nicht anonym, bietet aber dem Kunden mehr Sicherheit, im Internet nicht auf ein schwarzes Schaf hereinzufallen. ■

Andreas Th. Fischer
sonderheft@com-magazin.de

Prepaid-System Ukash: Ein Ukash-Bon wird nach zwölf Monaten wertlos (Bild F)

Weitere Infos

- http://finanzen.vsoni.com
  Das steckt hinter Kreditkartennummern

www.bookS 2.0

Elektronischer Personalausweis

Der neue elektronische Personalausweis soll Internet-Transaktionen sicherer machen. Die Technik ist jedoch nicht in jedem Fall sicher vor einem Angriff durch Trojaner.

Zum 1. November 2010 hat Deutschland einen neuen elektronischen Personalausweis eingeführt. Anders als bisherige Ausweise soll das neue Identifikationspapier auch Internet-Banking und Online-Shopping sicherer machen.

Aber noch vor dem Startschuss wurden erste Sicherheitsbedenken laut. So ist der geplante Authentifizierungsprozess nicht in jedem Fall vor Manipulationen durch einen Trojaner sicher, warnt der Chaos Computer Club (www.ccc.de/de/updates/2010/sicherheitsprobleme-bei-suisseid-und-epa).

Was bietet der neue Personalausweis?

Wie bisher können Sie sich mit dem neuen Personalausweis natürlich ausweisen, etwa gegenüber Polizeibeamten oder bei der Beantragung eines Bankkontos.

Darüber hinaus enthält der elektronische Personalausweis auch einen neuen Chip, der zusammen mit einem speziellen Lesegerät zur Identifikation des Besitzers bei Transaktionen im Internet dienen soll. Dieses Verfahren wird als eID (elektronische Identifizierung) bezeichnet.

Zudem wird es mit dem neuen Ausweis möglich sein, Dokumente elektronisch zu unterschreiben.

Webseiten, Automaten und Lesegeräte, die den elektronischen Personalausweis unterstützen, sind mit einem speziellen Logo gekennzeichnet (Bild A).

Logo: Seiten, die eine eID-Anmeldung unterstützen, haben dieses Logo (Bild A)

Was unterscheidet den neuen Ausweis von seinen Vorgängern?

Der elektronische Personalausweis ist kleiner. Die neue Größe entspricht der einer Scheckkarte.

Außerdem enthält er einen neuen Speicherchip. Auf diesem Chip sind unter anderem das für den Ausweis verwendete Lichtbild sowie optional zwei Fingerabdrücke gespeichert. Dadurch soll es Kriminellen erschwert werden, den Ausweis zu missbrauchen.

Daneben enthält der Ausweis einen RFID-Chip (Radio Frequency Identification). Das ist ein Funkchip, der über kurze Entfernungen Daten senden und empfangen kann.

vivobooks 2.0

So geht's: Elektronische Identifizierung (eID)

Ein Anwender kann sich mit der eID-Funktion (elektronische Identifizierung) seines elektronischen Personalausweises beispielsweise gegenüber einem Online-Shop ausweisen. Abgesichert wird das Verfahren mit einer sechsstelligen PIN, die der Anwender eintippt.

Fotos: Manuela Keller

Wie funktioniert die eID?

Sie benötigen ein spezielles Lesegerät, das Sie an Ihren PC anschließen. Manche Geräte haben einen herkömmlichen Kartenschlitz, in den der Ausweis gesteckt wird (Bild B). Bei den so genannten Basislesegeräten genügt es jedoch, den Ausweis einfach daraufzulegen (Bild C). Der Funkchip im Ausweis kommuniziert dann mit dem Lesegerät.

Außerdem muss auf dem PC die Ausweis-App (kostenlos, www.ausweisapp.bund.de) installiert sein. Diese Software kümmert sich um die Datenübertragung zwischen Ausweis und Online-Shop.

Melden Sie sich nun beispielsweise bei einem Online-Shop an, sendet der Anbieter zunächst sein Berechtigungszertifikat. Dieses Zertifikat wird dann in der Ausweis-App angezeigt. Anschließend entscheiden Sie, welche der angeforderten privaten Daten wie Vor- und Nachname oder Wohnort Sie übertragen wollen. Wer will, kann auch nur eine spezielle ID übertragen lassen, die eine halbwegs anonyme Nutzung verschiedener Internetangebote ermöglichen soll.

Zuletzt müssen Sie Ihre sechsstellige PIN (Persönliche Identifikationsnummer) eingeben, um sich zu authentifizieren. Anschließend überträgt die Ausweis-App die freigegebenen Daten an den Internetanbieter.

Ist die eID-Funktion sicher?

In Verbindung mit einem Basislesegerät ist die eID-Funktion nicht sicher.

Weil Basislesegeräte über keine Tastatur verfügen, erfolgt die Eingabe der sechsstelligen PIN mit der Computer-Tastatur. Befindet sich auf dem Rechner ein Trojaner, kann dieser die Eingabe der PIN belauschen. Bei Lesegeräten mit Tastatur ist dies nicht möglich, da die Datenübertragung verschlüsselt wird.

Das Problem wird noch verschärft, wenn Sie Ihre Karte nicht sofort wieder vom Basislesegerät herunternehmen, sondern sie dort liegen lassen. Dann kann der Trojaner die PIN und die Karte gemeinsam einsetzen, als hätte ein Dieb die Ausweiskarte geklaut.

Basislesegerät: Der neue elektronische Personalausweis liegt auf einem Basislesegerät. Dieses Gerät hat keine Tastatur und ist mit dem Ausweis per Funk verbunden (Bild C)

Was ist die Pseudonym-Funktion?

Als einer der Pluspunkte für den neuen Ausweis wird die Pseudonym-Funktion genannt. Damit sei es möglich, Online-Dienste zu nutzen, „ohne dass personenbezogene Daten übermittelt werden“. Zur Identifizierung des Nutzers dient dann eine spezielle ID, die für jeden Online-Dienst neu generiert wird. Ob man durch diese ID gegenüber Behörden identifizierbar bleibt, ist nicht bekannt – aber wahrscheinlich.

Lesegerät mit Display und Tastatur: Nur diese Geräteklasse bietet die höchste Sicherheit und eignet sich zudem für digitale Signaturen und Online-Banking mit HBCI (Bild B)

Wie funktioniert die digitale Unterschrift?

Der neue Personalausweis soll sich auch dazu verwenden lassen, digitale Dokumente rechtsverbindlich zu unterschreiben.

Dazu benötigen Sie ein spezielles Signaturzertifikat. Um dieses Zertifikat zu erhalten, müssen Sie sich per eID-Funktion ausweisen. Anschließend wird das Zertifikat auf den Ausweis geladen. Zusammen mit einer weiteren PIN dient das Zertifikat dann dazu, digitale Dokumente zu unterzeichnen.

Welches Lesegerät benötige ich?

Auf keinen Fall sollten Sie ein Basislesegerät ohne eigene Tastatur verwenden, weil bei diesen Modellen die Eingabe der PIN nicht sicher vor Trojanern ist. Unverständlicherweise sollen aber gerade diese Geräte zu vergünstigten Preisen oder gar kostenlos unter die Bevölkerung gebracht werden, um eine schnelle Verbreitung zu fördern.

Geräte mit Tastatur sind teurer. So nennt etwa Reiner SCT als Preise für seine Tastaturmodelle Cyberjack RFID Standard und Komfort 37,90 Euro beziehungsweise 119,90 Euro. Die Basisvariante ohne Tastatur kostet 34,90 Euro. SCM Microsystems bietet das Basislesegerät SCL011 für 25 Euro an.

Die Komfortmodelle lassen sich auch für digitale Signaturen und Online-Banking mittels HBCI (Homebanking Computer Interface) verwenden.

Was ändert sich darüber hinaus?

Der neue Personalausweis darf nicht mehr hinterlegt werden, etwa in einem Hotel. Zusammen mit einer geklauten PIN könnte er ohne Wissen des Besitzers missbraucht werden. ■

Andreas Th. Fischer
sonderheft@com-magazin.de

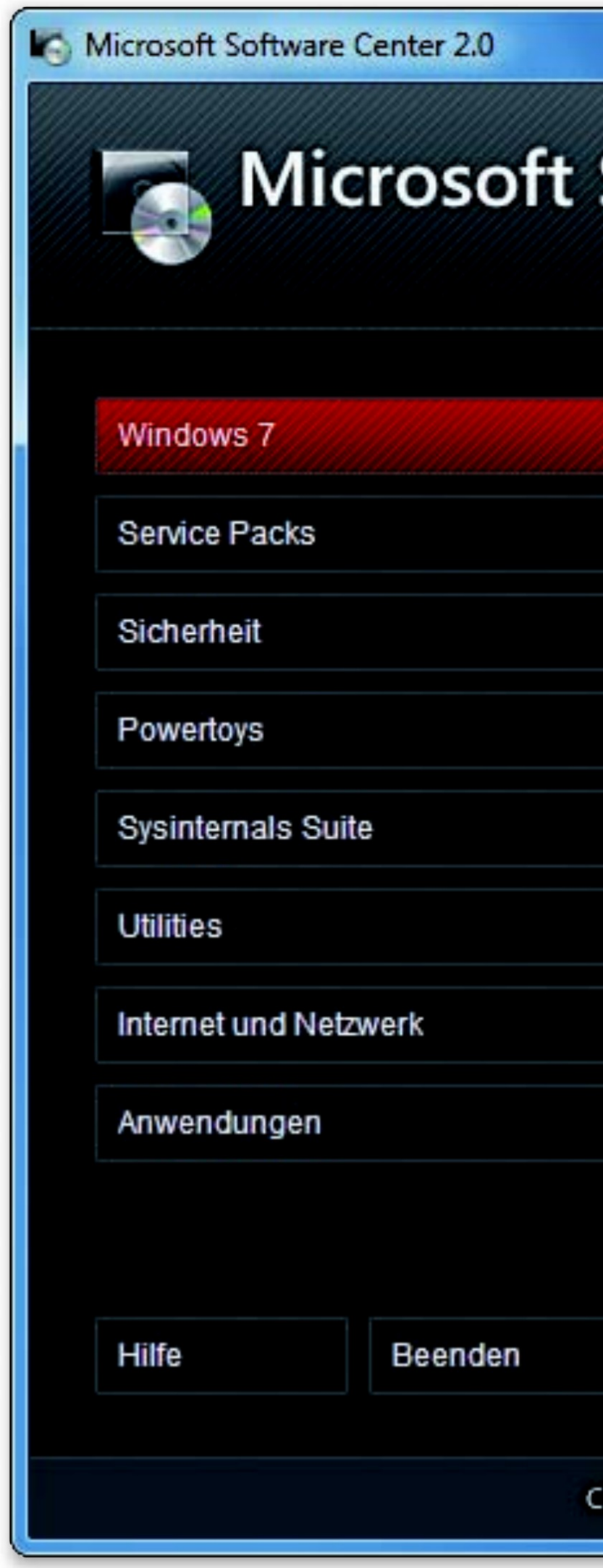
Weitere Infos

- www.ccepa.de/public/kartenleser.htm
  Übersicht über zertifizierte und nicht zertifizierte Kartenleser

wiwobooks 2.0

Microsoft Soft

Setup-DVDs von Windows 7, neue Service-Packs und vieles mehr: Das Microsoft Software Center 2.0 gibt Schnellzugriff auf die besten Tools von Microsoft.



Kompakt

- *Das Microsoft Software Center 2.0 verschafft Zugriff auf 206 aktuelle Programme von Microsoft.*
- *143 der Microsoft-Programme lassen sich direkt aus dem Microsoft Software Center 2.0 heraus installieren.*
- *Die übrigen 63 Programme können Sie bequem per Link aus dem Internet nachladen.*

Die Oberfläche des Microsoft Software Centers 2.0 hat die com!-Redaktion programmiert. Die eingebundenen Programme kommen von Microsoft. Sie erhalten dadurch Sofortzugriff auf 206 Programme. Sie finden das Software Center auf der Heft-DVD.

In Version 2.0 sind über 30 Programme neu – 50 wurden aktualisiert. Neu ist auch die integrierte Suche in der Hilfe-Seite.

Microsoft Software Center 2.0

Die meisten der Microsoft-Programme – 143 – lassen sich direkt aus dem Microsoft Software Center 2.0 heraus installieren. Für einige Programme hat die com!-Redaktion von Microsoft keine Freigaben erhalten: Diese insgesamt 63 Tools erreichen Sie bequem über die im Software Center hinterlegten Download-Links.

Das Microsoft Software Center liefert zu jedem Programm eine deutschsprachige Beschreibung, nennt die Systemvoraussetzungen sowie die Programmsprache und verlinkt außerdem zu weiterführenden Informationen von Microsoft.

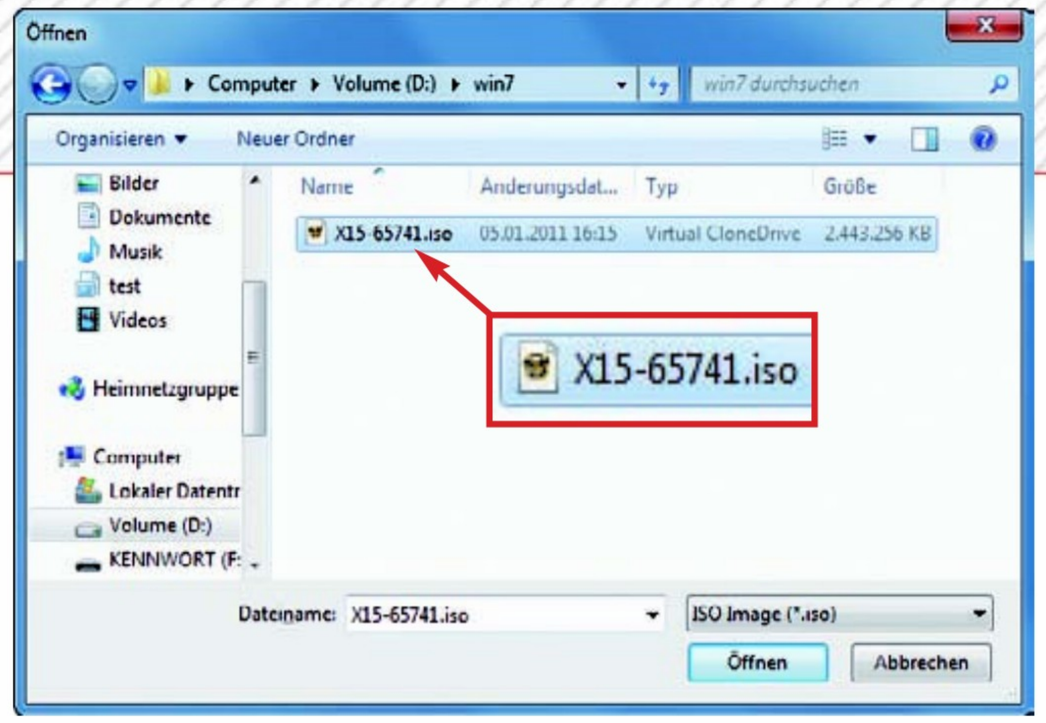
Das Microsoft Software Center läuft unter Windows XP, Vista und 7. Eine Übersicht aller 206 Microsoft-Programme finden Sie auf Seite 76. ▶

Inhalt

- **Microsoft Software Center 2.0**
  - Programmstart S. 70
  - Bedienung S. 70
- **Microsoft-Tools**
  - Setup-DVD von Windows 7 S. 70
  - Windows 7 USB/DVD Download-Tool S. 71
  - Windows Service Packs S. 72
  - Windows Virtual PC S. 72
  - Windows XP Mode S. 73
  - Microsoft Security Essentials S. 73
  - Deep Zoom Composer S. 74
  - Calculator Plus S. 75
  - Internet Explorer 9 S. 75
  - File System Explorer S. 76
- So geht's: Microsoft Software Center 2.0 S. 71
- Microsoft Software Center 2.0: Das ist drin S. 76

www.books2.0

ware Center 2.0



Setup-DVD von Windows 7: Das Microsoft Software Center 2.0 lädt auch die ISO-Images der Setup-DVDs von Windows 7 herunter (Bild A)

Programmstart

Sie brauchen das Microsoft Software Center nicht zu installieren. Es lässt sich direkt von der Heft-DVD starten. Wählen Sie dort die Rubrik „Computer, Microsoft Software Center“ und klicken Sie auf „Programm ausführen“.

Bedienung

Nach dem Programmstart erscheint das Hauptfenster des Microsoft Software Centers. Links sehen Sie die acht Rubriken „Windows 7“, „Service Packs“, „Sicherheit“, „Powertoys“, „Sysinternals Suite“, „Utilities“, „Internet und Netzwerk“ und „Anwendungen“.

Wenn Sie eine Rubrik aktivieren, erscheint in der rechten Fensterhälfte die Liste mit Programmen, die der Rubrik zugeordnet sind. Am rechten Fensterrand ist ein Scroll-Balken, mit dem Sie durch die Liste navigieren.

Bei Programmen, die direkt im Microsoft Software Center enthalten sind, finden Sie eine Schaltfläche mit der Bezeichnung „Installieren“. Je nachdem in welcher Form das Programm vorliegt, startet nach dem Klick die Set-

Windows 7 USB/DVD Download-Tool: Das Programm erstellt einen bootfähigen USB-Stick mit den Installationsdateien von Windows 7 (Bild B)

up-Routine oder bei einem ZIP-Archiv der Packer. Entpacken Sie dann das Programm in ein Verzeichnis Ihrer Wahl.

Bei Programmen, die nicht in das Microsoft Software Center 2.0 integriert sind, finden Sie den Button „Herunterladen“.

Um die Suchfunktion aufzurufen, klicken Sie im Hauptfenster auf die Schaltfläche „Hilfe“. Die Hilfe-Seite enthält eine vollständige Software-Übersicht. Sie lässt sich mit [Strg F] durchsuchen.

Microsoft-Tools

Das Microsoft Software Center bietet Zugriff auf 206 Programme von Microsoft. Die zehn besten stellen wir Ihnen hier vor.

Setup-DVD von Windows 7

Das ISO-Image enthält die Installationsdateien für Windows 7. Mit Lizenzschlüsseln lassen sich die Testversionen dauerhaft nutzen.

Das Microsoft Software Center 2.0 enthält in der Rubrik „Windows 7“ Download-Links zu den Setup-DVDs von Windows 7. Microsoft bietet die ISO-Images für Windows 7 nämlich zum kostenlosen Download an. Das ist besonders nützlich für Anwender, die beim Kauf ihres PCs keinen Setup-Datenträger mitgeliefert bekommen haben. Wenn Sie die 30-Tage-Testversionen von Windows 7 dauerhaft nutzen wollen, müssen Sie einen gültigen Lizenzschlüssel eingeben.

Die Images enthalten alle Windows-Versionen, sind aber auf die Varianten Windows 7 Home Premium und Windows 7 Professional vorkonfiguriert. Das bedeutet: Im Image befindet sich die Datei „ei.cfg“, in der steht, welche Windows-Version installiert werden soll.

Falls Sie möchten, dass Ihnen das Setup alle Versionen von Windows 7 zur Installation an-

wiwobooks 2.0

bietet, löschen Sie die Datei mit dem Tool ei.cfg Removal Utility 1.1 (kostenlos, http://code.kliu.org/misc/win7utils). Laden Sie das Tool herunter und entpacken Sie das Archiv. Starten Sie es mit einem Doppelklick auf die EXE-Datei. Markieren Sie jetzt das ISO-Image von Windows 7 und klicken Sie auf „Öffnen“ (Bild A). Das Tool verändert nun ein spezielles Bit im ISO-Image, damit die Datei „ei.cfg“ nicht mehr gefunden wird.

Um die ISO-Datei auf DVD zu brennen, nutzen Sie ein Brennprogramm Ihrer Wahl oder Imgburn 2.5.5.0 (kostenlos, www.imgburn.com und auf).

Wie Sie aus einem USB-Stick mit mindestens 4 GByte Speicherplatz einen Setup-Stick für Windows 7 erstellen, lesen Sie im folgenden Abschnitt „Windows 7 USB/DVD Download-Tool“.

Auf der Heft-DVD finden Sie außerdem PDF-Dateien mit nützlichen Anleitungen zur Setup-DVD von Windows 7: Der Artikel „Windows 7 Demo geknackt“ etwa beschreibt, wie Sie den Testzeitraum von Windows 7 beliebig ausdehnen. Der Beitrag „Individuelle Setup-DVD für Windows 7“ zeigt, wie Sie ein 1-Klick-Setup für Windows 7 erstellen, und in „Aktivierung sichern – und zurückspielen“ lesen Sie, wie Sie die erneute Aktivierung von Windows 7 legal umgehen.

Windows 7 USB/DVD Download-Tool

Das Tool kopiert die Setup-Dateien von Windows 7 auf einen USB-Stick. Damit lässt sich Windows 7 auch auf Netbooks installieren (für XP/Vista/7).

Subnotebooks oder Netbooks haben meist kein optisches Laufwerk. Wer auf so einem PC ein Betriebssystem wie Windows 7 installieren möchte, braucht ein externes DVD-Laufwerk oder einen bootfähigen USB-Stick, der die Installationsdateien von Windows 7 enthält.

Den bootfähigen USB-Stick mit den Installationsdateien erstellen Sie mit dem Windows 7 USB/DVD Download-Tool. Das Programm ist im Micosoft Software Center enthalten. Sie finden es in der Rubrik „Windows 7“. Außerdem brauchen Sie das ISO-Image der Setup-DVD von Windows 7 und einen USB-Stick mit mindestens 4 GByte Speicherplatz.

Beachten Sie, dass das Windows 7 USB/DVD Download-Tool alle auf dem USB-Stick vorhandenen Daten löscht.

Installieren und starten Sie das Tool. Geben Sie bei „Source file“ den Pfad zum ISO-Image an und klicken Sie auf „Next“. Klicken Sie auf „USB device“ und wählen Sie Ihren USB-Stick aus (Bild B). Erstellen Sie den Setup-Stick mit einem Klick auf „Begin copying“. Das Tool formatiert den USB-Stick, macht ihn bootfähig und kopiert die Installationsdateien auf den Datenträger. Der USB-Stick bootet fortan beliebige Rechner und installiert auf ihnen Windows 7. ▶

So geht's: Microsoft Software Center 2.0

Das Microsoft Software Center enthält insgesamt 206 Programme, unterteilt in acht Rubriken. Das Center muss nicht installiert werden und läuft direkt von Heft-DVD.

1 Hauptmenü
Hier wählen Sie eine Rubrik. Durchsuchen Sie sie mit [Strg F].

2 Installieren
Die Schaltfläche installiert das Programm direkt von der Heft-DVD.

3 Programmdetails
Hier finden Sie zusätzlich einen Link zur Webseite des Programms.

4 Hilfe
Hier finden Sie eine Liste mit allen Programmen. Sie lässt sich durchsuchen.

www.winbooks.at

Windows Service Packs

Das Microsoft Software Center enthält Links zu den aktuellen Service-Packs für Windows (für XP/Vista/7).

Die Service-Packs sind Softwarepakete, die alle Updates für XP, Vista und Windows 7 enthalten. Wenn Sie im Microsoft Software Center 2.0 auf „Herunterladen“ klicken, öffnet sich die Download-Seite. Dort erhalten Sie eine EXE-Datei, mit der Sie beliebige PCs auf den neuesten Stand bringen können. Packen Sie sie dazu auf einen USB-Stick.

Windows XP: Für Windows XP bietet Microsoft bereits die dritte Version eines Service-Packs an (Bild C). Das rund 313 MByte große Service Pack 3 enthält alle Aktualisierungen, die bis zum Erscheinen des Service-Packs veröffentlicht wurden – also auch die Updates, die in Service Pack 1 und 2 enthalten sind. Ein installiertes XP lässt sich allerdings nur dann mit Service Pack 3 aktualisieren, wenn vorher mindestens bereits das SP 1 installiert ist.

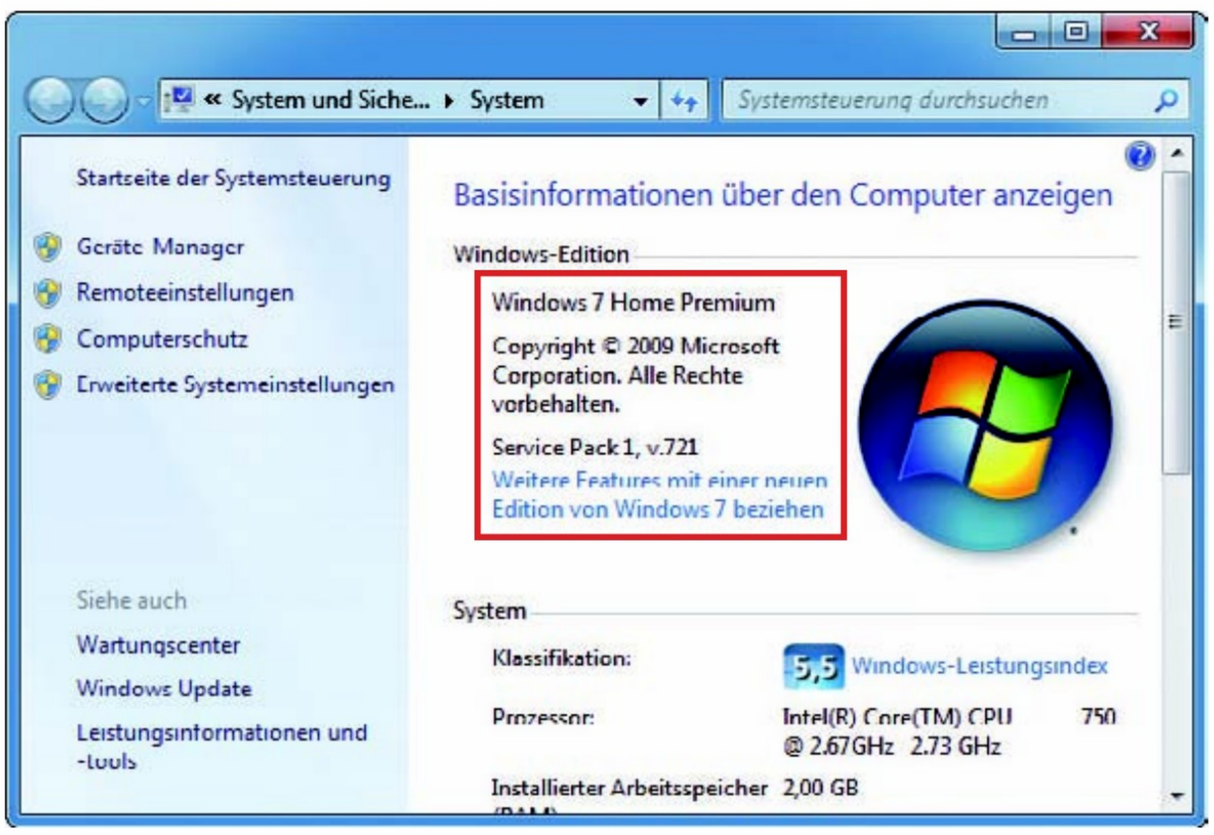
Windows Vista: Die aktuellste Version des Service-Packs für Vista ist die Version 2. Anders als bei XP enthält das Service Pack 2 nur die Patches, die seit dem Erscheinen des Service Packs 1 veröffentlicht wurden. Das bedeutet, dass Anwender der 32-Bit-Version von Vista insgesamt rund 780 MByte herunterladen müssen, Nutzer der 64-Bit-Version 1,3 GByte.

Service Pack 3 für XP: Die Standalone-Version des Service-Packs aktualisiert beliebige PCs mit Windows XP (Bild C)

Windows 7: Für Windows 7 ist von Microsoft das erste Service-Pack verfügbar (Bild D). Diese Version enthält alle Patches, Bugfixes und Updates, die Microsoft bislang für Windows 7 veröffentlicht hat. Microsoft bietet das Service-Pack in einer 64-Bit- und einer 32-Bit-Version an. Das Patch-Paket für ein 64-Bit-Windows ist rund 870 MByte groß, das Patch-Paket für ein 32-Bit-Windows nur 515 MByte.

Wenn Sie testen wollen, wie sich das Service-Pack auf Ihr Windows-7-System und Ihre Anwendungen auswirkt, sollten Sie vor der Installation einige Dinge beachten. Näheres dazu steht im Artikel „Service Pack 1 RC 1 für Windows 7“. Sie finden ihn als PDF auf der Heft-DVD sowie als Download unter www.com-magazin.de im Heft-Archiv in der com!-Ausgabe 2/2011.

Basisinformationen über den Computer: Hier sehen Sie, welches Service-Pack auf Ihrem PC installiert ist. Das Fenster rufen Sie mit der Tastenkombination [Windows Pause] auf (Bild D)



Windows Virtual PC

Die Software erstellt auf einem Computer mit Windows 7 virtuelle Maschinen mit unterschiedlichen Betriebssystemen (für 7).

Windows Virtual PC ist Microsofts neueste Virtualisierungstechnik. Beachten Sie, dass das Programm ausschließlich unter Windows 7 läuft. Nach dem Start simuliert das Programm einen vollständigen PC mit der dazugehörenden Hardware. Windows Virtual PC unterstützt nur Windows-Betriebssysteme.

Um Windows Virtual PC zu nutzen, muss Ihr Rechner die hardwaregestützte Virtualisierung unterstützen. Dabei handelt es sich um eine Funktion des Prozessors. Sie erlaubt den direkten Zugriff auf die CPU und erhöht damit die Leistung der virtuellen Maschine. Ob Ihr PC die hardwaregestützte Virtualisierung be-

wiwobooks 2.0

herrscht, stellen Sie mit dem Tool Microsoft Hardware-Assisted Virtualization Detection Tool 1.0 fest (Bild E). Dieses Programm lässt sich direkt aus dem Software Center heraus installieren.

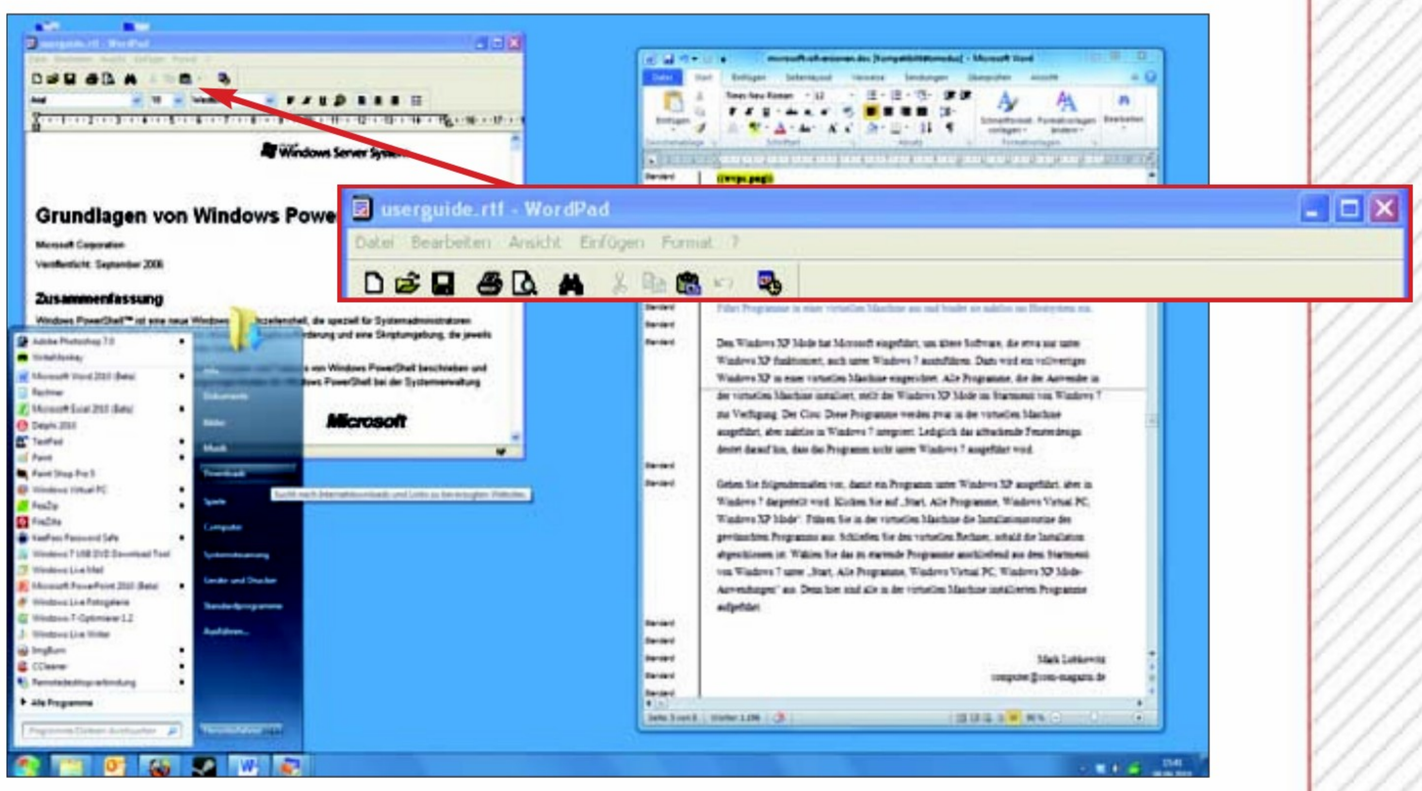
Falls Ihre CPU keine hardwaregestützte Virtualisierung unterstützt, installieren Sie den Patch KB977206 (kostenlos, http://support.microsoft.com/kb/977206). Nach diesem Update lässt sich Windows Virtual PC auch auf älteren PCs verwenden.

Windows XP Mode

Der Windows XP Mode führt XP-Anwendungen auf einem Computer mit Windows 7 aus (für 7).

Der XP-Mode ist eine virtuelle Maschine mit Windows XP Professional. So lässt sich alte Software unter Windows 7 weiterverwenden.

Die Besonderheit des XP-Modes: Alle installierten Programme sind in das Startmenü von Windows 7 integriert und werden nahtlos ausgeführt. Das bedeutet: Wenn Sie ein altes Programm starten, bekommen Sie gar nicht mit, dass im Hintergrund die virtuelle Maschine aktiv ist. Sie erkennen diese Programme nur an dem für XP typischen Rahmen (Bild F).



Windows XP Mode: Programme, die in Windows XP Mode ausgeführt werden, sind nahtlos in Windows 7 integriert und nur am klassischen XP-Fensterrahmen zu erkennen (Bild F)

Hardware-Assisted Virtualization Detection Tool 1.0: Das Programm ermittelt, ob Ihr PC hardwaregestützte Virtualisierung unterstützt. Damit arbeitet Windows Virtual PC nämlich deutlich schneller (Bild E)

Wer kein Windows 7 Ultimate oder Professional auf seinem Rechner hat, kann den XP-Mode zwar installieren, der Start bricht jedoch mit einem Hinweis auf die fehlende Berechtigung ab. Falls Sie jedoch eine alte Lizenz von Windows XP Professional übrig haben, dann rüsten Sie den XP-Mode einfach manuell nach. Wie Sie das anstellen, lesen Sie im Artikel „XP-Mode für Home Premium“. Den Artikel finden Sie im PDF-Format auf Heft-DVD sowie als Download unter www.com-magazin.de im Heft-Archiv in der com!-Ausgabe 2/2010.

Microsoft Security Essentials

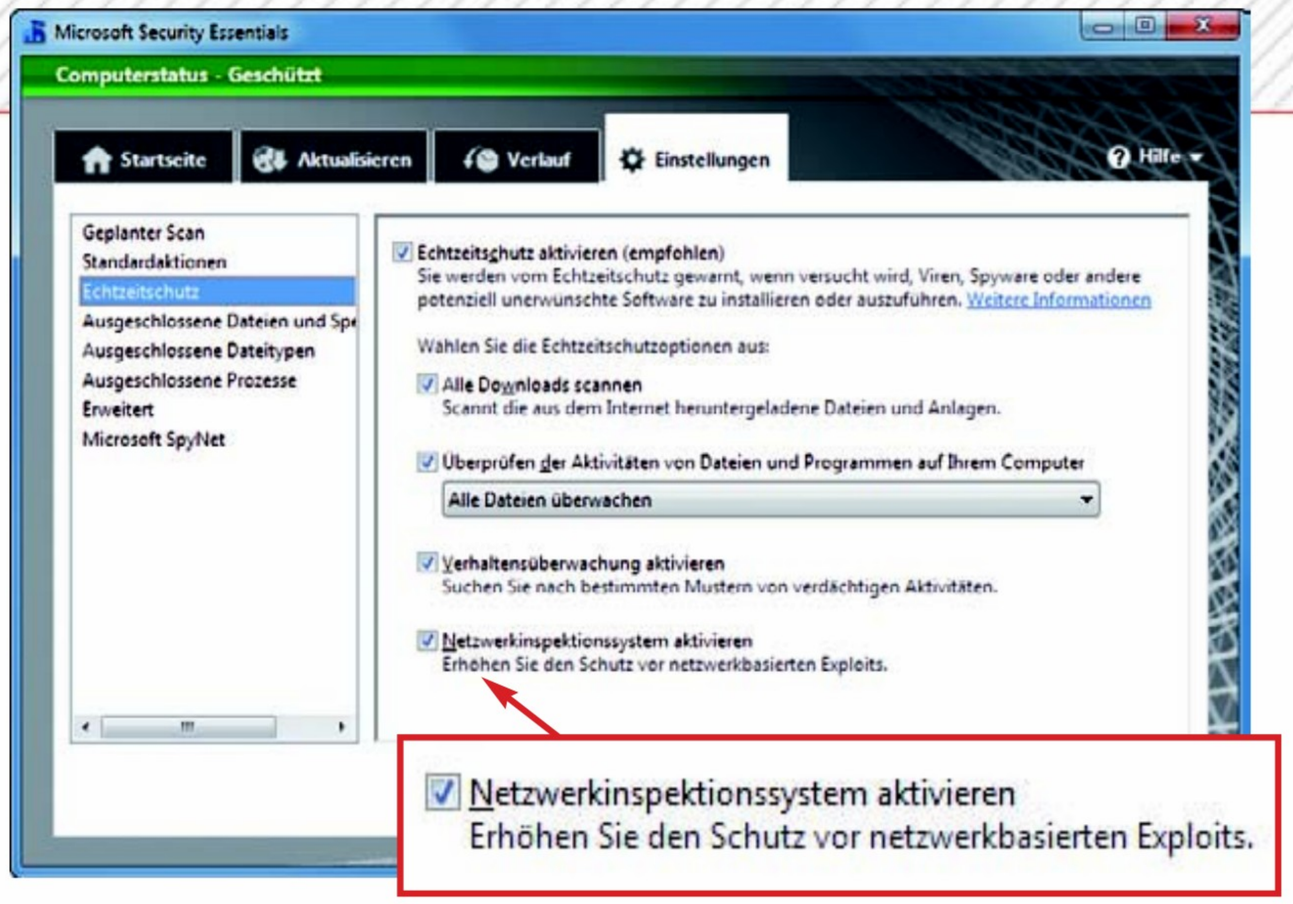
Die neue Version der Virenschutzsoftware von Microsoft scannt besser und schützt nun auch vor Netzwerkangriffen (für XP/Vista/7).

Die neue Antivirensoftware von Microsoft wurde teilweise überarbeitet und hat neue Funktionen erhalten.

Eine der wichtigsten Neuerungen ist die verbesserte Heuristik. Dadurch soll Microsoft Security Essentials 2.0 Schadsoftware noch besser am verdächtigen Verhalten erkennen.

Die Schutzsoftware prüft darüber hinaus Dateien, wenn sie heruntergeladen oder ausgeführt werden. ▶

wiwobooks 2.0



Microsoft Security Essentials 2.0: Die Schutzsoftware überwacht den Netzwerkverkehr nun auch auf Paketbasis und stellt auch so Schadsoftware fest (Bild G)

Außerdem schützt die neue Option „Netzwerkinspektionssystem aktivieren“ jetzt auch gegen Netzwerkangriffe (Bild G). Dazu nutzt die Software die Windows Filtering Platform (WFP). Das Programm hat dadurch Zugriff auf den Paketverkehr im Netzwerk und kann ein- und ausgehenden Datenverkehr untersuchen und bei Gefahr eingreifen. WFP wurde mit Vista eingeführt und steht unter XP nicht zur Verfügung.

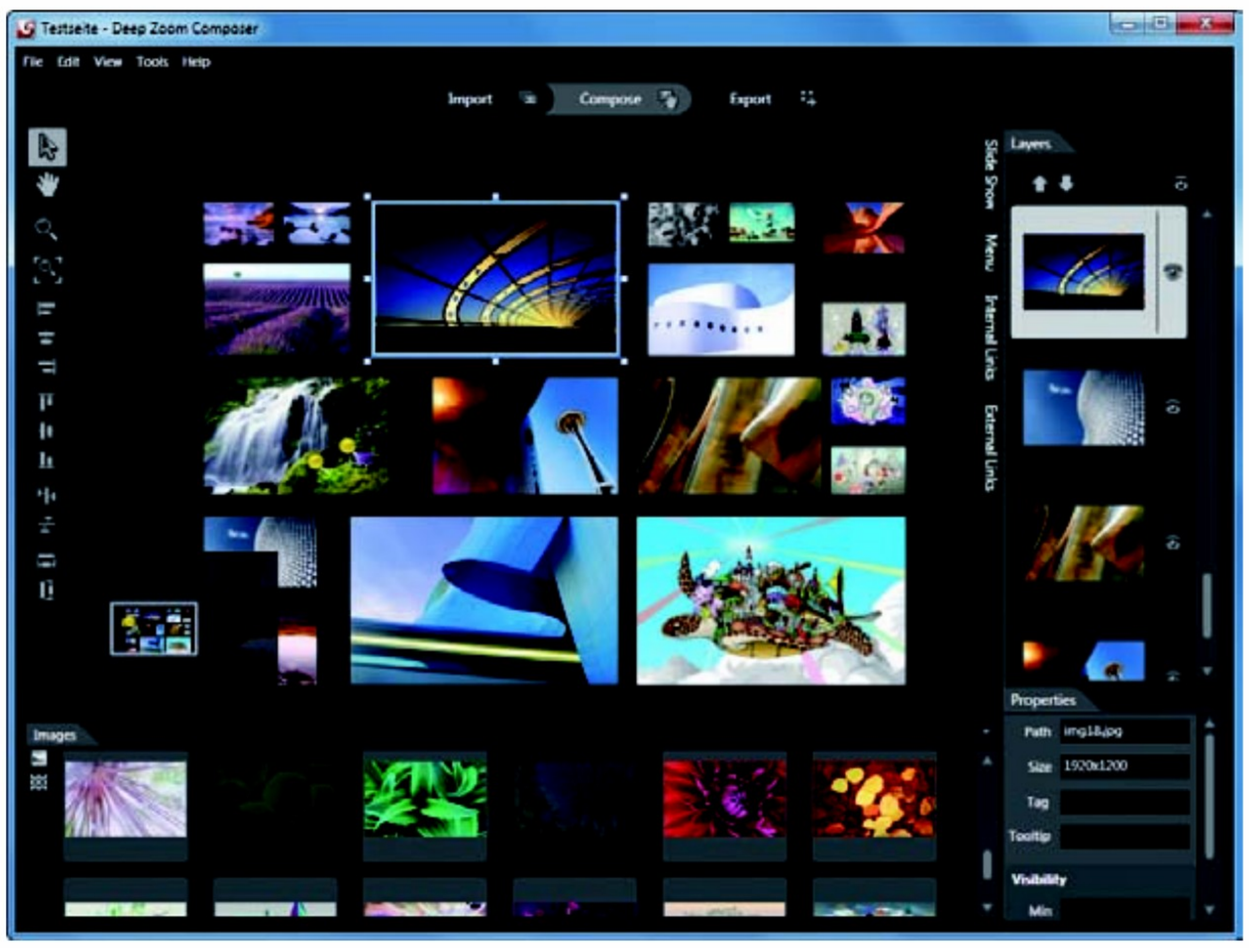
Praktisch ist auch eine Option, mit der sich die Systembelastung begrenzen lässt. Das ist nützlich bei Rechnern, die schnell überhitzen oder nicht besonders leistungsstark sind. Auf dem Register „Einstellungen“ in der Rubrik „Geplanter Scan“ lässt sich definieren, wie viel Prozent der CPU-Auslastung ein Programm beanspruchen darf. Bei schwachen Systemen ist ein Wert von 20 oder 30 Prozent eine gute Wahl.

Deep Zoom Composer

Die Software präpariert Bilder so, dass man bei gleichbleibender Bildqualität sehr stark in sie hineinzoomen kann (für XP/Vista/7).

Das englischsprachige Programm Deep Zoom Composer erstellt innerhalb weniger Minuten eine Bildergalerie für die Homepage. Die Besonderheit: In die hochaufgelösten Fotos lässt sich ohne Qualitätsverlust hineinzoomen – ähnlich wie bei Online-Shops, wo der Anwender beispielsweise die Kleidung bis auf die Fasern unter die Lupe nehmen kann.

Damit Sie das Tool verwenden können, muss mindestens Silverlight 3 installiert sein.



Deep Zoom Composer 1.0: Das neue, englischsprachige Programm von Microsoft bereitet Bilder so vor, dass man ohne Qualitätsverlust in sie hineinzoomen kann (Bild H)

Installieren und starten Sie den Deep Zoom Composer. Wählen Sie „New Project …“. Die Rubrik „Import“ ist nun aktiv. Klicken Sie rechts auf „Add image …“ und fügen Sie alle Bilder hinzu, die Sie für die Bildergalerie verwenden möchten. Aktivieren Sie oben in der Mitte die Rubrik „Compose“. Stellen Sie dann Ihre Bildergalerie zusammen. Ziehen Sie dazu die Bilder in die Fenstermitte und arrangieren Sie sie (Bild H).

Die Werkzeugleiste am linken Fensterrand hilft Ih-

www.books 20

nen, die Fotos anzuordnen. Nachdem Sie alle Bilder am gewünschten Ort platziert haben, klicken Sie oben in der Mitte auf „Export“. Vergeben Sie einen Namen und klicken Sie auf „Export“. Die Bildergalerie können Sie nun zum Beispiel auf Ihrer Website veröffentlichen.

Calculator Plus

Der Profirechner bietet Funktionen zur Umrechnung von Währungen, Maßen und physikalischen Größen (für XP).

Calculator Plus ist ein aufgebohrter Taschenrechner für Windows XP. Neben den Funktionen, die auch der normale Windows-Taschenrechner „calc.exe“ bereits anbietet, bringt Calculator Plus viele weitere nützliche Funktionen mit – etwa einen Währungsrechner.

Die Ansicht des Taschenrechners ist aufgrund des Fensterdesigns und der Farbgebung etwas gewöhnungsbedürftig. Die gewohnte klassische Ansicht erhalten Sie über „Ansicht, klassische Ansicht“.

Bevor Sie Währungen umrechnen, laden Sie zunächst die aktuellen Wechselkurse von der Europäischen Zentralbank herunter. Klicken Sie dazu auf „Bearbeiten, Umrechnungskurse der EZB importieren“. Danach wählen Sie unter „Kategorie“ die Option „Währungen“ (Bild I).

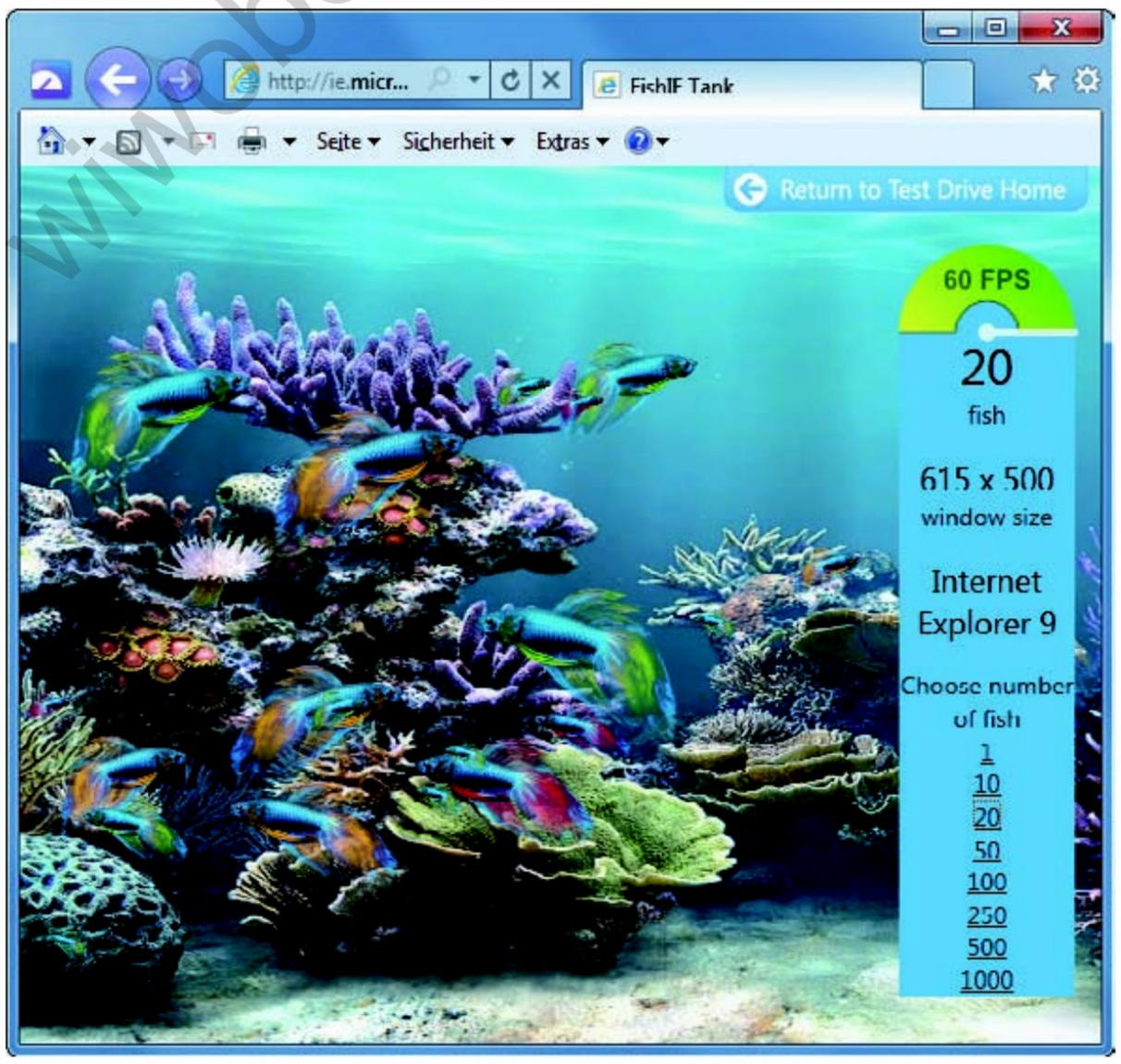
Calculator Plus: Der wissenschaftliche Rechner bietet auch einen Umrechnungsmodus für Währungen. Die aktuellen Wechselkurse holt er sich von der EZB (Bild I)

Internet Explorer 9

Der neue Browser nutzt die Leistung der Grafikkarte. Spezielle Webseiten lassen sich so schneller darstellen (für Vista/7).

Der Internet Explorer 9 bringt einige interessante neue Funktionen mit. So lassen sich Webseiten in der Taskleiste ablegen und wie Apps verwenden. Rufen Sie beispielsweise die Suchmaschine www.bing.de auf und ziehen Sie den Browser-Tab in die Taskleiste – dann wird er dort sofort angehängt. Wenn Sie jetzt mit einem Rechtsklick auf das Icon klicken, finden Sie dort nicht nur den Link zur Suchmaschine, sondern auch eine Jumplist mit speziellen Funktionen. Bei Bing sind das etwa Wetterdienst, Finanznachrichten, News oder ein Routenplaner.

Für mehr Sicherheit bei Downloads soll das Smartscreen-Application-Reputation-System sorgen. Bei einem Download stuft die Funktion die Datei ein und gibt bei Bedarf eine Warnmeldung aus. ▶



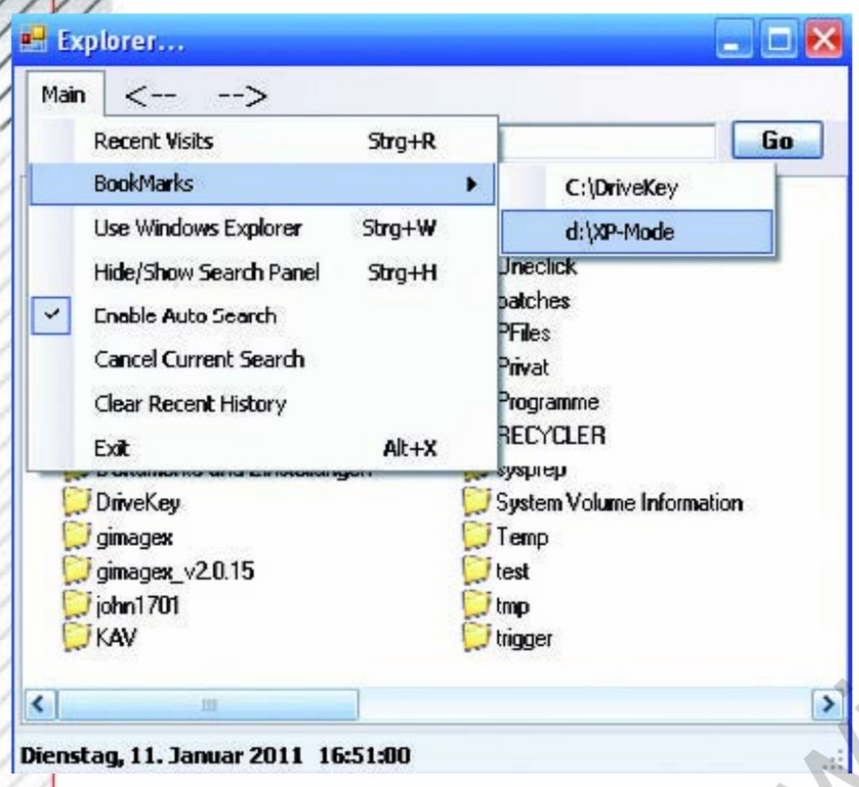
Internet Explorer 9: Den Aquarium-Test bestehen nur Browser, die den Grafikchip zur Berechnung nutzen – wie der neue Microsoft-Browser (Bild J)

www.books2.0

Der IE 9 nutzt erstmals auch die Grafikkarte zur Darstellung von Webseiten und deren Inhalten. Vor allem bei HTML5 sowie bei Video-Inhalten bringt das einen deutlichen Leistungszuwachs. Beim Test auf der Seite http://ie.microsoft.com/testdrive/performance/FishIETank/ (Bild J) erreichte der Browser durchweg 60 Frames pro Sekunde – bei deaktivierter Hardware-Beschleunigung sank der Wert auf 3 fps.

File System Explorer

Das Tool beschleunigt die Suche nach bestimmten Dateien und erstellt Bookmarks für wichtige Ordner (für XP).



File System Explorer: Das Utility erstellt Bookmarks für häufig benötigte Ordner (Bild K)

Der File System Explorer ist ein kleines Tool, das die Arbeit mit Dateien und Ordnern vereinfacht.

Wenn Sie häufig mit speziellen Ordnern arbeiten, Sie sich aber nicht durch die Ordnerstruktur auf der Festplatte klicken wollen, erstellen Sie mit File System Explorer Bookmarks der wichtigsten Ordner. Wechseln Sie dazu einmal in den Ordner und erstellen Sie mit [Strg I] ein Lesezeichen des Ordners. Um schnell in das Verzeichnis zu wechseln, klicken Sie im File System Explorer auf „Main, Bookmarks“ und dort dann auf den hinterlegten Ordner (Bild K). Wenn Sie das Verzeichnis mit dem Windows-Explorer öffnen wollen, nutzen Sie den Tastaturbefehl [Strg W]. ■

Oliver Ehm
sicherheit@com-magazin.de

Weitere Infos

- www.microsoft.com/downloads/de-de/default.aspx
  Download-Center von Microsoft
- http://research.microsoft.com/en-us
  Website der Forschungsabteilung von Microsoft

Microsoft Software Center 2.0: Das ist drin

Windows 7

- D Windows 7 Home Premium (32 Bit)
- D Windows 7 Home Premium (64 Bit)
- D Windows 7 Professional (32 Bit)
- D Windows 7 Professional (64 Bit)
- WIM2VHD 6.1.7600.0
- Windows 7 Upgrade Advisor 2.0.4000.0
- Windows 7 USB/DVD Download Tool 1.0
- D Windows AIK für Windows 7 2.0
- D Windows-Easy Transfer für Vista (32 Bit)
- D Windows-Easy Transfer für Vista (64 Bit)
- D Windows-Easy Transfer für XP (32 Bit)
- Windows Easy Transfer für XP (64 Bit)
- D Windows Virtual PC 6.1.7600.16393
- D Windows XP Mode 1.3.7600.16422

Service Packs

- D Windows 7 Service Pack 1 RC 1 (64 Bit)
- D Windows 7 Service Pack 1 RC 1 (32 Bit)
- D Windows XP Service Pack 3 (32 Bit)
- D Windows XP Service Pack 2 (64 Bit)
- D Windows Vista Service Pack 2 (64 Bit)
- D Windows Vista Service Pack 2 (32 Bit)
- Microsoft Office 2007 Service Pack 1
- Microsoft Office Project 2007 Service Pack 1
- Microsoft Office Visio 2007 Service Pack 1

Sicherheit

- D Baseline Security Analyzer 2.1.1 (32 Bit)
- D Baseline Security Analyzer 2.1.1 (64 Bit)
- D Microsoft Fix-it Center
- Microsoft Security Essentials 2.0 (Vista/7 32 Bit)
- Microsoft Security Essentials 2.0 (Vista/7 64 Bit)
- Microsoft Security Essentials 2.0 (XP 32 Bit)
- D Tool zum Entfernen bösartiger Software (32 Bit)
- D Tool zum Entfernen bösartiger Software (64 Bit)
- Personal Vibe 2.0.0.0
- Promqry UI 1.0
- Rootkit Revealer 1.71
- Windows Defender 1593 (32 Bit)
- Windows Defender 1593 (64 Bit)
- D Windows Steady State 2.5

Powertoys

- Alt-Tab Replacement 1.0
- CD Slide Show Generator 1.0
- Cleartype Tuner Powertoy 1.0
- Color Control Panel Applet
- HTML Slide Show Wizard 6.0
- Image Resizer 1.0
- Open Command Window Here 1.0
- Power Calculator 1.0
- D RAW Image Thumbnailer and Viewer 1.0
- Synctoy 2.1 (32 Bit)
- Synctoy 2.1 (64 Bit)
- Taskbar Magnifier 1.0
- Tweak UI 2.10
- Virtual Desktop Manager 1.0
- Webcam Timershot 1.0

www.books 2.0

Sysinternals Suite

- Access Chk 5.0
- Access Enum 1.32
- AD Explorer 1.42
- Ad Restore 1.1
- Autologon 3.00
- Autoruns 10.06
- Bg Info 4.16
- Cache Set 1.0
- Clock Res 2.0
- Contig 1.55
- Core Info 2.11
- Ctrl 2 Cap 2.0
- Debug View 4.76
- Desktops 1.02
- Disk 2 VHD 1.63
- Disk Ext 1.1
- Disk Mon 2.01
- Disk Usage 1.34
- Disk View 2.4
- EFS Dump 1.02
- Handle 3.42
- Hex 2 Dec 1.0
- Junction 1.06
- LDM Dump 1.02
- List DLLs 2.25
- Live Kd 5.0
- Load Order 1.0
- Logon Sessions 1.21
- NTFS Info 1.0
- Page Defrag 2.32
- Pend Moves 1.1
- Portmon 3.02
- Proc Dump 3.0
- Process Explorer 14.01
- Process Monitor 2.93
- Proc Features 1.1
- Ps Exec 1.98
- Ps File 1.02
- Ps Get SID 1.44
- Ps Info 1.77
- Ps Kill 1.13
- Ps List 1.28
- Ps Logged On 1.33
- Ps Log List 2.71
- Ps Passwd 1.22
- Ps Service 2.24
- Ps Shutdown 2.52
- Ps Suspend 1.06
- Reg Del Null 1.1
- Reg Jump 1.01
- Rootkit Revealer 1.71
- Sdelete 1.51
- Share Enum 1.6
- Shell Runas 1.01
- Sig Check 1.71
- Streams 1.56
- Strings 2.41
- Sync 2.0
- TCP View 3.02
- VM Map 3.01
- Volume ID 2.0
- Whois 1.01
- Winobj 2.21
- Zoom It 4.1

Utilities

- .NET Framework 1.1 Redistributable Package
- .NET Framework 2.0 Redistributable Package
- .NET Framework 3.0 Redistributable Package
- .NET Framework 3.5
- D .NET Framework 4
- Active Sync 4.5
- D Agent (Genie)
- D Agent (Merlin)
- D Agent (Peedy)
- D Agent (Robby)
- D Application Watcher
- D Calculator Plus
- D Customized Task Manager
- Debug Diagnostic Tool 1.1 (32 Bit)
- Debug Diagnostic Tool 1.1 (64 Bit)
- D Devcon
- D Enhanced Event Log Viewer
- D Enhanced Task Bar Explorer
- D File System Explorer
- D Font Properties Extension 2.30
- D Framework Checker
- Group Bar 1.3.0.0
- D Joulemeter 1.0 Alpha
- Microsoft Deployment Toolkit 2010 1.0
- Microsoft Egypt Nile Theme 1.0
- Microsoft Hardware-Assisted Virtualization Detection 1.0
- D Microsoft Product Support Reports 1.2 (32 Bit)
- D Microsoft Product Support Reports 1.3 (64 Bit)
- Microsoft Scalable Fabric 1.1
- D Microsoft Speed Launch
- Microsoft USB Flash Drive Manager (Standard) 1.0.0
- D Microsoft Virtual CD-ROM Control Panel 2.1
- D Microsoft Virtual PC 2007 SP1 6.0.192.0 (32 Bit)
- D Microsoft Virtual PC 2007 SP1 6.0.192.0 (64 Bit)
- Microsoft XML Paper Specification Pack 1.2 (XP)
- Microsoft XML Paper Specification Pack 1.2 (Vista)
- Outlook-Add-In: Sicherung für Ordner 1.0 1.0
- D Snarf 1.7.005
- D Software Certification Toolkit (32 Bit)
- D Software Certification Toolkit (64 Bit)
- D Timezone 2.1
- D Tweakomatic 1.0
- User Profile Deletion Utility 5.2.3790.1060
- D User State Migration Tool 2.6.2 (32 Bit)
- D User State Migration Tool 2.6.2 (64 Bit)
- Windows Live Essentials
- D Windows Memory Diagnostic
- Windows Power Shell 1.0
- Windows Vista Upgrade Advisor 1.0
- XML-Notepad 2007 2.5

Internet und Netzwerk

- Internet Explorer 9 (32 Bit)
- Internet Explorer 9 (64 Bit)
- Microsoft Location Finder 2.0.1
- Microsoft Network Monitor 3.4 (32 Bit)
- Microsoft Network Monitor 3.4 (64 Bit)
- D Port Reporter 1.01
- Snip IT Add-On for Internet Explorer 1.0.1
- D Virtual Wifi 1.0
- Windows Desktop Search for Networks 1.0.1.0
- Windows Desktop Search for Internet Explorer 1.0.1.0
- Windows Search für XP 4.0
- Windows Search für Vista 4.0

Anwendungen

- Deep Zoom Composer 1.0.1945.1
- Excel Viewer 2003
- HD Photo Plug-in for Adobe Photoshop 1.0
- Jet Stream 1.1
- Microsoft Easy Camera Calibration Tool 1.0
- Microsoft Image Composite Editor 1.35 (32 Bit)
- Microsoft Image Composite Editor 1.35 (64 Bit)
- Microsoft Mathematics 2.0.040811.01
- D Microsoft Office – Entfernen verborgener Daten 1.1
- Microsoft Office 2007 Add-in Save as PDF or XPS 1.0
- Microsoft Office Compatibility Pack 3.0
- Microsoft Office SharePoint Designer 2007 SP1
- Microsoft Outlook Connector 4.0
- D Microsoft Photo Story 3 for Windows XP 3.0
- Microsoft Pro Photo Tools 2.0
- D Photosynth Plug-in for Photoshop 1.0
- Powerpoint Viewer 2007 1.0
- Video Cube 1.1
- D Visual Basic 2010 Express
- D Visual C# 2010 Express
- D Visual C++ 2010 Express
- D Visual Studio 2010 Express Editions
- D Visual Web Developer 2008 Express Edition
- Windows Media Player für Windows XP 11.0
- Windows Movie Maker für Vista 2.6
- D Windows XP Power Toys Video Screensaver
- D Windows XP Video Decoder Checkup Utility
- Word Viewer 1.0

www.books 2.0

Alle -Programme finden Sie auf der Heft-DVD im Microsoft Software Center. Alle D-Programme laden Sie aus dem Internet nach.

Die 10 besten WLAN-Tools

Die nützlichen Programme spüren Hotspots auf, ermitteln den besten Standort für Ihre WLAN-Geräte, messen die Geschwindigkeit und sorgen für Sicherheit in drahtlosen Netzwerken.

Ganz gleich ob Netbook, Notebook, Smartphone oder Internetradio: Immer mehr Geräte gehen per WLAN ins Internet.

Auf den folgenden Seiten finden Sie zehn kostenlose Spezial-Tools, die Informationen auslesen, Hotspots aufspüren und den Datendurchsatz messen. Zudem lassen sich vergessene WLAN-Passwörter auslesen und unverschlüsselte Verbindungen sichern. Auch lässt sich Ihre Wohnung hinsichtlich der Signalstärken vermessen.

Adapter Watch 1.05

Das Tool liest nützliche Infos zu Netzwerkadaptern aus wie MAC-Adresse und Chipsatz.

Mit Adapter Watch 1.05 lassen sich Details zu Ihren Netzwerkkarten und anderen Netzwerkadaptern anzeigen (kostenlos, www.nirsoft.net/utils/awatch.html und auf).

Wenn Sie etwa auf der Suche nach einem passenden Netzwerktreiber oder einem Update sind, ist es wichtig zu wissen, welcher Chipsatz verbaut ist.

Kompakt

- *Alle Tools gibt es kostenlos im Internet. Die meisten Utilities sind auch auf Heft-DVD.*

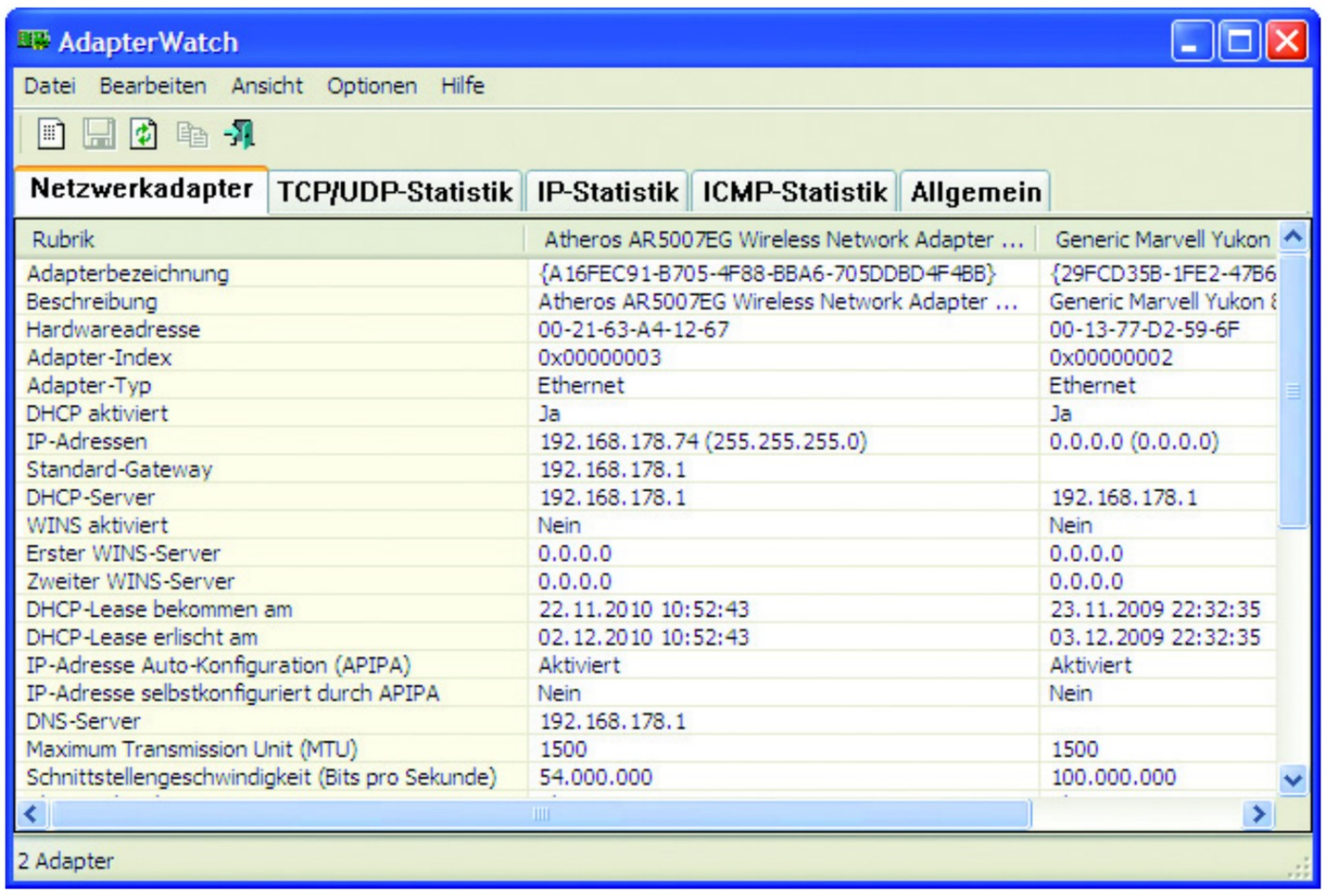
Zudem verrät Adapter Watch die MAC-Adresse des Geräts, also die eindeutige ID, sowie die aktuelle IP-Adresse (Bild A). Auch der Datendurchsatz wird ausgewertet. Außerdem lassen sich mit der Software über den DHCP-Server

Inhalt

Die 10 besten WLAN-Tools

- Adapter Watch 1.05 S. 78
- Capsa Free Edition 7.4 S. 79
- Ekahau Heatmapper 1.02 S. 80
- Hotspot Shield 1.571 S. 80
- Inssider 2.0 S. 81
- Netspeed Monitor 2.5.4.0 S. 82
- Net Surveyor 2.0 S. 82
- RK-WLAN-Keygen 1.4 S. 82
- Wefi 4.0.1.0 S. 83
- Wireless Keyview 1.34 S. 83

So geht's: Ekahau Heatmapper 1.02 S. 79
Software-Übersicht S. 80
So geht's: Inssider 2.0 S. 81
So geht's: RK-WLAN-Keygen 1.4 S. 82



Adapter Watch 1.05: Das Tool liest wichtige Informationen über Ihren Netzwerkadapter aus. Die helfen etwa bei Treiber-Updates und Netzwerkproblemen (Bild A)

bezogene IP-Adressen wechseln. Dazu wählen Sie „Datei, IP-Adresse frei setzen" und klicken anschließend auf „erneuern". Dies ist zum Beispiel bei manchen Tauschbörsen nützlich, um Download-Limits zu umgehen.

Der Befehl „Ansicht, HTML-Bericht aller Einträge erstellen" erzeugt eine HTML-Datei mit einem ausführlichen Bericht. Adapter Watch ist portabel.

Capsa Free Edition 7.4

Das Analyse-Tool untersucht Ihr Netzwerk bis hinunter auf die Ebene einzelner Pakete.

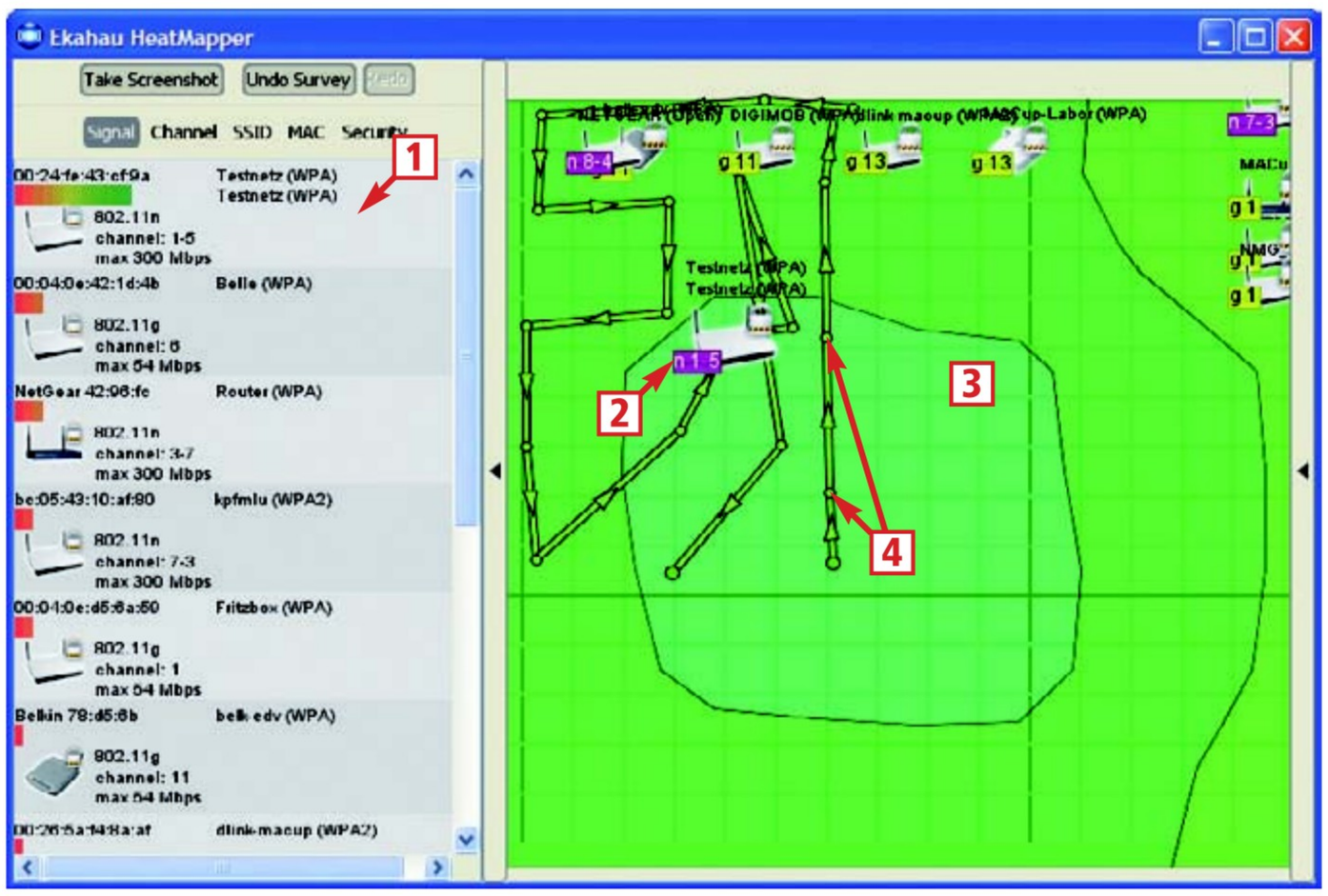
Capsa Free Edition 7.4 ist ein multifunktionelles Analyseprogramm (kostenlos, www.colasoft.com/capsa/capsa-free-edition.php). Es erfordert vor dem Download eine Registrierung.

Die Software ist recht vielschichtig und komplex. Am besten sehen Sie sich deshalb zu Beginn die verschiedenen Szenarien an, die auf der Webseite www.colasoft.com/capsa/features.php ▶

www.obooks 2.0

So geht's: Ekahau Heatmapper 1.02

Ekahau Heatmapper 1.02 misst die Signalstärken in Ihrer Wohnung (kostenlos, www.ekahau.com/products/heatmapper/products/overview.html). Damit finden Sie den besten Standort für Ihre WLAN-Geräte.



1 Signal
Die Liste der Funknetze ist nach Signalstärke sortiert.

2 Ausgewähltes Netz
Das Router-Symbol des angezeigten Netzes steht in der Mitte.

3 Dunkelgrüner Bereich
Hier ist der Empfang am besten.

4 Messpunkte
An jedem Messpunkt erfasst das Programm die Signalstärke.

beschrieben sind – allerdings nur auf Englisch.

Nach dem Start wählen Sie bei „Adapter“ die zu überwachende Netzwerkverbindung aus. Im unteren Bereich wählen Sie beispielsweise „Full Analysis“ und klicken anschließend auf das Symbol mit dem weißen Pfeil. Es erscheint die Analyse-Ansicht mit zahlreichen Reitern (Bild B).

„Dashboard“ zeigt Grafiken von Traffic-Analysen. „Protocol“ listet die Daten nach Netzwerkprotokollen unterteilt auf. „Matrix“ erstellt eine grafische Übersicht der Internetverbindungen, und „Packet“ führt Sie hinunter bis auf die Ebene der einzelnen Netzwerkpakete. Im Reiter „Log“ schließlich finden Sie eine Liste aller Internetverbindungen.

Über das Kontextmenü lassen sich die meisten Analysen exportieren.

Software-Übersicht

Programm	Quelle	Seite
Adapter Watch 1.05 (Liest Adapter-Infos aus)	www.nirsoft.net/utils/awatch.html	78
Capsa Free Edition 7.4 (Tiefen-Analyse von Netzwerken)	www.colasoft.com/capsa/capsa-free-edition.php	79
Ekahau Heatmapper 1.02 (Misst Signalstärken)	www.ekahau.com/products/heatmapper/overview.html	80
Hotspot Shield 1.571 (VPN-Tunnel)	www.hotspotshield.com	80
Inssider 2.0 (WLAN-Sniffer)	www.metageek.net/products/inssider	81
Netspeed Monitor 2.5.4.0 (Traffic-Analyse)	www.floriangilles.de/software/netspeedmonitor	82
Net Surveyor 2.0 (WLAN-Spürhund)	www.nutsaboutnets.com	82
RK-WLAN-Keygen 1.4 (Schlüsselgenerator)	http://members.aon.at/knapp	82
Wefi 4.0.1.0 (Findet Hotspots)	www.wefi.com	83
Wireless Keyview 1.34 (Liest WLAN-Schlüssel aus)	www.nirsoft.net/utils/wireless_key.html	83

Alle -Programme finden Sie auf Heft-DVD in der Rubrik „Security-Tools, WLAN-Tools“.

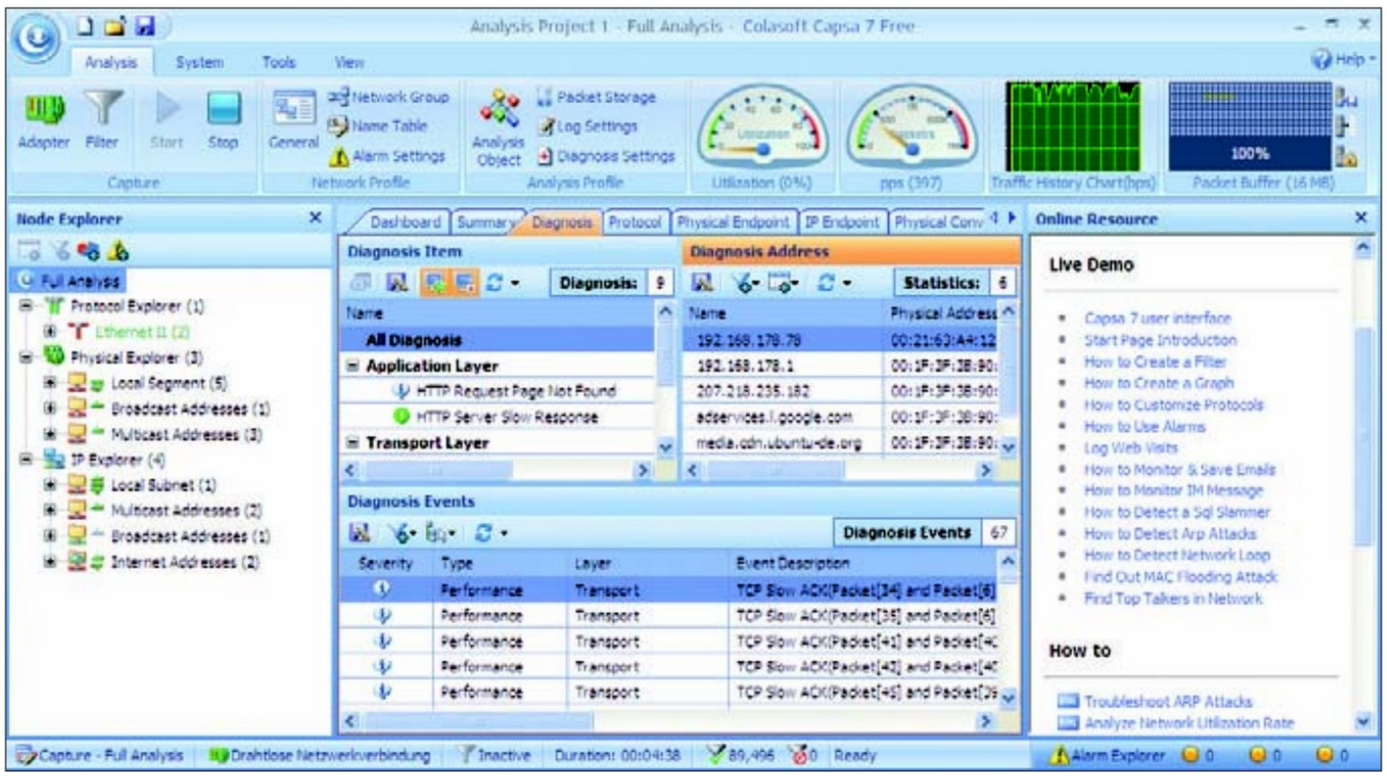
Ekahau Heatmapper 1.02

Das Tool misst Signalstärken und findet den perfekten Standort für Ihre WLAN-Geräte.

Die Leistung des Funknetzes variiert je nach Standort mitunter erheblich. Ekahau Heatmapper 1.02 zeigt Ihnen, wo in Ihrer Wohnung der WLAN-Empfang am besten ist und wo er weniger gut ist (kostenlos, www.ekahau.com/products/heatmapper/overview.html).

Falls vorhanden, laden Sie nach dem Start des Tools einen Grundriss Ihrer Wohnung, ansonsten verwenden Sie das einfache Gitternetz des Tools.

Nun bewegen Sie sich langsam mit Ihrem WLAN-Gerät durch Ihre Wohnung und klicken regelmäßig mit der Maus auf die Karte. Heatmapper misst bei jedem Klick die Signalstärke und markiert den Standort. Sobald Sie in jedem Winkel waren, schließen Sie die Messung mit einem Klick mit der rechten Maustaste ab. Heatmapper erstellt daraufhin eine grafische Übersicht. Grüntöne bedeuten guter Empfang, Gelb und Rot weisen auf einen schlechten Empfang hin.



Capsa Free Edition 7.4: Das komplexe Programm erfordert etwas Einarbeitung, wertet dann aber restlos alle Daten Ihres Netzwerks aus (Bild B)

Hotspot Shield 1.571

Schützt Ihren PC, wenn Sie über einen unverschlüsselten Hotspot online gehen.

Zwar sind öffentliche WLAN-Hotspots eine feine Sache, um unterwegs im Internet zu surfen, Ihr Rechner ist dabei aber nicht gesichert.

Hotspot Shield 1.571 richtet einen verschlüsselten VPN-Tunnel zu einem Server in den USA ein (kostenlos, www.hotspotshield.com und auf). Das Tool überträgt dann die Datenkommunikation zwischen Ihrem PC und dem VPN-Server über einen Tunnel (Bild C).

Somit können Ihre Daten von niemandem mitgelesen werden. Das Tool verhindert, dass Schnüffler und Hacker private Daten abfangen.

Hotspot Shield ist kostenlos. Bei der Installation bekommen Sie eine Browser-Toolbar angeboten. Es empfiehlt sich, diese nicht zu installieren. Entfernen Sie daher das Häkchen bei „Include the Hotspot Shield Toolbar (recommended)“. Am besten löschen Sie auf der folgenden Seite auch alle Häk-

WiWobooks 2.0

chen. Sie verhindern damit auch, dass Ihr Browser eine neue Startseite erhält.

Ob Hotspot Shield und damit der Schutz aktiv ist, erkennen Sie an dem Icon im System-Tray, über das Sie das Programm auch steuern. Wenn das Icon rot ist, dann surfen Sie ganz normal über Ihre Internetverbindung. Wenn es grün ist, dann surfen Sie über den gesicherten VPN-Tunnel. Um Hotspot Shield ein- oder auszuschalten, klicken Sie das Icon mit der rechten Maustaste an und wählen „Verbinden/EIN“ beziehungsweise „Trennen/AUS“.

Hotspot Shield 1.571: Ein VPN-Tunnel macht auch unverschlüsselte Verbindungen abhörsicher (Bild C)

Inssider 2.0

Der WLAN-Sniffer analysiert alle verfügbaren Funknetze in Ihrer Umgebung.

Inssider 2.0 zeigt detaillierte Echtzeit-Informationen zu allen Funknetzen in der näheren Umgebung an (kostenlos, www.metageek.net/products/inssider). Inssider ist der Nachfolger von Netstumbler, das nicht mehr weiterentwickelt wird.

Das Tool sucht nach dem Start automatisch nach drahtlosen Netzen und zeigt Funkparameter wie SSID, Kanal und Verschlüsselungsart an, falls möglich auch die Geo-Koordinaten und den Zeitpunkt, zu dem Inssider den Access-Point zum ersten Mal und zuletzt gefunden hat.

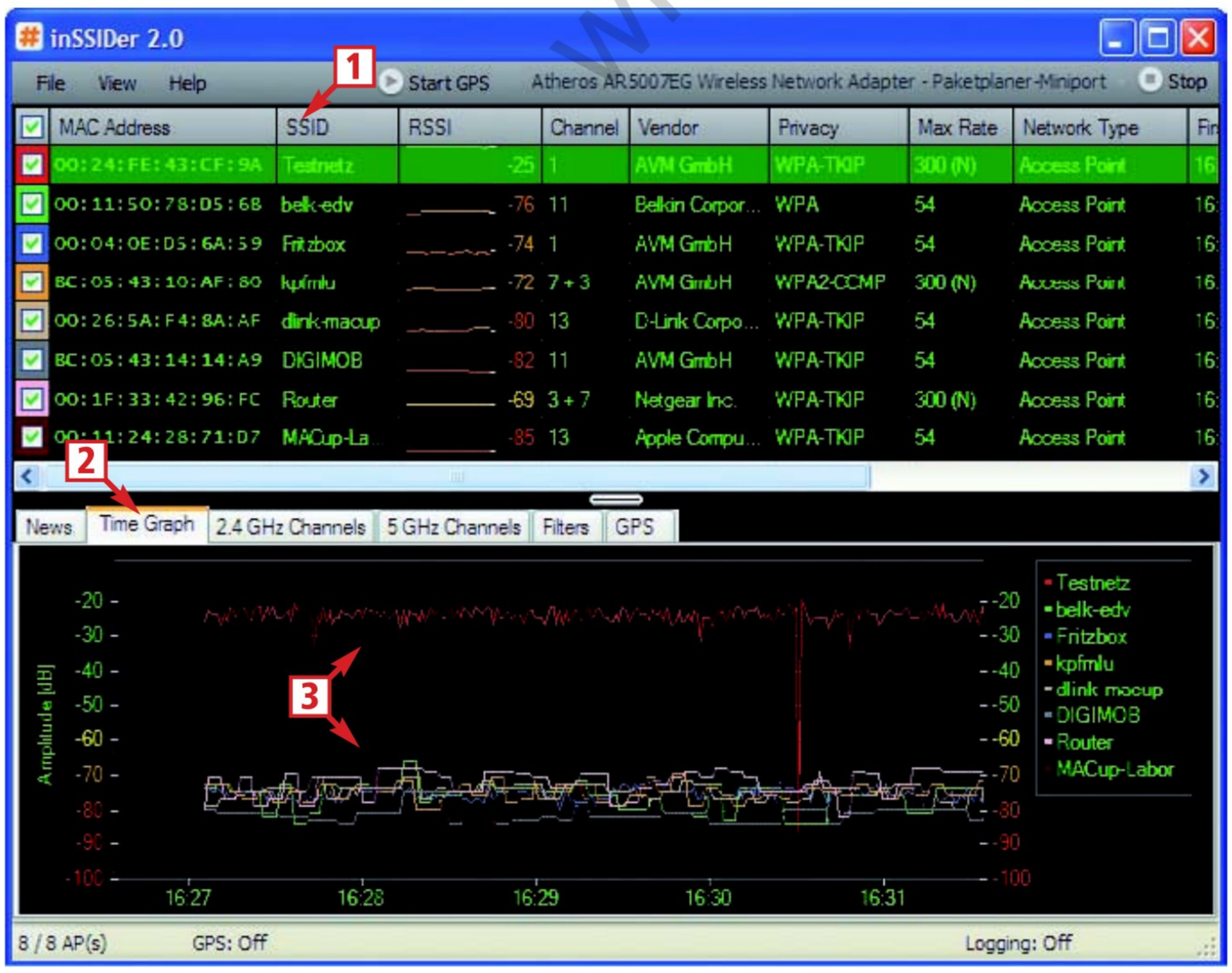
Über die verschiedenen Reiter sehen Sie Messungen der Signalstärken in Echtzeit und erfahren, welches Funknetz welchen Kanal verwendet. Wenn mehrere Funknetze den gleichen Kanal benutzen, dann kommt es oft zu Störungen. Wechseln Sie in diesem Fall mit Ihrem WLAN zu einem Kanal, der nicht genutzt wird.

Die verschiedenen Tabellen und Grafiken lassen sich direkt in die Zwischenablage kopieren und somit auch in anderen Programmen wie Excel nutzen. Hinweis: Inssider benötigt das Microsoft .NET Framework 2.0. ▶

www.obooks2.0

So geht's: Inssider 2.0

Inssider 2.0 spürt Funknetze in der Nachbarschaft auf und analysiert sie (kostenlos, www.metageek.net/products/inssider). Das Tool zeigt Netzparameter wie SSID, Kanal und Verschlüsselungsart an und misst die Empfangsstärke in Echtzeit.



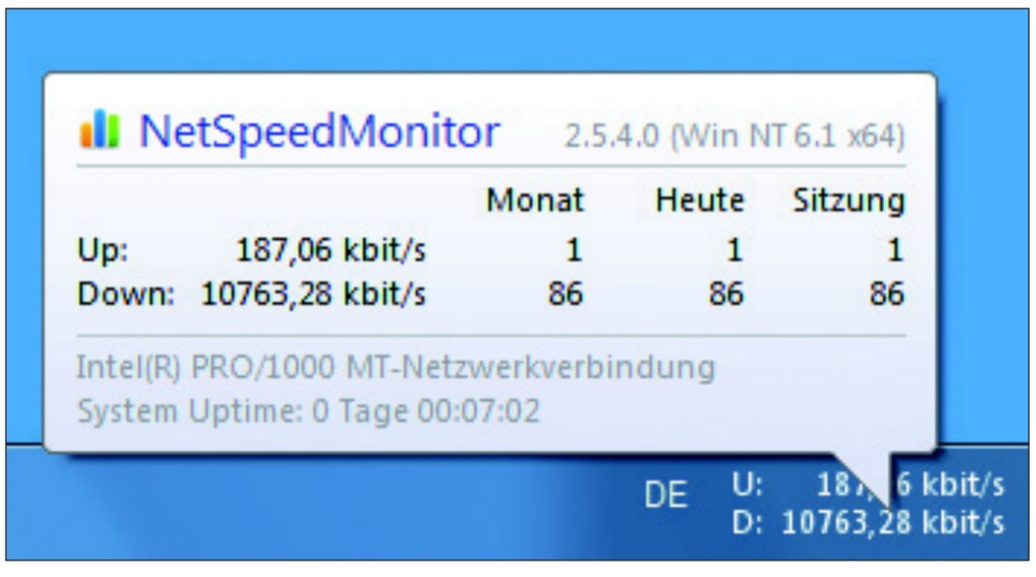
1 SSID
Hier sehen Sie die Liste der aufgespürten Funknetze.

2 Time Graph
Zeigt die Signalstärke der Funknetze in Echtzeit.

3 Messwerte
Je größer der Wert, desto besser ist der Empfang.

Netspeed Monitor 2.5.4.0

Das Tool misst das Tempo Ihres Funknetzes und speichert die Werte in einer Datenbank.



Netspeed Monitor 2.5.4.0: Das Tool misst die Up- und Download-Geschwindigkeit und zeigt die Werte in der Taskleiste an (Bild D)

Netspeed Monitor 2.5.4.0 misst den Up- und Download-Traffic Ihres Netzwerks und zeigt dessen Werte in Echtzeit in der Taskleiste an (kostenlos, www.floriangilles.de/software/netspeedmonitor). Damit merken Sie auch schnell, ob ein Programm online geht.

Um die Geschwindigkeitsmessung zu aktivieren, klicken Sie mit der rechten Maustaste auf die Taskleiste und aktivieren bei „Symbolleisten" den Eintrag „NetSpeedMonitor". Sie sehen nun in Echtzeit das Up- und Download-Tempo in der Taskleiste eingeblendet (Bild D). Wenn Sie mit dem Mauszeiger über die Messwerte fahren, dann öffnet sich ein Pop-up mit dem Gesamtdatenverkehr – unterteilt in Monat, Tag und Sitzung. Diese Werte speichert das Tool in einer Datenbank, die Sie im Kontextmenü über „Datenverkehr" erreichen.

Net Surveyor 2.0

Der WLAN-Scanner wertet die Eigenschaften von aufgespürten Funknetzen grafisch aus.

Net Surveyor 2.0 sammelt Infos zu allen verfügbaren Hotspot-Quellen und stellt diese grafisch dar (kostenlos, www.nutsaboutnets.com und auf).

Die Daten werden in Echtzeit gesammelt und in verschiedenen Grafiken dargestellt. Damit sehen Sie auch, an welchem Standort Sie den besten Empfang haben.

Außerdem bietet Net Surveyor zahlreiche Informationen, die das Einrichten drahtloser Netzwerke erleichtern, zum Beispiel Signalstärken, Kanalbelegungen und Übertragungsraten (Bild E). Auf Wunsch generiert das Programm Berichte im PDF-Format.

RK-WLAN-Keygen 1.4

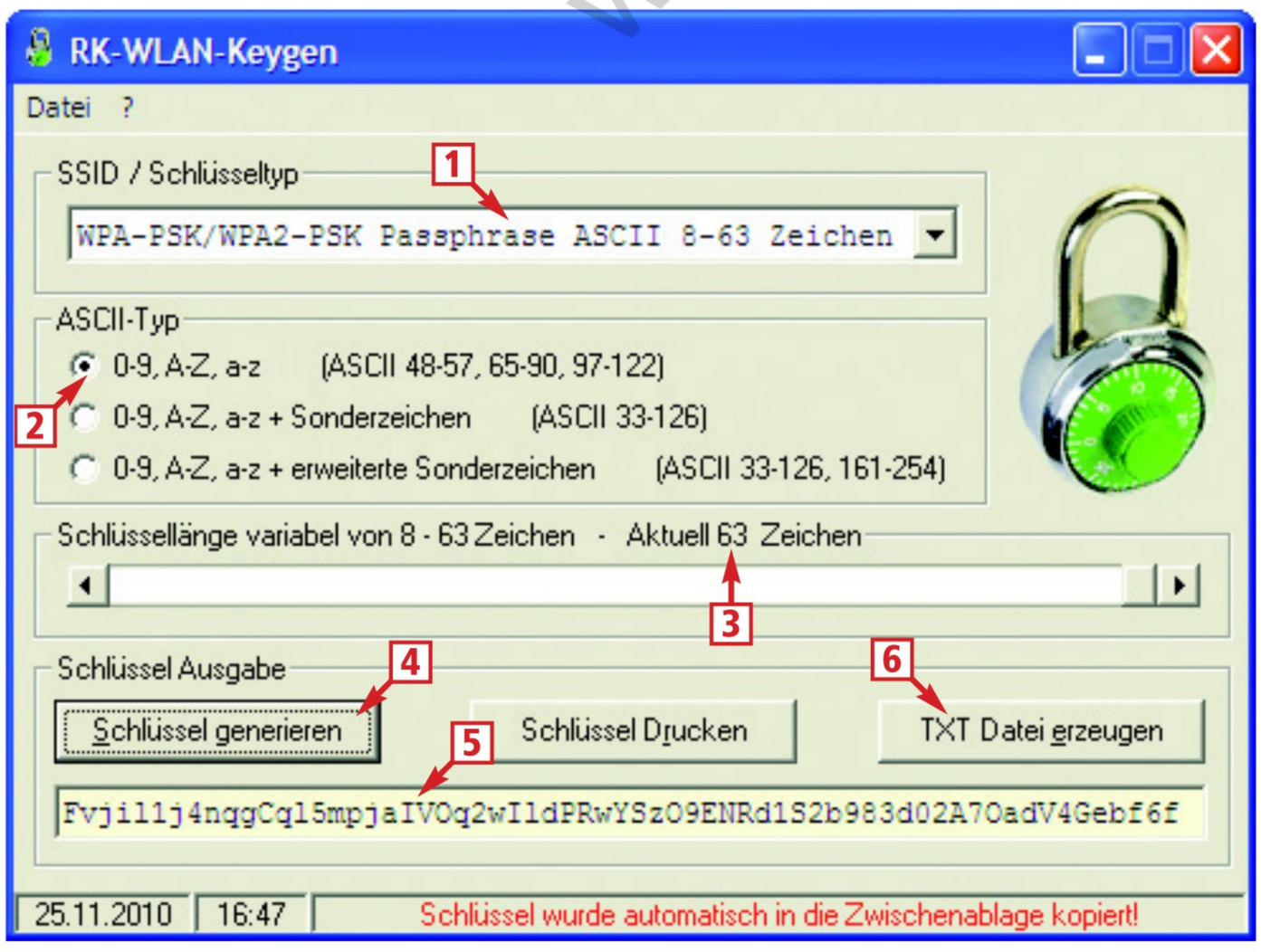
Das Tool erzeugt zufällige WLAN-Schlüssel, die kein Hacker knackt.

Der einzige sichere Verschlüsselungsstandard für WLAN ist WPA2. Ein kurzes Passwort lässt sich aber mit Spezial-

winobooks 2.0

So geht's: RK-WLAN-Keygen 1.4

RK-WLAN-Keygen 1.4 erzeugt zufällige, unknackbare WLAN-Schlüssel (kostenlos, http://members.aon.at/knapp und auf). Sie geben dabei den Zeichensatz und die gewünschte Schlüssellänge vor.



1 Schlüsseltyp
Hier stellen Sie Typ und Länge des Schlüssels ein …

2 ASCII-Typ
… und hier den Zeichensatz.

3 Schlüssellänge
Der Schlüssel sollte 63 Zeichen lang sein.

4 Schlüssel generieren
Ein Klick erzeugt den zufälligen Schlüssel.

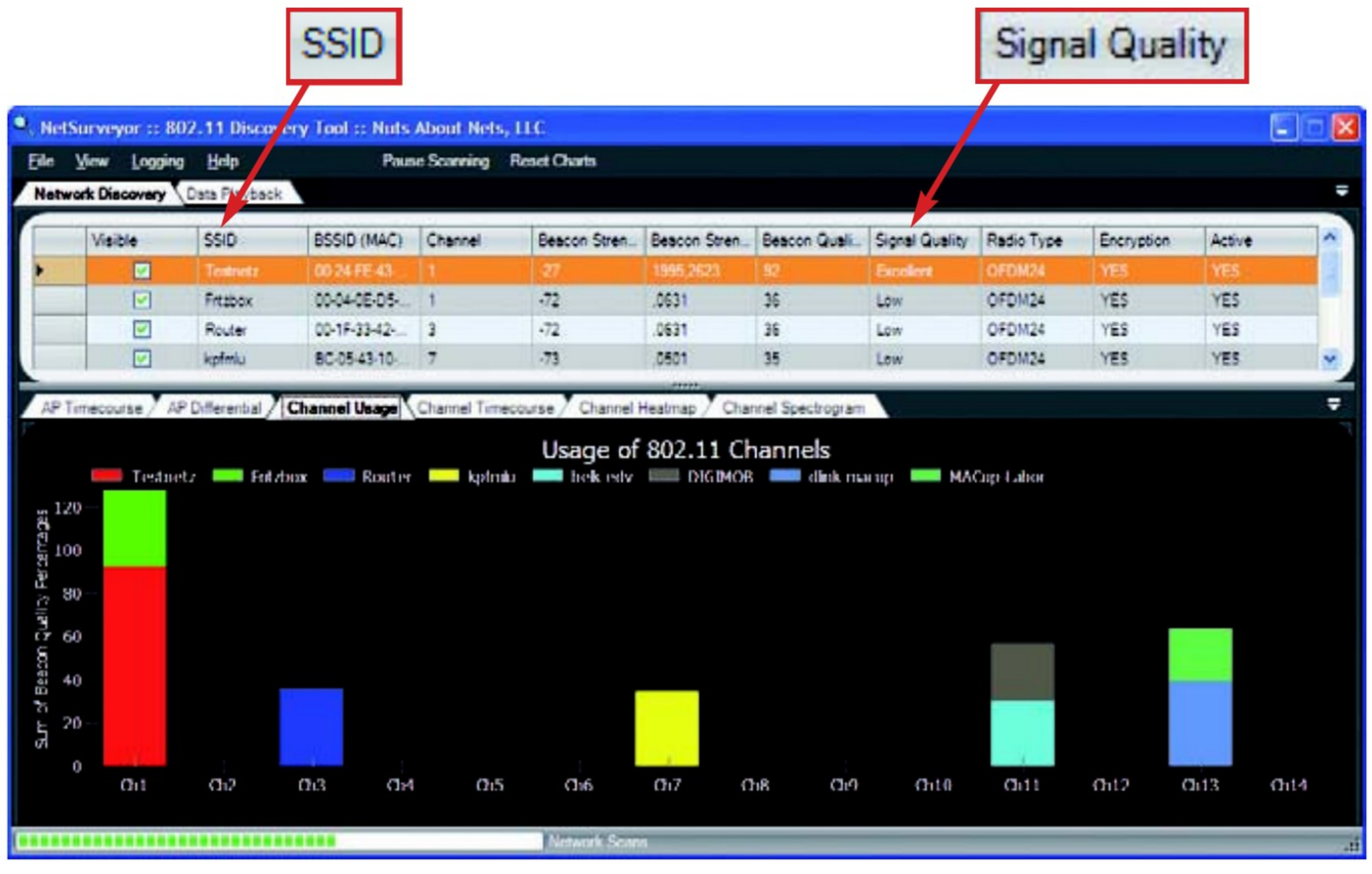
5 Schlüssel
Der generierte Schlüssel befindet sich auch in der Zwischenablage.

6 TXT Datei erzeugen
Der Button speichert den Schlüssel in einer Textdatei.

Tools schnell knacken. RK-WLAN-Keygen 1.4 schützt gegen Datendiebe, indem es auf Knopfdruck zufällige, komplexe Schlüssel erzeugt (kostenlos, http://members.aon.at/knapp und auf).

Wählen Sie nach dem Start unter „SSID/Schlüsseltyp“ den Eintrag „WPA-PSK/WPA2-PSK Passphrase ASCII 8-63 Zeichen“ aus. Aktivieren Sie dann bei „ASCII-Typ“ die erste Option und stellen Sie mit dem Schieberegler die Schlüssellänge auf 63 Zeichen. Ein Klick auf „Schlüssel generieren“ erstellt nun einen 63 Zeichen langen WPA2-Schlüssel, den mit den heutigen Mitteln niemand knacken kann.

Eine Kopie des erzeugten Schlüssels landet automatisch in der Zwischenablage und lässt sich damit leicht in die Router-Konfiguration kopieren.



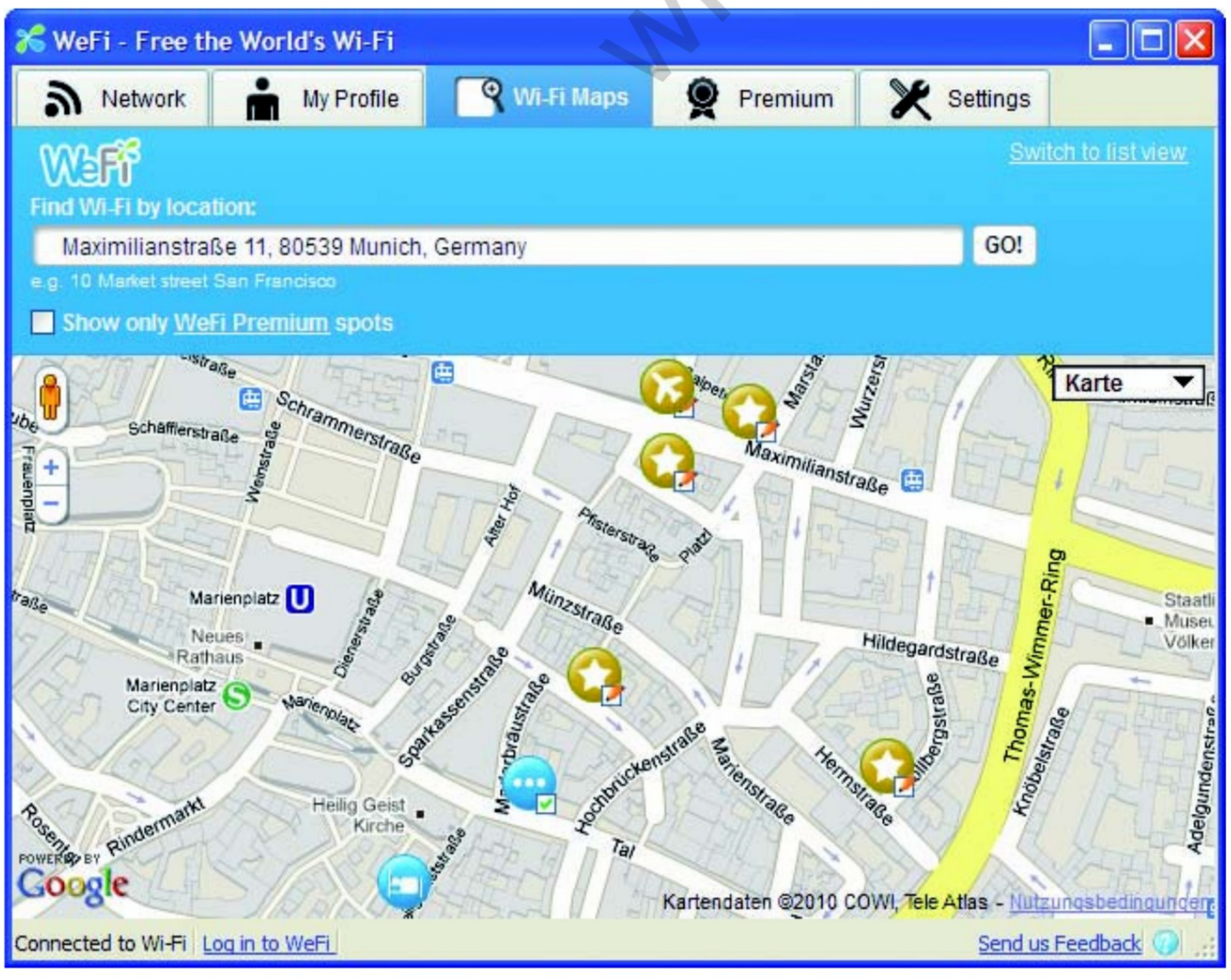
Net Surveyor 2.0: Oben sehen Sie die Eigenschaften der gefundenen Funknetze. Unten sehen Sie, welches Funknetz welchen Kanal belegt (Bild E)

Wefi 4.0.1.0

Wefi kennt Tausende Hotspots und spürt neue auf.

Wefi 4.0.1.0 stellt Verbindungen mit offenen WLAN-Netzen her (kostenlos, www.wefi.com). Das Programm sucht automatisch nach öffentlichen Hotspots, etwa in Hotels, Cafés oder auf Flughäfen.

Nach dem Start meldet Wefi 4.0.1.0 sämtliche WLAN-Netze in Reichweite und speichert auf Wunsch die Zugangsdaten. Wenn Sie später erneut im Empfangsbereich sind, dann verbindet sich Wefi automatisch mit dem entsprechenden Hotspot. Im Reiter „We-Fi Maps“ sehen Sie einen Stadtplan von Google Maps mit den Hotspots (Bild F).



Wefi 4.0.1.0: Auf der Karte sind alle Hotspots markiert, die das Programm kennt (Bild F)

Wireless Keyview 1.34

Das praktische Werkzeug liest vergessene WLAN-Kennwörter aus.

Ein sicherer WLAN-Schlüssel muss lang und kryptisch sein. Wenn Sie ihn einmal vergessen, kommen Sie mitunter nicht mehr ins Internet. Der Schlüssel ist aber auf Ihrem Rechner gespeichert und lässt sich auslesen.

Windows XP speichert jeden WLAN-Schlüssel in der Registry, während Vista ihn verschlüsselt im Dateisystem ablegt. Windows 7 verwendet das Windows Data Protection System.

Bei Windows XP und Vista liest Wireless Keyview 1.34 alle lokal gespeicherten Schlüssel direkt aus (kostenlos, www.nirsoft.net/utils/wireless_key.html und auf).

Bei Windows 7 benötigen Sie Code Injection. Dazu wählen Sie in Wireless Keyview den Menüpunkt „File, Advanced Options“ und aktivieren dort die Option „Use code injection method (For Windows 7 only)“. Damit liest Wireless Keyview auch hier die Schlüssel aus. ■

Andreas Dumont
sonderheft@com-magazin.de

Weitere Infos

- http://wiki.uni-konstanz.de/wlan
  Umfangreiches Wissen zum Thema WLAN

WiWobooks 2.0

Der Rettungs-Stick 1.0.4

Beseitigen Sie fehlerhafte Software-Installationen, retten Sie wertvolle Daten und reanimieren Sie streikende Windows-PCs. Der Rettungs-Stick 1.0.4 bootet die wichtigsten Notfall-Systeme für Windows-PCs.

Ein nützliches com!-Tool macht aus Ihrem USB-Stick einen bootfähigen Rettungs-Stick mit den wichtigsten Notfall-Systemen (kostenlos, www.com-magazin.de und auf).

Damit starten Sie im Ernstfall den Reparaturdatenträger für Windows 7, bootfähige Virenscanner von Avira und Kaspersky, Windows-PE-Systeme wie die Ultimate Boot CD for Windows und andere Boot-Tools, zum Beispiel Parted Magic.

Näheres zum Reparaturdatenträger für Windows 7 lesen Sie im Artikel auf Seite 90.

Inhalt

Der Rettungs-Stick 1.0.4

- **Das müssen Sie wissen**
  - Wozu brauche ich den Rettungs-Stick? S. 84
  - Was benötige ich für die Installation? S. 84
  - Startet der Stick an jedem PC? S. 84
- **Vorbereitungen**
  - Reparaturdatenträger erstellen S. 85
  - Windows PE erstellen S. 86
- **Installation**
  - Stick vorbereiten S. 87
  - Stick installieren S. 87
- **Rettungs-Stick nutzen**
  - Rettungs-Stick booten S. 88
  - Reparaturdatenträger S. 88
  - Antivirus-Tools S. 88
  - Windows-Tools S. 88
  - Festplatten-Tools S. 89
  - Analyse-Tools S. 89

Der Rettungs-Stick: Die richtigen Tools für den Notfall S. 85

Software-Übersicht S. 86

So geht's: Die Ultimate Boot CD for Windows 3.60 S. 89

Kompakt

- *Der Rettungs-Stick 1.0.4 startet den Reparaturdatenträger für Windows 7, ein Mini-Windows, zwei Virenscanner und weitere Boot-Systeme.*

Das müssen Sie wissen

Der Rettungs-Stick bootet mehrere Notfall-Systeme für Windows-PCs.

Wozu brauche ich den Rettungs-Stick?

Der multibootfähige Rettungs-Stick (Bild A) hilft Ihnen, Ihren PC einer genaueren Prüfung zu unterziehen. Mit dem Avira Antivir Rescue System 3.6.9 und der Kaspersky Rescue Disk 10 stellt der Stick Ihnen zwei ausgezeichnete Virenscanner bereit. Der Vorteil dieser bootfähigen Virenscanner: Möglicherweise vorhandene Viren Ihres Windows-Systems sind während des Komplett-Scans nicht aktiv und lassen sich leichter aufspüren.

Der Rettungs-Stick ist aber auch dann hilfreich, wenn Ihr PC nicht mehr booten will. Bei solch einem Daten-GAU lässt sich der Rechner über den Rettungs-Stick starten, um nach einer fehlgeschlagenen Software-Installation Wiederherstellungpunkte zu aktivieren oder die komplette Windows-Installation durch ein Systemabbild zu restaurieren.

Was benötige ich für die Installation?

Für die Komplett-Installation benötigen Sie einen bootfähigen USB-Stick mit mindestens 2 GByte Speicherplatz. Das com!-Installationspaket übernimmt für Sie die Installation. Optional lassen sich über zusätzliche ISO-Dateien der Reparaturdatenträger für Windows 7 und Boot-CDs mit einem Mini-Windows einbinden. Wie Sie diese ISO-Dateien erhalten, lesen Sie im Abschnitt „Vorbereitungen".

Startet der Stick an jedem PC?

Der Rettungs-Stick startet an jedem PC, dessen BIOS das Booten vom USB-Stick unterstützt. Aufgrund der unterschied-

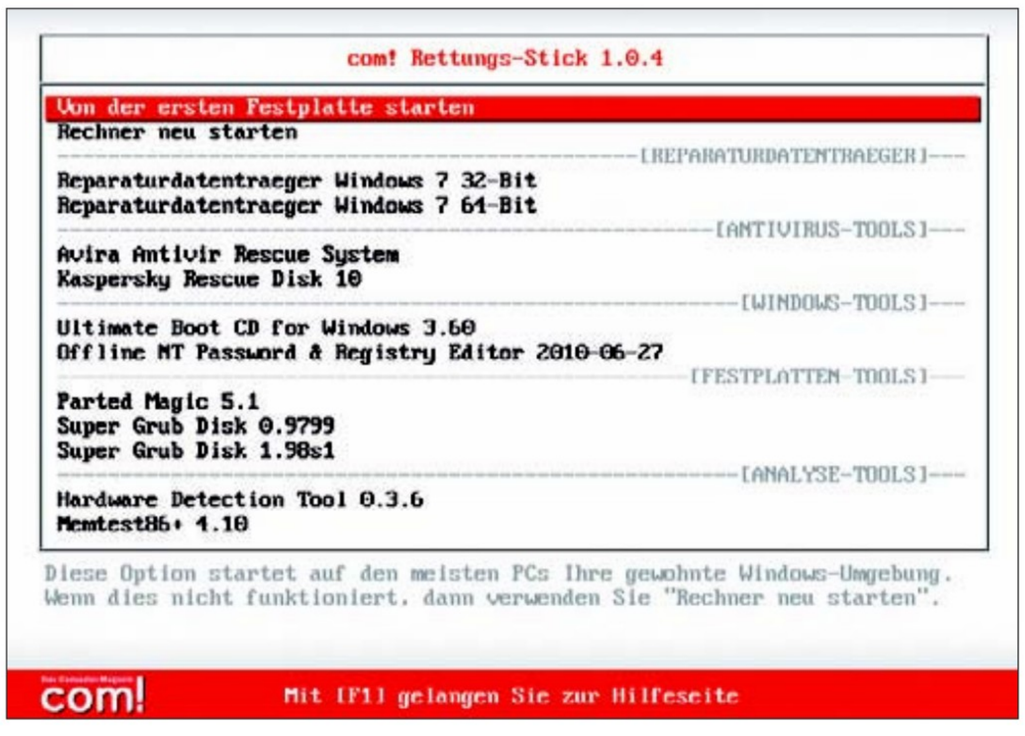
Infrarecorder Portable 0.52: Das Tool speichert den Reparaturdatenträger für Windows 7 als ISO-Datei (Bild B)

www.books 2.0

lichen Hardware-Komponenten kann es jedoch passieren, dass sich nicht jedes der Notfall-Systeme booten lässt. Zudem müssen Sie sich beim Booten von Notfall-Systemen mit einem Mini-Windows an langsameren PCs auf längere Startzeiten einstellen.

Vorbereitungen

In den Rettungs-Stick lassen sich zusätzliche ISO-Dateien einbinden, die Sie vor der Installation erstellen sollten.



Rettungs-Stick 1.0.4: Das multibootfähige Notfall-System startet Virenscanner und die wichtigsten Tools zur Rettung von Windows-PCs (Bild A)

Reparaturdatenträger erstellen

Unter Windows 7 lässt sich eine Notfall-CD brennen, die Ihnen hilft, Systemfehler zu beseitigen. Der Rettungs-Stick ist in der Lage, diesen Reparaturdatenträger vom USB-Stick zu booten. Dazu müssen Sie ein ISO-Abbild der Notfall-CD erstellen.

Wenn Sie unter Windows 7 noch keinen Reparaturdatenträger erstellt haben, dann halten Sie einen CD-Rohling bereit, klicken auf „Start, Systemsteuerung“ und wechseln mit „System und Sicherheit“ zu „Sichern und Wiederherstellen“. Im linken Fensterbereich klicken Sie auf „Systemreparaturdatenträger erstellen“ und folgen den Anweisungen.

Nachdem Sie den Reparaturdatenträger gebrannt haben, speichern Sie ein Abbild der CD als ISO-Datei. Dazu entpacken Sie das ZIP-Archiv von Infrarecorder Portable 0.52 in einen beliebigen Ordner Ihres PCs (kostenlos, http://infrarecorder.org und auf). ▶

www.books 2.0

Der Rettungs-Stick: Die richtigen Tools für den Notfall

Auf dem Rettungs-Stick 1.0.4 finden Sie zehn bootfähige Notfall-Systeme. Die Tabelle zeigt, welches System wir für bestimmte Rettungsaufgaben empfehlen.

	Windows-7-Reparaturdatenträger	Avira Antivir Rescue System	Kaspersky Rescue Disk 10	Ultimate Boot CD for Windows 3.60	Offline NT Password & Registry Editor	Parted Magic 5.2	Super Grub Disk 0.9799	Super Grub Disk 1.98s1	Hardware Detection Tool 0.3.6	Memtest86+ 4.10
Wiederherstellungspunkt aktivieren für Windows 7	●									
Systemabbild einspielen für Windows 7	●									
Windows-Registry bearbeiten				●						
Windows-Passwort zurücksetzen					●					
Viren finden und entfernen		●	●							
Spyware finden und entfernen				●						
Gelöschte Dateien wiederherstellen				●		●				
Gelöschte Partitionen wiederherstellen						●				
Dateien auf CD/DVD sichern				●						
Dateien auf Webserver sichern				●						
Notfall-Windows starten				●						
Partitionen kopieren / bearbeiten						●				
Festplatte kopieren						●				
Boot-Sektor reparieren für Windows XP / Vista				●						
Boot-Sektor reparieren für Windows 7	●									
Boot-Sektor reparieren für Grub							●	●		
Linux-Partition booten							●	●		
Arbeitsspeicher prüfen										●
Hardware-Informationen sammeln									●	
Hilfe im Internet suchen				●						

Danach legen Sie den Reparaturdatenträger in das CD-Laufwerk ein und starten Infrarecorder Portable, indem Sie die Datei „InfraRecorder.exe“ öffnen.

Klicken Sie auf die Schaltfläche „Read Disc“ (Bild B) und wählen Sie als „Quelle“ das Laufwerk mit dem Reparaturdatenträger aus. Klicken Sie anschließend auf die Schaltfläche hinter dem Eingabefeld „Image Datei“ und wählen Sie den Speicherort für die ISO-Datei. Wenn der Reparaturdatenträger für Windows 7 32 Bit bestimmt ist, dann verwenden Sie den Dateinamen `32win7.iso`, die Variante für 64-Bit-Systeme nennen Sie `64win7.iso`.

Windows PE erstellen

Ultimate Boot CD for Windows 3.60 erstellt auf Basis des Windows Preinstallation Environments (Windows PE) eine Notfall-CD (kostenlos, www.ubcd4win.com). Der Rettungs-Stick ist in der Lage, diese CD als ISO-Datei zu booten (Bild C). Um diese ISO-Datei zu erzeugen, benötigen Sie neben Ultimate Boot CD for Windows 3.60 lediglich eine Installations-CD für Windows XP SP2.

Ultimate Boot CD for Windows 3.60 erhalten Sie im Internet unter www.ubcd4win.com/downloads.htm. Klicken Sie auf „Mirror #1“ und dann auf „Download“. Nach Abschluss des Datentransfers starten Sie die Datei „UBCD4WinV360.exe“, um das Tool zu installieren.

Übernehmen Sie alle Standardvorgaben und klicken Sie nach Abschluss der Installation auf „Fertigstellen“, um das Tool zu starten. Sollte der Start fehlschlagen, dann klicken Sie das Desktop-Symbol „UBCD4Win“ mit der rechten Maustaste an und wählen „Als Administrator ausführen“.

Sobald die Programmoberfläche erscheint (Bild D), legen Sie die Installations-CD von Windows XP SP2 ein. Klicken Sie dann auf die Schaltfläche hinter dem Eingabefeld „Quelle“ und geben Sie den Pfad zur Installations-CD an. Danach ändern Sie bei „ISO-Image erstellen“ den Dateinamen auf `ubcd4win.iso`.

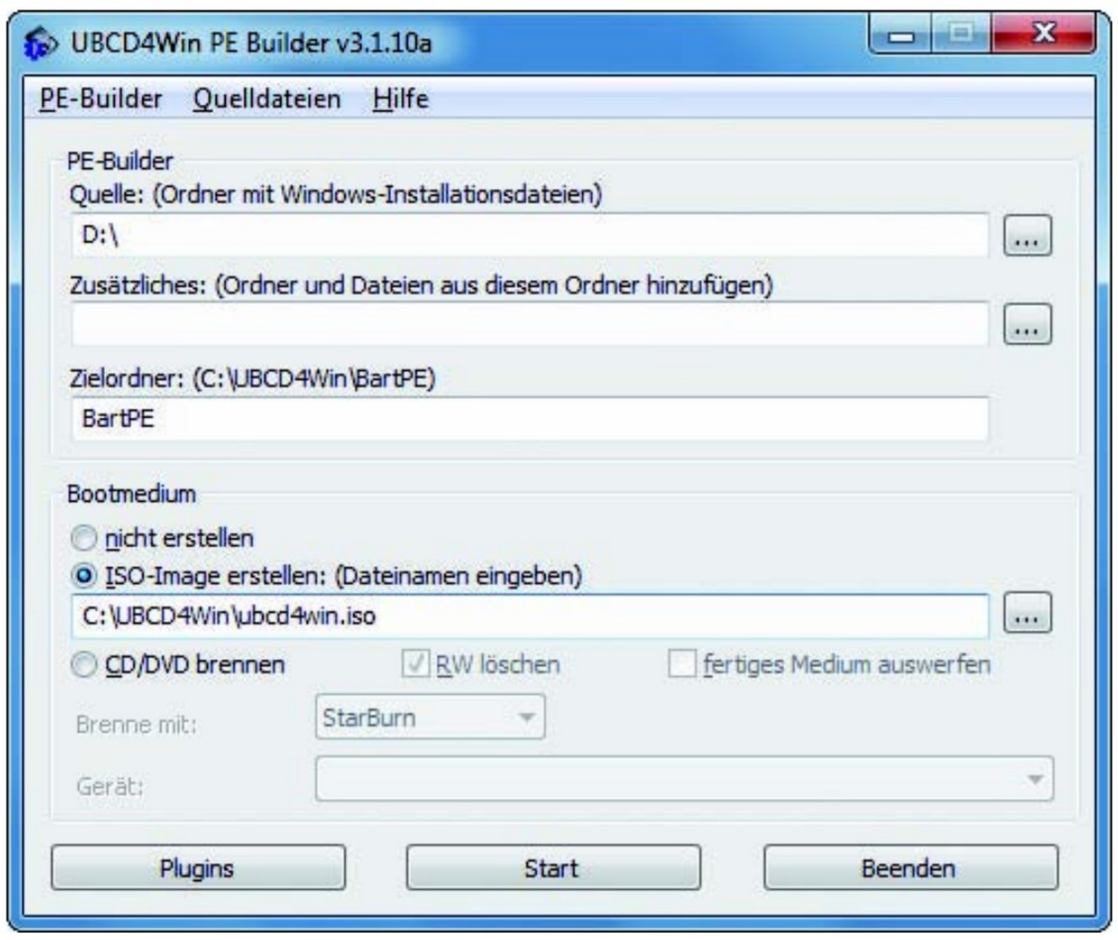
Die Schaltfläche „Plugins“ führt Sie zu einem Dialog, in dem sich die Ultimate Boot CD for Windows Ihren Bedürfnissen anpassen lässt. Eine Einstellung sollten Sie auf jeden Fall ändern. Damit das Windows-System der Notfall-CD mit dem deutschen Tastaturtreiber startet, passen Sie im Ordner „C:\UBCD4Win\plugin\!Critical\User Settings\“ die Datei „User-Settings.inf“ mit einem Editor wie Notepad an. Suchen Sie nach `Muti·Language·Keyboard·Support`. In diesem Bereich setzen Sie ein Semikolon vor die Zeile

```
0x1,·"Keyboard·Layout\Preload",·"1",·"00000409"·;
```

und entfernen dann das Semikolon und das Leerzeichen vor dieser Zeile:

```
;·0x1,·"Keyboard·Layout\Preload",·"1",·"00000407"·;
```

Nach dem Speichern der Datei genügt ein Klick auf „Start“, um Ihre Ultimate Boot CD for Windows zu erzeugen.



Ultimate Boot CD for Windows 3.60: Wenn diese Notfall-CD auf Ihren Rettungs-Stick soll, dann erstellen Sie mit diesem Tool die ISO-Datei der CD (Bild D)

Software-Übersicht

Programm	Internet	Seite
Avira Antivir Rescue System 3.6.9 (Virenscanner)	www.avira.de	88
com! Rettungs-Stick 1.0.4 (Installationspaket)	www.com-magazin.de/ergaenzungen	84
Hardware Detection Tool 0.3.6 (System-Informationen)	http://hdt-project.org	89
Hiren's Boot CD 13.1 (Boot-CD)	www.hirensbootcd.org	87
HP USB Disk Storage Format Tool 2.2.3 (Format-Tool)	http://download.softwareload.de/HP-USB-Disk-Storage-Format-Tool/46615	87
Infrarecorder Portable 0.52 (ISO-Dateien erstellen)	http://infrarecorder.org	85
Kaspersky Rescue Disk 10 (Virenscanner)	http://devbuilds.kaspersky-labs.com/devbuilds/RescueDisk10	88
Memtest86+ 4.10 (Speichertest)	www.memtest.org	89
Offline NT Password & Registry Editor 2010-06-27 (Passwort-Tool)	http://pogostick.net/~pnh/ntpasswd	89
Parted Magic 5.2 (Notfall-CD)	www.partedmagic.com	89
Super Grub Disk 0.9799 (Boot-Hilfe)	www.supergrubdisk.org	89
Super Grub Disk 1.98s1 (Boot-Hilfe)	www.supergrubdisk.org	89
Ultimate Boot CD for Windows 3.60 (Boot-CD erstellen)	www.ubcd4win.com	88
U3 Launchpad Removal (USB-Tool)	www.u3.sandisk.com	87

Alle -Programme finden Sie auf Heft-DVD in der Rubrik „Security-Tools, Rettungs-Stick“.

WWWbooks 2.0

Installation

Ein Setup-Skript führt Sie durch die Installation des Rettungs-Sticks. Zuvor müssen Sie Ihren USB-Stick allerdings bootfähig formatieren.

Stick vorbereiten

Bevor Sie den Rettungs-Stick installieren, sichern Sie zunächst alle Daten Ihres USB-Sticks und verwenden dann das HP USB Disk Storage Format Tool 2.2.3, um Ihren Stick bootfähig zu formatieren (kostenlos, http://download.softwareload.de/HP-USB-Disk-Storage-Format-Tool/46615).

Wählen Sie bei „Device“ Ihren USB-Stick und bei „File system“ das Dateisystem „FAT32“. Deaktivieren Sie alle „Format options“ und beginnen Sie die Formatierung des Sticks mit „Start, Ja“.

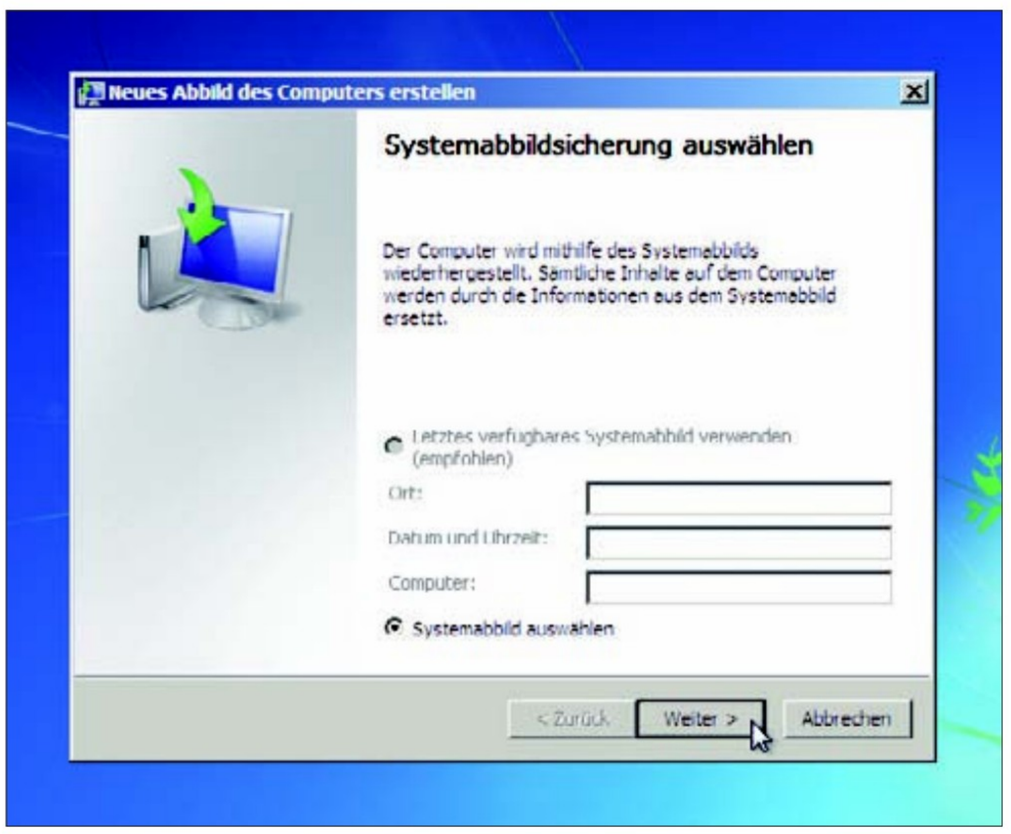
Wenn Sie einen U3-Stick verwenden, entfernen Sie zuvor die U3-Funktionalität mit U3 Launchpad Removal (kostenlos, www.u3.sandisk.com und auf).

Stick installieren

Nachdem Sie Ihren USB-Stick bootfähig formatiert haben, entpacken Sie das Archiv „rstick104.zip“ in das Hauptverzeichnis Ihres Sticks (kostenlos, www.com-magazin.de und auf). Wenn Sie anschließend mit [Windows E] den Windows-Explorer öffnen und in das Hauptverzeichnis des Sticks wechseln, dann finden Sie dort die Verzeichnisse „boot“ und „rescue“ sowie das Setup-Skript „install.cmd“.

Wenn Sie, wie im Abschnitt „Vorbereitungen“ beschrieben, ISO-Dateien des Reparaturdatenträgers für Windows 7 und der Ultimate Boot CD for Windows erstellt haben, dann kopieren Sie nun die Dateien „ubcd4win.iso“ und „32win7.iso“ beziehungsweise „64win7.iso“ ebenfalls auf den Stick, und zwar in den Ordner „rescue“.

Optional lässt sich auch die Hiren's Boot CD 13.1 in den Rettungs-Stick integrieren (kostenlos, www.hirensboot



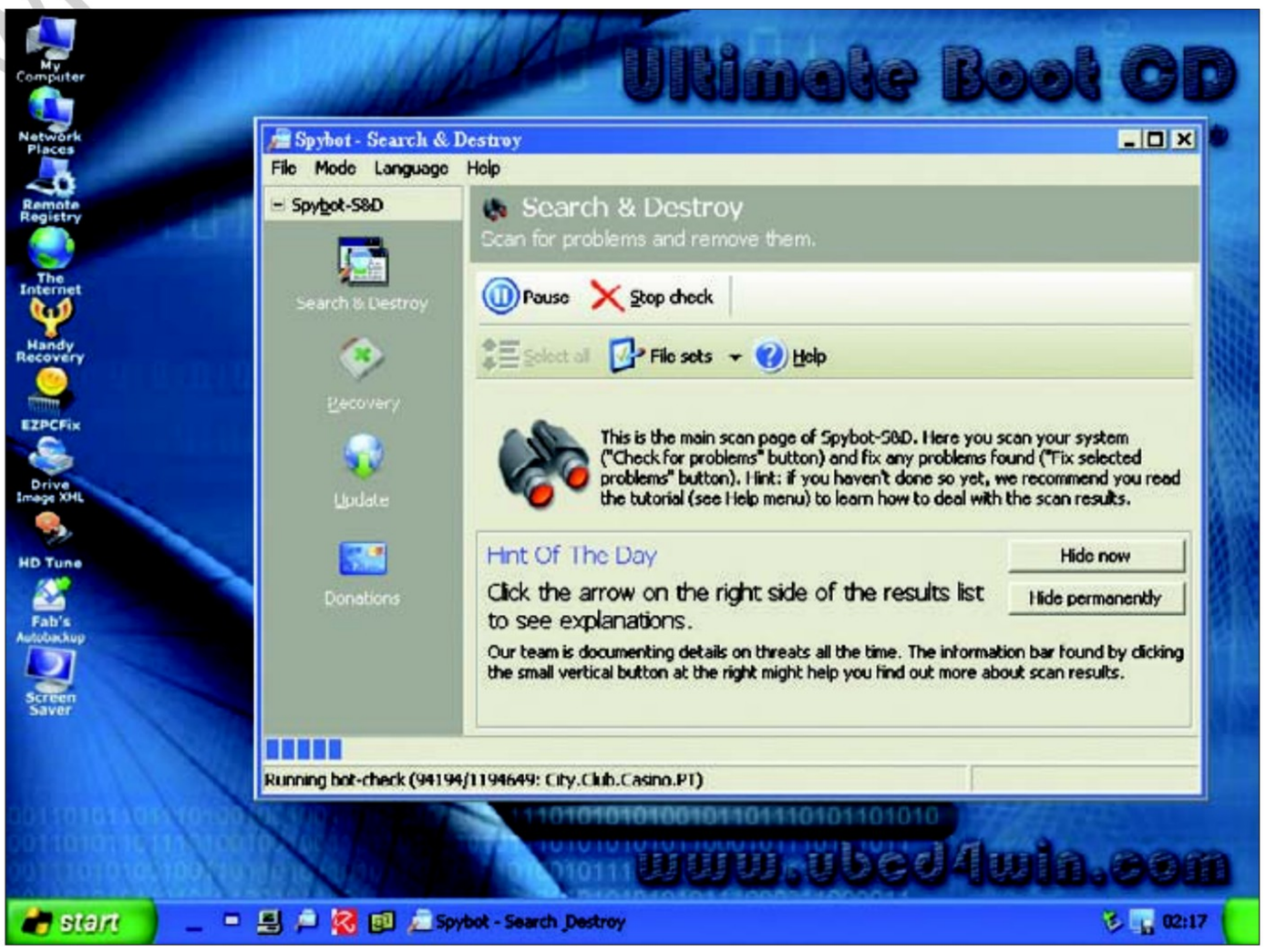
Reparaturdatenträger: Wenn Ihr Windows 7 komplett zerstört ist, dann spielt dieses Tool ein unbeschädigtes Systemabbild ein (Bild E)

cd.org). Die umfangreiche Live-CD mit Diagnose-Tools, Benchmarks, Imaging-Programmen, BIOS-Werkzeugen, Passwort-Knackern und vielem mehr enthält ebenfalls ein Windows PE. Diese Nutzung von Windows ist allerdings illegal, da es dafür keine Erlaubnis von Microsoft gibt. Auch einige Tools der CD lassen sich gesetzwidrig einsetzen. Wenn Sie die Hiren's Boot CD trotzdem installieren möchten, dann kopieren Sie deren ISO-Datei unter dem Namen „hirens.iso“ ebenfalls in den Ordner „rescue“.

Das Setup-Skript „install.cmd“ im Hauptverzeichnis des Sticks führt Sie dann durch die weitere Installation. Das Skript entpackt das Avira Antivir Rescue System, installiert einen Bootloader im Master Boot Record des USB-Sticks und konfiguriert die Startaufrufe für die im Ordner „rescue“ abgelegten ISO-Dateien der Notfall-Systeme.

Unter Vista und Windows 7 klicken Sie das Setup-Skript „install.cmd“ mit der rechten Maustaste an, wählen „Als Administrator ausführen“ und folgen dann den weiteren Anweisungen. Bei Windows XP reicht ein Doppelklick auf „install.cmd“ zum Start der Installation.

Vorsicht: Das Setup-Skript „install.cmd“ überschreibt den Master Boot Record (MBR). Starten Sie niemals eine versehentlich auf der Festplatte abgelegte Kopie des Skripts, da sonst Ihr Windows-Betriebssystem beschädigt werden könnte. ▶



Ultimate Boot CD for Windows 3.60: Dieses Notfall-System des Rettungs-Sticks enthält bewährte Windows-Tools wie den Spyware-Jäger Spybot Search & Destroy (Bild C)

vivobooks 2.0

Rettungs-Stick nutzen

Nach einer Komplett-Installation lassen sich zehn Notfall-Systeme vom Rettungs-Stick booten.

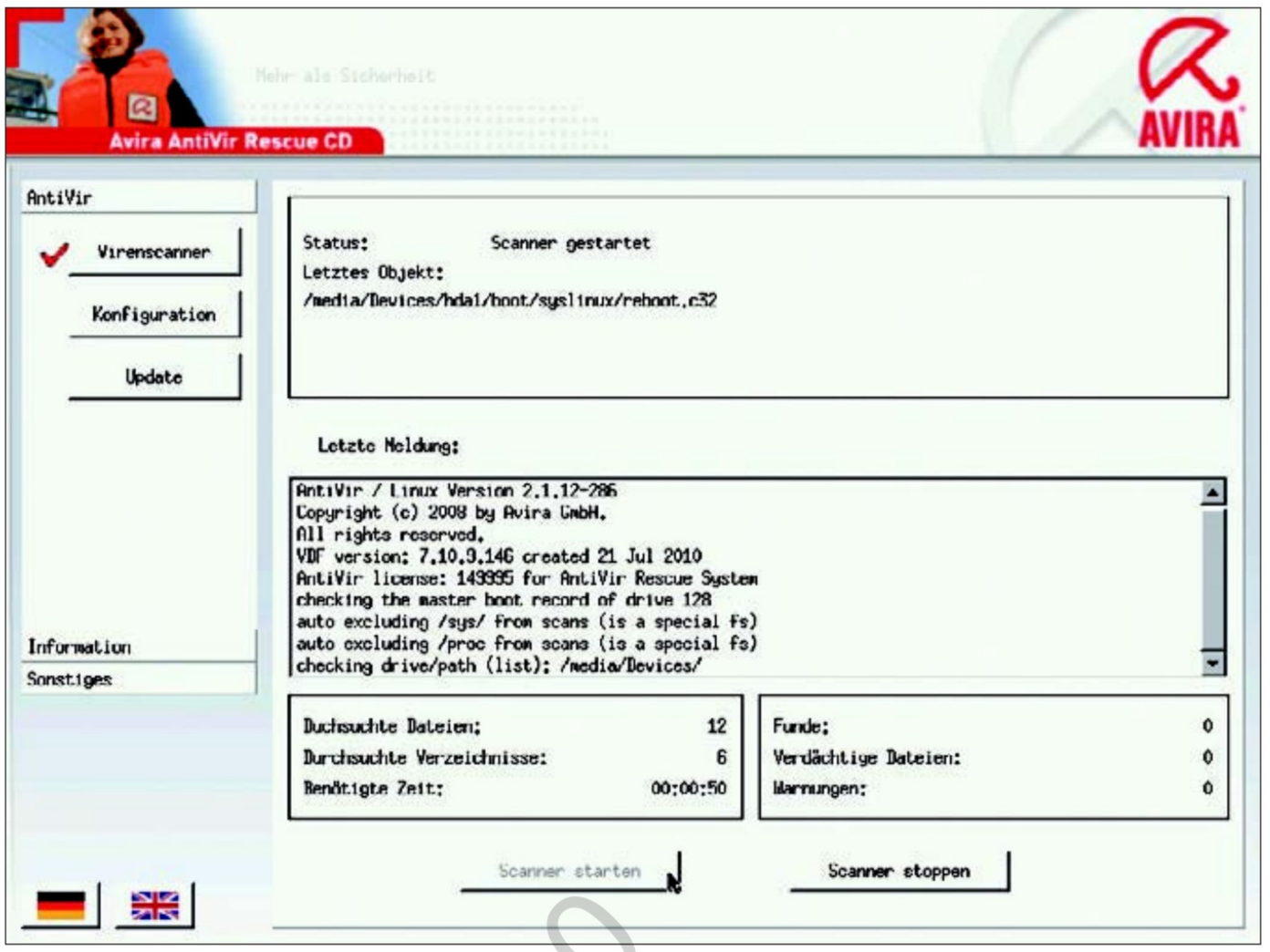
Rettungs-Stick booten

Um vom Rettungs-Stick zu starten, ändern Sie die Boot-Reihenfolge im Boot-Menü oder direkt im BIOS. Wechseln Sie dazu ins BIOS, indem Sie beim Booten die Taste [F2] oder [Entf] drücken. Die entsprechenden Boot-Parameter finden Sie meist unter „Advanced BIOS Features“. Speichern Sie die Änderungen im BIOS mit „Save & Exit Setup“.

Wenn Sie den PC vom Rettungs-Stick booten, erscheint das Auswahlmenü. Markieren Sie mit [Aufwärtspfeil] und [Abwärtspfeil] das gewünschte Notfall-System. Unterhalb des Menüs finden Sie eine Kurzinfo zu Ihrer Auswahl, und mit der Eingabetaste starten Sie das markierte System.

Reparaturdatenträger

Der **Reparaturdatenträger für Windows 7** bootet ein Mini-Windows mit Hilfsprogrammen zum Beheben schwerer Systemfehler. Das Notfall-System löst diverse Startprobleme, reaktiviert Wiederherstellungspunkte und spielt bei Bedarf auch ein zuvor angelegtes Systemabbild ein (Bild E). Achtung: Auf langsameren PCs kann der Startvorgang des Reparaturdatenträgers mehrere Minuten dauern.



Antivirus-Tools: Das Avira Antivir Rescue System 3.6.9 und die Kaspersky Rescue Disk 10 booten von Ihrem Rettungs-Stick und prüfen den PC auf Schadsoftware (Bild F)

Antivirus-Tools

Das **Avira Antivir Rescue System 3.6.9** (Bild F) verwendet eine deutsche Bedienoberfläche. Sobald das System gestartet ist, aktualisieren Sie die Virensignaturen. Dazu klicken Sie auf „Update, Ja“.

Die **Kaspersky Rescue Disk 10** kann eine Protokolldatei auf der untersuchten Festplatte speichern. Sobald die Oberfläche geladen ist, wechseln Sie zu „Update“ und aktualisieren die Virensignaturen mit „Update ausführen“. Wechseln Sie zu „Untersuchung von Objekten“, aktivieren Sie allen Partitionen, die Sie prüfen wollen, und starten die Virensuche mit „Untersuchung von Objekten starten“.

Windows-Tools

Die **Ultimate Boot CD for Windows 3.60** startet ein abgespecktes XP, das Zugriff auf über 100 Windows-Tools bietet. Für den Start vom Rettungs-Stick sollte Ihr PC über mindestens 2 GByte Arbeitsspeicher verfügen. Nach dem Start wird das ISO-Abbild der Ultimate Boot CD for Windows in den Arbeitsspeicher geladen. Danach erscheint das Boot-Menü der CD. Wählen Sie „Launch "The Ultimate Boot CD for Windows"“. So-

Parted Magic 5.2: Das Linux-System bietet Ihnen nach dem Start vom Rettungs-Stick Zugriff auf leistungsstarke Datenretter wie Photorec, Testdisk oder Clonezilla (Bild G)

wiwobooks 2.0

bald der erste Dialog erscheint, klicken Sie auf „Start Shell“, um zum Desktop zu gelangen. Passen Sie mit „Start, System, Display Resolution“ die Bildschirmauflösung an. Alle Tools der CD finden Sie unter „Start, Programs“.

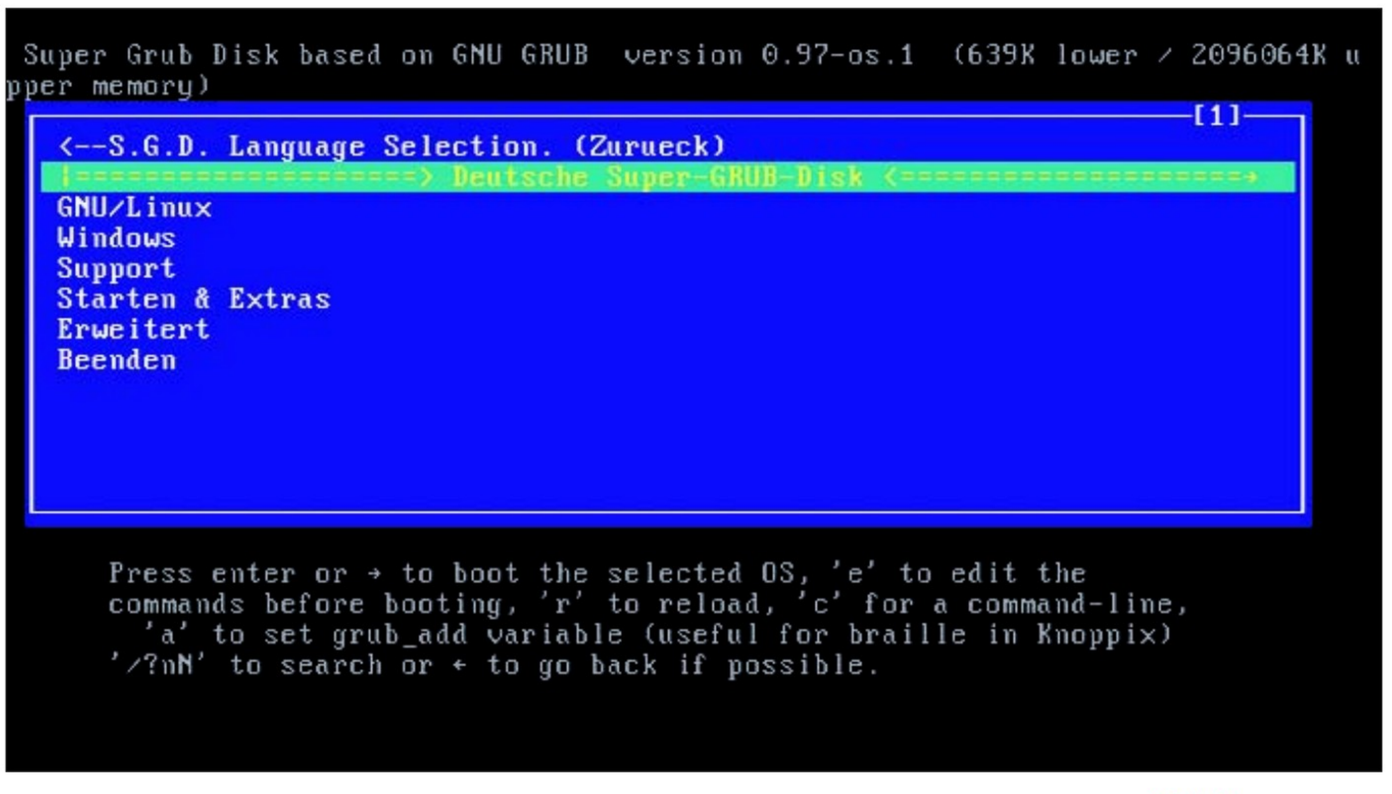
Im Boot-Menü des Rettungs-Sticks finden unter „Windows-Tools“ den **Offline NT Password & Registry Editor 2010-06-27**. Dieses Tool ermöglicht, Windows-Passwörter zu löschen, ohne sich am Computer anzumelden.

Nach dem Programmstart erscheint eine Liste aller Windows-Partitionen. Geben Sie die Kennziffer der Windows-Installation, deren Passwort Sie zurücksetzen möchten, bei „Select“ ein. Folgen Sie den Anweisungen. Die Tastaturbelegung ist englisch.

Festplatten-Tools

Unter den Festplatten-Tools des Rettungs-Sticks finden Sie **Parted Magic 5.2** (Bild G). Den Partitionsmanager Gparted starten Sie per Doppelklick auf „Partitionierungswerkzeug“. Die Datenretter Testdisk und Photorec finden Sie nach einem Klick auf das Symbol von Parted Magic unter „System Tools“.

Mit **Super Grub Disks** (Bild H) lassen sich Partitionen aktivieren oder Linux-Betriebssysteme trotz beschädigtem Bootloader starten.



Super Grub Disk 0.97: Das Tool hilft Ihnen bei Problemen mit dem Boot-Manager Grub (Bild H)

Analyse-Tools

Das **Hardware Detection Tool 0.3.6** ermittelt die verbaute Hardware Ihres PCs. Der Speichertest **Memtest86+ 4.10** prüft, ob der RAM fehlerhaft ist. ■

Stefan Kuhn
sonderheft@com-magazin.de

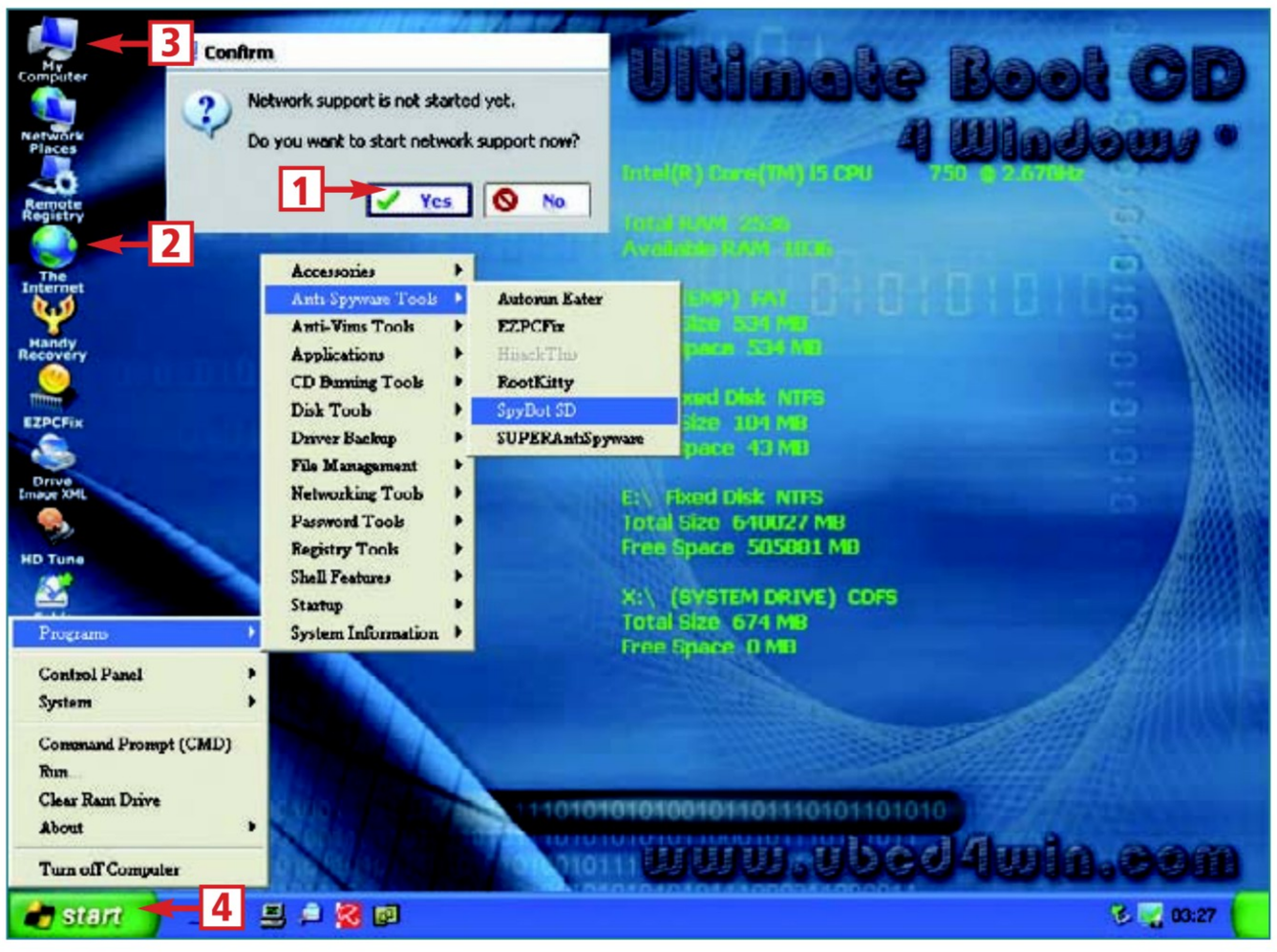
Weitere Infos

- www.com-magazin.de/tipps/2110
  So ändern Sie die Boot-Reihenfolge am PC

wiwobooks 2.0

So geht's: Die Ultimate Boot CD for Windows 3.60

Die Ultimate Boot CD for Windows 3.60 bootet ein Mini-Windows mit den wichtigsten Rettungs-Tools (kostenlos, www.ubcd4win.com). Die Bedienoberfläche gleicht der von Windows XP.



1 Netzwerk starten
In diesem Startdialog aktivieren Sie mit „Yes“ Ihre Internetverbindung.

2 Internet Explorer
Ein Klick auf dieses Desktop-Symbol startet den Internet Explorer 6.0.

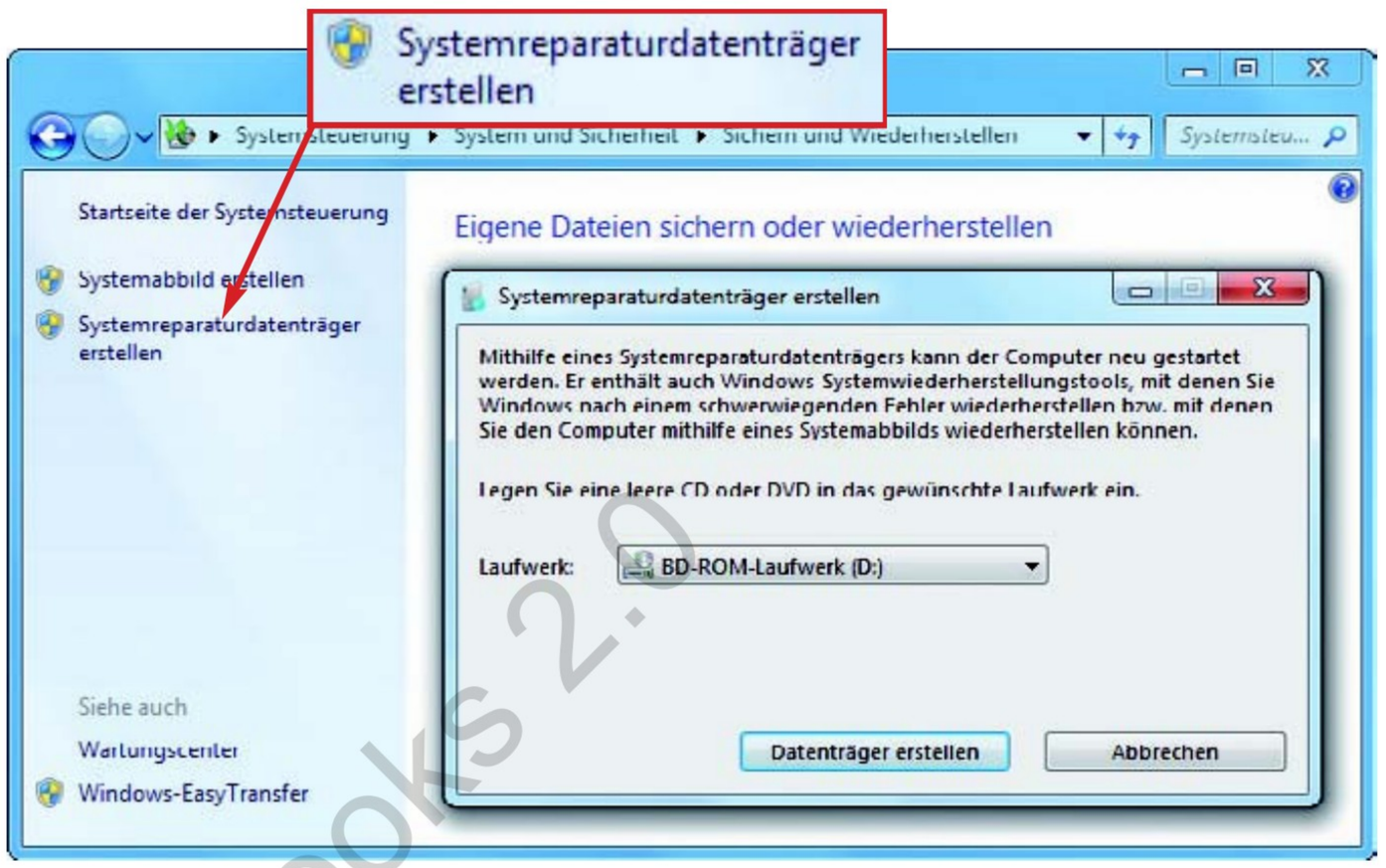
3 Windows-Explorer
Klicken Sie hier, um den Arbeitsplatz im Windows-Explorer zu öffnen.

4 Startmenü
Alle weiteren Tools der Notfall-CD finden Sie im XP-ähnlichen Startmenü.

Reparaturdatenträger

Windows 7 läuft zwar recht stabil. Sollte es aber doch einmal zu Problemen kommen und der PC nicht mehr starten, dann hilft Ihnen eine kostenlose Notfall-CD: der Microsoft Reparaturdatenträger für Windows 7.

Der Microsoft Reparaturdatenträger für Windows 7 startet von CD ein bootbares Mini-Windows mit einigen Hilfsprogrammen zum Beheben schwerer Systemfehler. Das kostenlose Notfall-System löst diverse Startprobleme, reaktiviert Wiederherstellungspunkte und spielt bei Bedarf auch ein zuvor angelegtes Systemabbild ein.



Der Reparaturdatenträger: Mit dieser Option erstellt Windows 7 Ihre Notfall-CD. Der Reparaturdatenträger kann Wiederherstellungspunkte aktivieren und zuvor gesicherte Systemabbilder einspielen (Bild A)

Wer benötigt den Reparaturdatenträger?

Der Reparaturdatenträger für Windows 7 bietet Ihnen die gleichen Funktionen wie das Recovery Environment auf der Installations-DVD von Windows 7. Der Reparaturdatenträger ist deshalb vor allem für Käufer von PCs mit vorinstallierten OEM-Versionen von Windows 7 sinnvoll, bei denen keine Installations-DVD mitgeliefert wird. Zudem lässt sich ein ISO-Abbild des Reparaturdatenträgers auch vom USB-Stick starten, was den Einsatz auf PCs ohne CD-Laufwerk ermöglicht (siehe weiter unten).

Eignet sich der Reparaturdatenträger für jedes Windows 7?

Die 32-Bit- und 64-Bit-Versionen von Windows 7 erfordern unterschiedliche Versionen des Reparaturdatenträgers. Allerdings eignen sich die 32-Bit- und 64-Bit-Versionen des Reparaturdatenträgers jeweils für alle Editionen von Windows 7, ganz gleich ob Sie Home Premium, die Professional- oder die Ultimate-Variante verwenden.

Wo bekomme ich den Reparaturdatenträger?

Der Reparaturdatenträger ist nicht als Download verfügbar, Sie müssen ihn selbst erstellen. Dazu halten Sie einen CD-Rohling bereit, klicken auf „Start, Systemsteuerung“ und wechseln mit „System und Sicherheit“ zu „Sichern und Wiederherstellen“. Im linken Bereich des Fensters nutzen Sie nun „Systemreparaturdatenträger erstellen“ und folgen den Anweisungen (Bild A).

Wie erstelle ich den Reparaturdatenträger, wenn mein PC kein CD-Laufwerk hat?

Der Reparaturdatenträger ist nicht abhängig von Ihrer Windows-Lizenz und lässt sich an jedem PC mit Windows 7 erstellen. Es spricht also nichts dagegen, den Reparaturdatenträger am Rechner eines Bekannten zu erstellen. Wichtig ist nur, dass dort ebenfalls ein 32-Bit-Windows installiert ist, wenn auf Ihrem PC ein 32-Bit-Windows läuft. Das gilt entsprechend für 64-Bit-Systeme. Prüfen Sie deshalb mit [Windows Pause], ob Sie mit einem 32-Bit- oder einem 64-Bit-System arbeiten.

Wie starte ich den Reparaturdatenträger?

Wenn Sie den Reparaturdatenträger in Ihr CD- oder DVD-Laufwerk einlegen und den Rechner neu starten, dann startet das Recovery Environment der Notfall-CD meist automatisch. Bestätigen Sie dazu lediglich die Aufforderung „Drücken Sie eine beliebige Taste, um von CD oder DVD zu starten …“. Wenn der Reparaturdatenträger nicht booten will, dann müssen Sie wahrscheinlich die Boot-Reihenfolge im BIOS anpassen, um von CD statt von Festplatte zu booten.

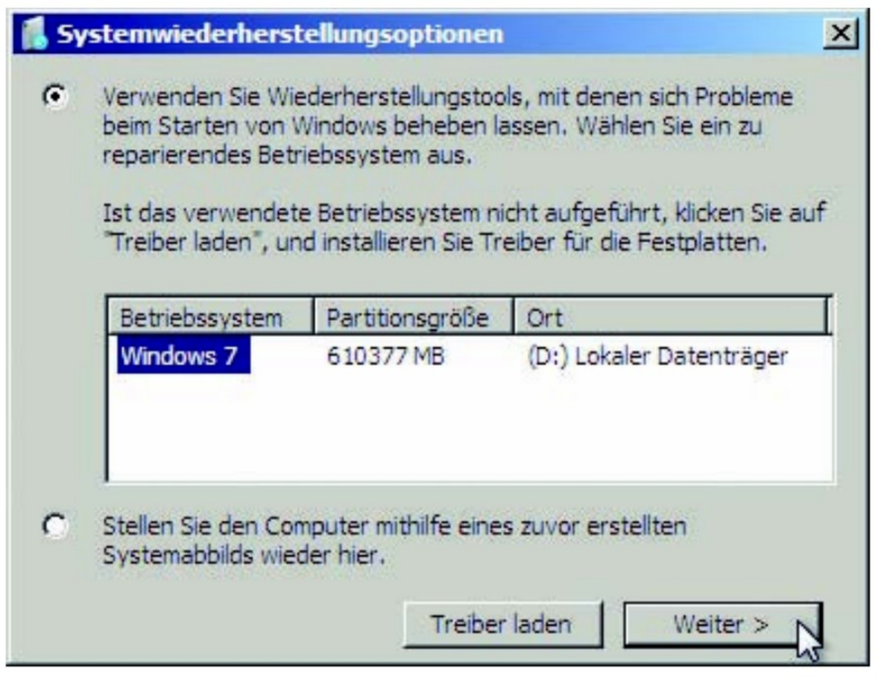
Sobald das Recovery Environment des Reparaturdatenträgers komplett geladen ist, wählen Sie „Deutsch“ als Sprache aus. Im Folgedialog warten Sie, bis Ihre Windows-Installation gefunden wurde, und wählen diese dann zur Reparatur aus (Bild B). Lassen Sie sich dabei nicht davon irritieren, dass der Reparaturdatenträger Ihre Windows-

Wiwobooks 2.0

Installation auf Laufwerk „D:“ statt unter „C:“ anzeigt. Dies liegt daran, dass mit der Windows-7-Installation eine versteckte Rettungspartition auf Ihrer Festplatte angelegt wurde, die das Recovery Environment als Laufwerk „C:“ erkennt.

Welche Tools umfasst der Reparaturdatenträger?

Der Reparaturdatenträger enthält fünf Tools, die im unten stehenden Kasten beschrieben sind. Einen beschädigten Bootloader Ihrer Windows-Installation stellen Sie mit der „Systemstartreparatur“ wieder her. Lässt sich Windows nach einem Update oder einer Software-Installation nicht mehr starten, dann hilft Ihnen die „Systemwiederherstellung“. Mit dieser Funktion setzen Sie das System auf einen ausgewählten Zeitpunkt zurück. Lässt sich Ihr PC nicht wiederbeleben, dann rettet Sie nur noch eine „Systemabbild-Wiederherstellung“ vor einer Neuinstallation. Voraussetzung dafür ist, dass Sie zu einem früheren Zeitpunkt über die Systemsteuerung mit „System und Sicherheit, Sichern und Wiederherstellen, Systemabbild erstellen“ ein Systemabbild erstellt und dieses auf einer anderen Partition Ihres PCs gespeichert haben.



Windows 7 reparieren: In diesem Dialog wählen Sie Ihre Windows-Installation zur Reparatur aus (Bild B)

Lassen sich auch andere Tools mit dieser Notfall-CD starten?

Die „Eingabeaufforderung“ des Reparaturdatenträgers bietet Ihnen durchaus die Möglichkeit, portable Anwendungen zu starten. Auf diese Weise lässt sich etwa ein Tool wie Free Commander 2009.02b (kostenlos, www.freecommander.com) starten, um Daten auf eine andere Partition oder Festplatte zu kopieren. Wenn Sie den Reparaturdatenträger vom USB-Stick starten, dann kopieren Sie die portablen Anwendungen einfach ebenfalls auf den Stick. ■

Stefan Kuhn
sonderheft@com-magazin.de

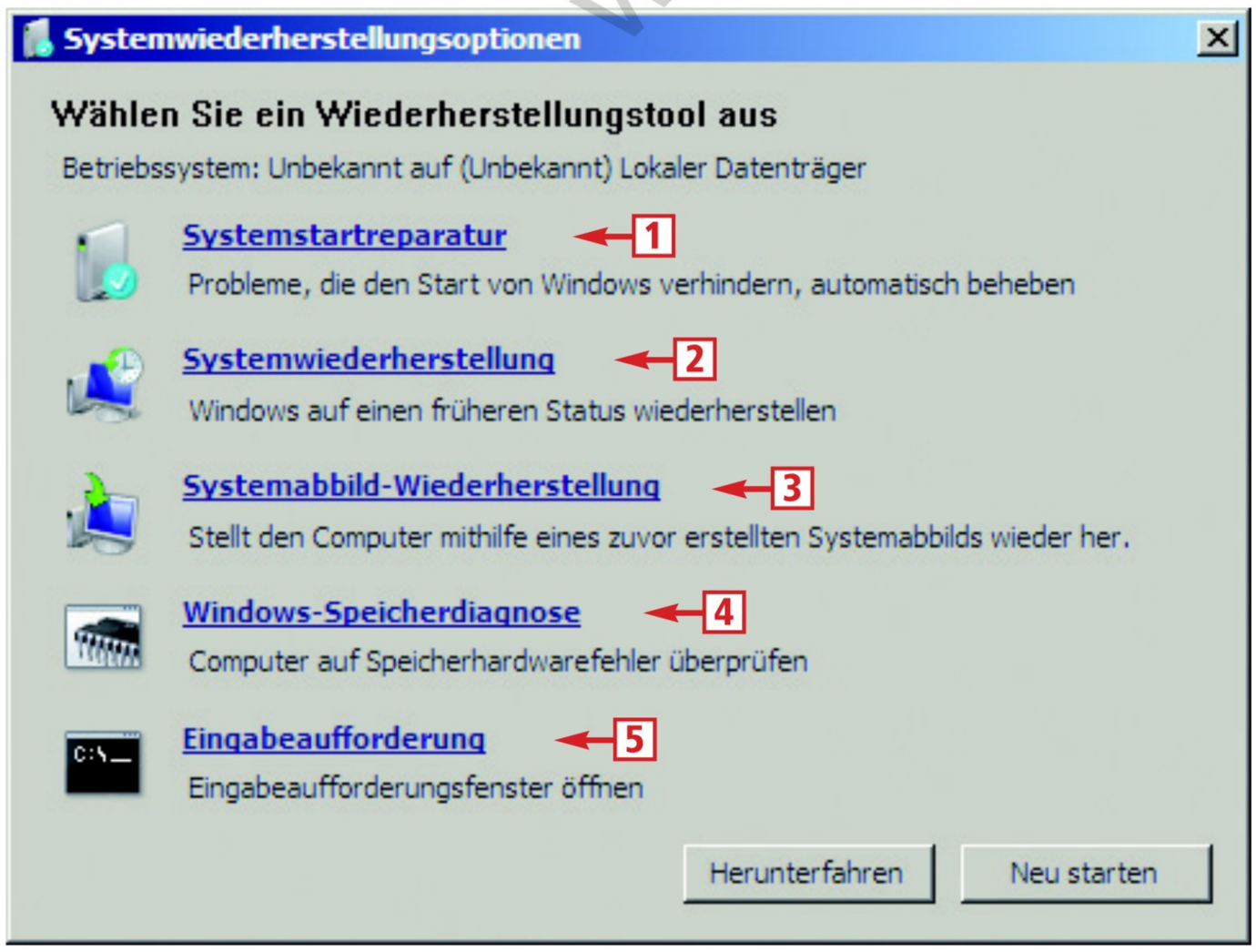
Weitere Infos

- http://windows.microsoft.com/de-DE/windows7/Create-a-system-repair-disc
  Video-Anleitung zum Erstellen des Reparaturdatenträgers für Windows 7
- www.com-magazin.de/tipps/2110
  So ändern Sie die Boot-Reihenfolge am PC

www.books 2.0

So geht's: Der Reparaturdatenträger für Windows 7

Der Reparaturdatenträger startet von CD und hilft Ihnen, schwere Systemfehler in Windows 7 zu beseitigen. Dazu bietet Ihnen das Auswahlmenü des Reparaturdatenträgers die folgenden fünf Systemwiederherstellungsoptionen.



1 Systemstartreparatur
Stellt einen beschädigten Bootloader Ihrer Windows-Installation wieder her.

2 Systemwiederherstellung
Lädt einen Wiederherstellungspunkt, etwa um Fehler einer Software-Installation zu beseitigen.

3 Systemabbild-Wiederherstellung
Lädt ein mit Windows 7 zuvor erstelltes, vollständiges Systemabbild Ihrer Installation.

4 Windows-Speicherdiagnose
Prüft, ob der Arbeitsspeicher Ihres Rechners fehlerhaft ist.

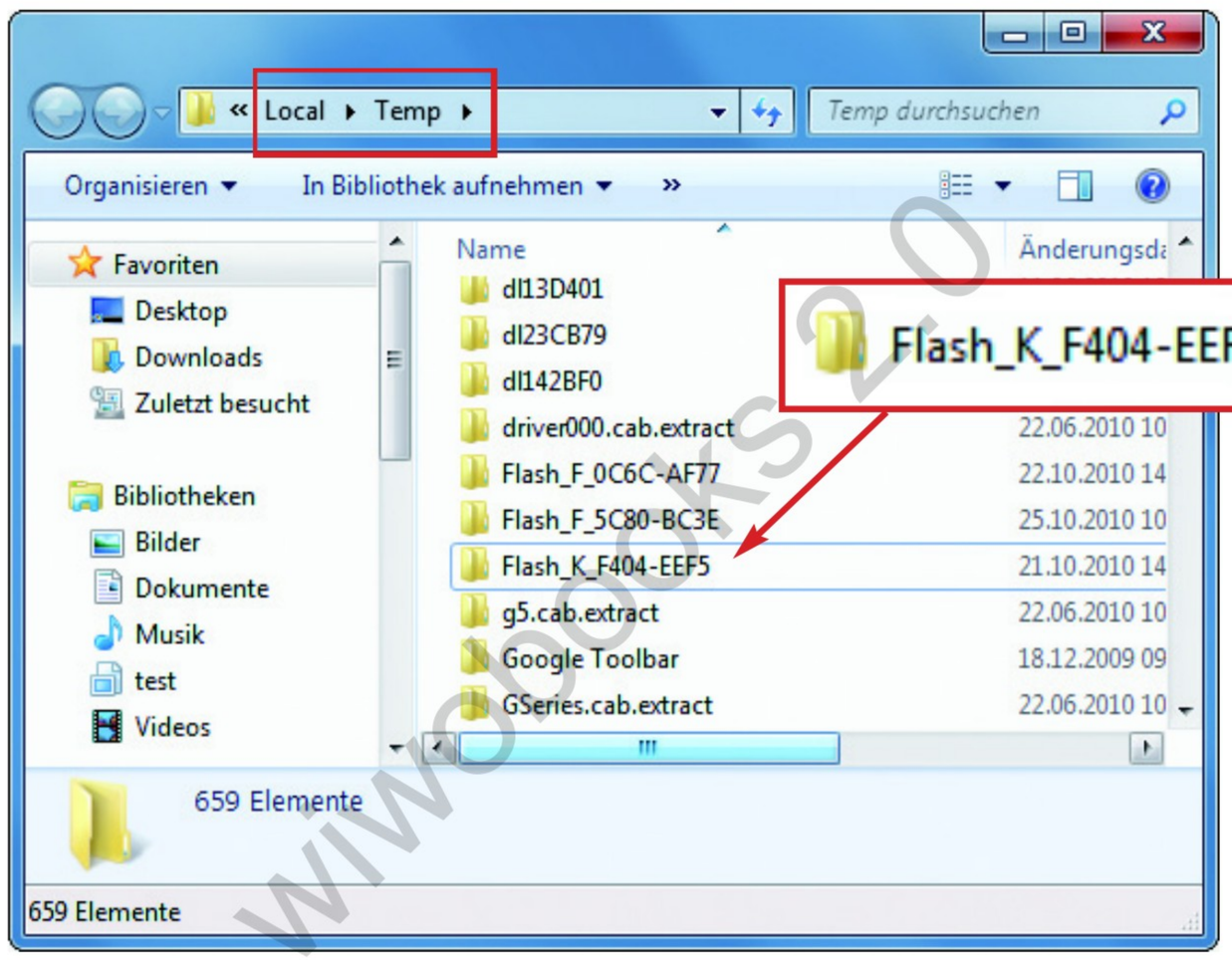
5 Eingabeaufforderung
Bietet Ihnen alle Möglichkeiten der Windows-Kommandozeile.

USB-Stick sichern: USB Flash Copy 1.5

Das Tool USB Flash Copy 1.5 sichert die Daten des USB-Sticks auf den PC, sobald er eingesteckt wird. Mit Profilen lassen sich spezielle Sicherungsjobs für unterschiedliche Sticks anlegen.

Das Problem bei USB-Sticks ist deren Mobilität. Das heißt, da sie nicht immer am PC angeschlossen sind, ist es schwierig, sie automatisch von einer Backup-Software sichern zu lassen.

Das Tool USB Flash Copy 1.5 bietet eine Lösung für das Problem (kostenlos, www.usbflashcopy.com und auf). Es läuft im Hintergrund und überwacht die USB-Steckplätze. Wird ein bekannter Stick mit dem Rechner verbunden, startet automatisch der Kopiervorgang.



Standardprofil: Die Sicherung landet im „Temp"-Ordner. Hier sehen Sie das Backup des Sticks „Flash_K_F404-EEF5". „Flash" nennt USB Flash Copy den Stick, wenn kein Name vergeben wurde. „K" steht für den Laufwerkbuchstaben, „F404-EEF5" ist die Seriennummer (Bild A)

Von USB Flash Copy 1.5 gibt es zwei Versionen. Die eine – Basic Mode genannt – ist kostenlos. Die andere mit der Bezeichnung Silent Stealth Mode kostet rund 29 Euro. Der einzige Unterschied zwischen den Versionen ist, dass die kostenlose Variante beim Kopieren der Daten eine Fortschrittsanzeige anzeigt. Bei der Kaufversion lässt sich die Anzeige verbergen.

Lesen Sie, wie Sie USB Flash Copy einrichten und bedienen und wie Sie Profile erstellen.

Praktisch: USB Flash Copy prüft alle 60 Minuten, ob sich der Datenbestand auf dem angeschlossenen Stick verändert hat. Sind neue Daten oder neue Versionen von Dateien vorhanden, werden sie automatisch auf die Festplatte kopiert.

Tipp: Damit der Datenbestand auf der Festplatte immer aktuell ist, starten Sie den Kopiervorgang, bevor Sie den Stick abziehen, manuell. So stellen Sie sicher, immer sämtliche Dateien kopiert zu haben.

Auf DVD

Sie finden USB Flash Copy 1.5 auf in der Rubrik „Security-Tools, USB Flash Copy".

Kompakt

- *USB Flash Copy sichert komfortabel die Daten Ihres USB-Sticks auf die Festplatte.*
- *Das Programm erlaubt es, Sicherungsprofile für unterschiedliche USB-Sticks zu erstellen.*
- *Anhand der Seriennummer erkennt das Programm den Stick und führt die im Profil definierte Sicherung aus.*

Bedienung

USB Flash Copy ist ein Sofort-Tool. Das bedeutet: Das Programm muss nicht installiert werden. Erstellen Sie einfach mit dem Windows-Explorer unter „C:" einen neuen Ordner mit der Bezeichnung `USB·Flash·Copy` und kopieren Sie in diesen Ordner die Datei „usbflashcopy.exe". Erstellen Sie anschließend eine Verknüpfung auf dem Desktop, damit Sie das Tool mit einem Doppelklick schnell aufrufen können. Wechseln Sie dazu in den Ordner „USB Flash Copy" und klicken Sie mit der rechten Maustaste auf die Datei

Inhalt

USB-Stick sichern: USB Flash Copy

- **Bedienung**
  - Programmstart S. 93
  - Schnellsicherung S. 93
  - Individuelle Sicherung S. 93
- **Konfiguration**
  - Externe Festplatten sichern S. 94
  - Autostart einrichten S. 94

So geht's: USB Flash Copy 1.5 S. 93

„usbflashcopy.exe". Wählen Sie im Kontextmenü die Option „Senden an, Desktop (Verknüpfung erstellen)". Augenblicklich erscheint ein entsprechendes Symbol auf dem Desktop.

Programmstart

Starten Sie USB Flash Copy mit einem Doppelklick auf das Desktop-Symbol. Windows gibt daraufhin eine Sicherheitswarnung aus, mit der es meldet, dass der Herausgeber der Software nicht verifiziert werden konnte. Entfernen Sie das Häkchen bei „Vor dem Öffnen dieser Datei immer bestätigen", damit die Meldung künftig unterdrückt wird und das Programm sofort startet.

USB Flash Copy startet minimiert. Das bedeutet: Es erscheint beim Start kein Fenster, sondern das Programm wechselt sofort in den Hintergrund. Das Programmfenster erscheint erst, wenn Sie einen USB-Stick einstecken.

Schnellsicherung

Verbinden Sie Ihren USB-Stick mit dem PC. Sobald Windows den Treiber für den Stick geladen hat, poppt ein Fenster von USB Flash Copy auf. Es meldet, dass ein neuer Datenträger gefunden wurde, und fordert Sie dazu auf, die nötigen Einstellungen für den Datenträger zu definieren.

Für die schnelle, unkomplizierte Datensicherung klicken Sie auf „Use default profile". USB Flash Copy sichert alle Dateien vom Stick in das Verzeichnis „%temp%\Flash_%root%_%serial%\". Im Klartext befindet sich der Ordner im Verzeichnis „C:\Users\<Benutzername>\AppData\Local\Temp\<Bezeichnung des USB-Sticks>" (Bild A).

Individuelle Sicherung

Wer seine USB-Sticks lieber systematisch in bestimmten Ordnern sichern möchte, der sollte Sicherungsprofile erstellen. Diese Profile sind speziell an einzelne Sticks angepasst. Das Tool USB Flash Copy erkennt einen USB-Stick an seiner Seriennummer und sichert dessen Daten automatisch in den vordefinierten Order, sobald der USB-Stick mit dem Rechner verbunden ist. Bei unbekannten Sticks erscheint die Meldung, dass ein neues Medium erkannt wurde.

Individuelle Sicherungsprofile für USB-Sticks lassen sich sehr einfach erstellen. Verbinden Sie den entsprechenden USB-Stick mit dem PC. USB Flash Copy meldet, dass ein neuer Datenträger erkannt wurde. Klicken Sie im Fenster auf die Schaltfläche „New profile …".

Ein Konfigurationsfenster erscheint. In der Rubrik „General" erhalten Sie ▶

So geht's: USB Flash Copy 1.5

USB Flash Copy 1.5 sichert automatisch die Dateien vom USB-Stick auf den PC (kostenlos, www.usbflashcopy.com und auf). Das Programm erkennt den Stick anhand seiner Seriennummer und führt anschließend die vorab festgelegten Aktionen automatisch durch.

1 New profile …
Hier erstellen Sie für jeden USB-Stick ein eigenes Sicherungsprofil.

2 Use default profile
Eine Standardsicherung führen Sie mit einem Klick auf diese Schaltfläche durch.

3 Never backup this media
Klicken Sie auf diese Schaltfläche, damit das Programm den Stick künftig ignoriert.

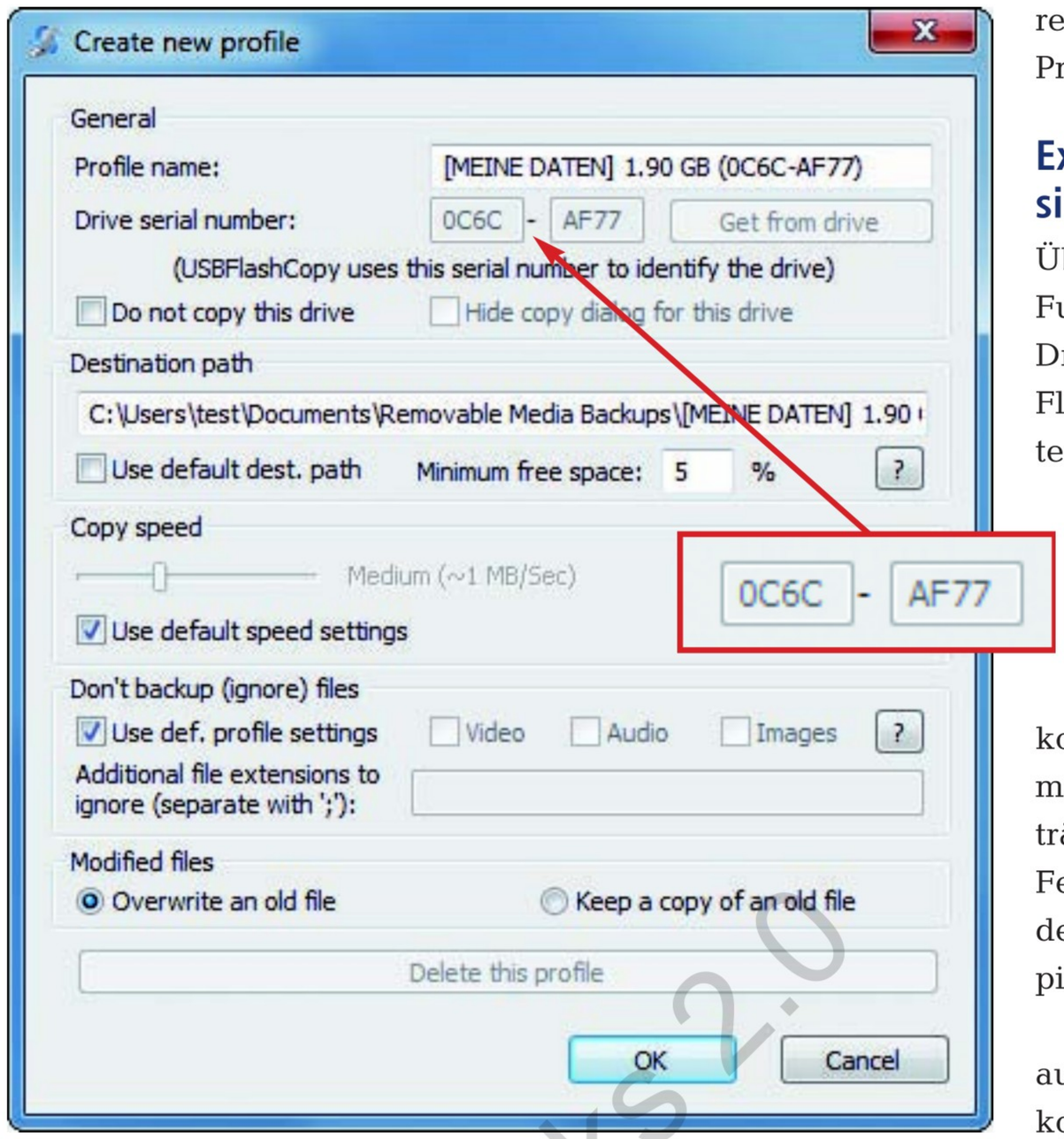
wiwobooks 2.0

Infos zum Stick, zum Beispiel den Namen und die Seriennummer (Bild B). Außerdem lässt sich hier definieren, ob die Daten des Sticks überhaupt kopiert werden sollen.

Unmittelbar darunter schlägt Ihnen das Programm einen Sicherungs-Ort für die Daten vor – er lässt sich jedoch anpassen.

Wer bestimmte Dateien von der Sicherung ausnehmen will, entfernt das Häkchen bei „Use def. profile settings“. Danach lassen sich Videos, Musik oder Bilder von vornherein ausschließen. In der Eingabezeile darunter lassen sich sogar bestimmte Dateitypen anhand der Dateiendung von der Sicherung ausnehmen.

Unter „Modified files“ definieren Sie, ob USB Flash Copy die alten Dateien durch neuere Versionen ersetzen oder die alten Daten erhalten soll. Dies entspricht einer inkrementellen Sicherung.



Profil erstellen: Hier sehen Sie das Sicherungsprofil für den USB-Stick mit dem Namen „MEINE DATEN“ und der Seriennummer „0C6C-AF77“ (Bild B)

Konfiguration

Einmal eingerichtet, arbeitet USB Flash Copy selbsttätig im Hintergrund. Sie müssen sich keine Gedanken mehr über das Programm machen, da eigentlich alles automatisch abläuft.

Es gibt jedoch Situationen, in denen der Anwender eine bestimmte Aktion des Programms sofort benötigt, weil er etwa auf die gesicherten Daten zugreifen will oder das Prüfintervall des Datenbestands verkürzen möchte (Bild C).

Vielleicht soll aber auch nur das Sicherungsprofil für den Stick modifiziert werden.

All diese Aufgaben lassen sich im Kontextmenü des Programms erledigen. Klicken Sie dazu im System-Tray mit der rechten Maustaste auf das Programmsymbol.

Externe Festplatten sichern

Über die Kontextmenü-Funktion „Settings, Media Drives“ bringen Sie USB Flash Copy dazu, auch externe Festplatten oder USB-Sticks, die Windows nicht als Wechseldatenträger, sondern als Festplatte erkennt, zu sichern. USB Flash Copy kopiert nämlich standardmäßig nur Wechseldatenträger und keine externen Festplatten, selbst wenn dem Datenträger ein Kopierprofil zugeordnet ist.

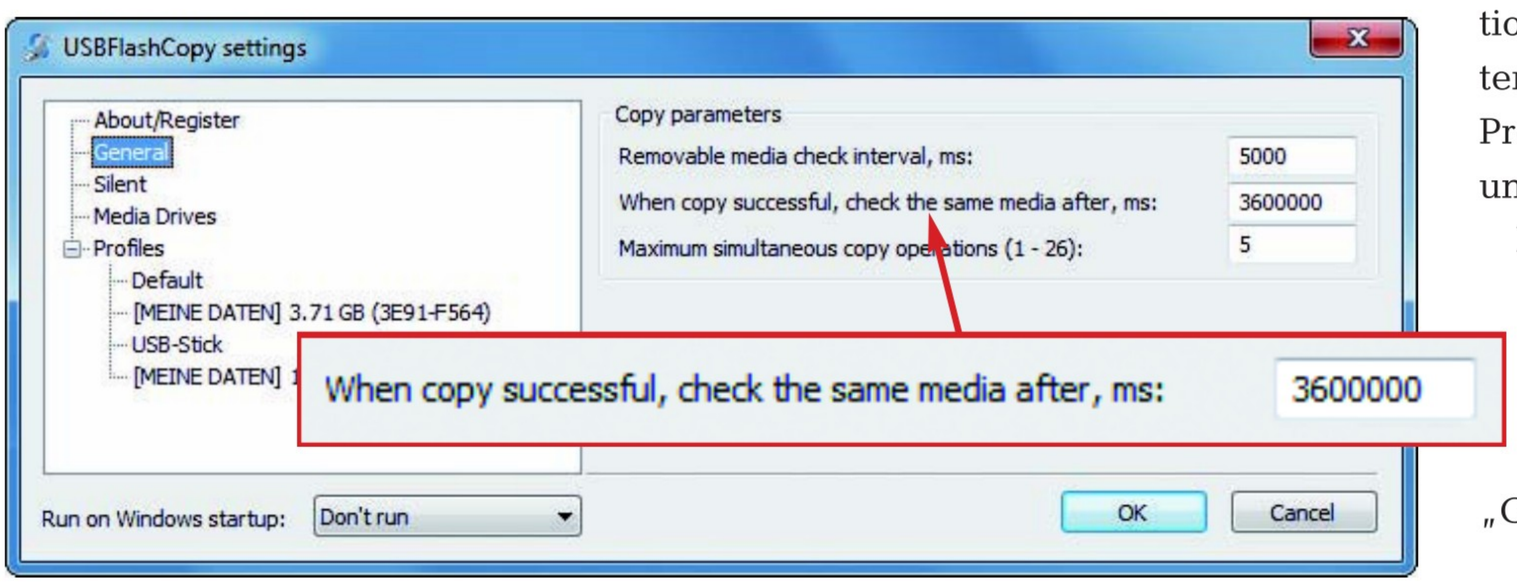
Damit USB Flash Copy auch externe Festplatten kopiert, wählen Sie in der Funktion „Media Drives“ beim entsprechenden Laufwerkbuchstaben im Aufklappmenü den Parameter „Force“.

Autostart einrichten

In der Standardeinstellung muss USB Flash Copy manuell per Doppelklick gestartet werden, bevor es aktiv wird. Diese Einstellung ist aber unpraktisch, da der Programmstart leicht vergessen wird. Besser ist es, wenn USB Flash Copy bereits beim Windows-Start automatisch aufgerufen wird.

In den Programmeinstellungen nehmen Sie die entsprechende Konfiguration vor. Klicken Sie dazu mit der rechten Maustaste im System-Tray auf das Programmsymbol von USB Flash Copy und wählen Sie „Settings“.

Im Konfigurationsfenster öffnen Sie anschließend links unten bei „Run on Windows startup“ das Aufklappmenü und stellen dort „For all Users“ ein. Bestätigen Sie mit „OK“. ■



Sicherungsintervall festlegen: Hier definieren Sie, in welchen Zeiträumen USB Flash Copy prüfen soll, ob neue Daten kopiert werden müssen – hier nach jeweils 3.600.000 Millisekunden, also 60 Minuten (Bild C)

Oliver Ehm
sonderheft@com-magazin.de

Windows 2.0

com! auch ohne CD/DVD im Abo erhältlich.

Für sensationelle 28,80 € erhalten Sie 12 x com! nach Hause geliefert.

Und das Beste: Wir schenken Ihnen zur Begrüßung 10,– € Geldprämie als Verrechnungsscheck dazu.

Unser Geschenk!

Ihre Vorteile

12 x pünktliche und bequeme Lieferung frei Haus
12 x handfeste Tipps und Tricks für Ihren PC
12 x Anleitungen, um Ihren PC optimal zu nutzen

On top

10,– € Willkommensgeschenk als Verrechnungsscheck

Mehr Infos unter: www.com-magazin.de/magazin

PC richtig abschließen

Ihr Windows-Passwort ist nicht sicher: Tools wie Ophcrack können es leicht auslesen. Das ist dann gefährlich, wenn Ihr PC frei zugänglich ist oder wenn Sie Ihr Notebook verlieren. Sichern Sie Ihren PC deshalb zusätzlich mit Syskey.

Windows speichert alle Ihre Benutzernamen und Passwörter in einer Kennwortdatenbank (Security Accounts Manager, SAM) auf der Festplatte.

Das Problem: Tools wie Ophcrack 3.3.1 (kostenlos, http://ophcrack.sourceforge.net) können die Datenbank leicht knacken und die Passwörter lesen.

Mehr Schutz gegen unbefugten Zugriff auf Ihren PC bietet das in Windows ab XP enthaltene Tool Syskey.

USB-Stick als PC-Schlüssel: Das Windows-Tool Syskey sichert die Kennwortdatenbank mit einem Schlüssel. Den Schlüssel speichert es auf Wunsch auf einem USB-Stick. Danach lässt sich der PC nur noch starten, wenn der USB-Stick eingesteckt ist (Bild A)

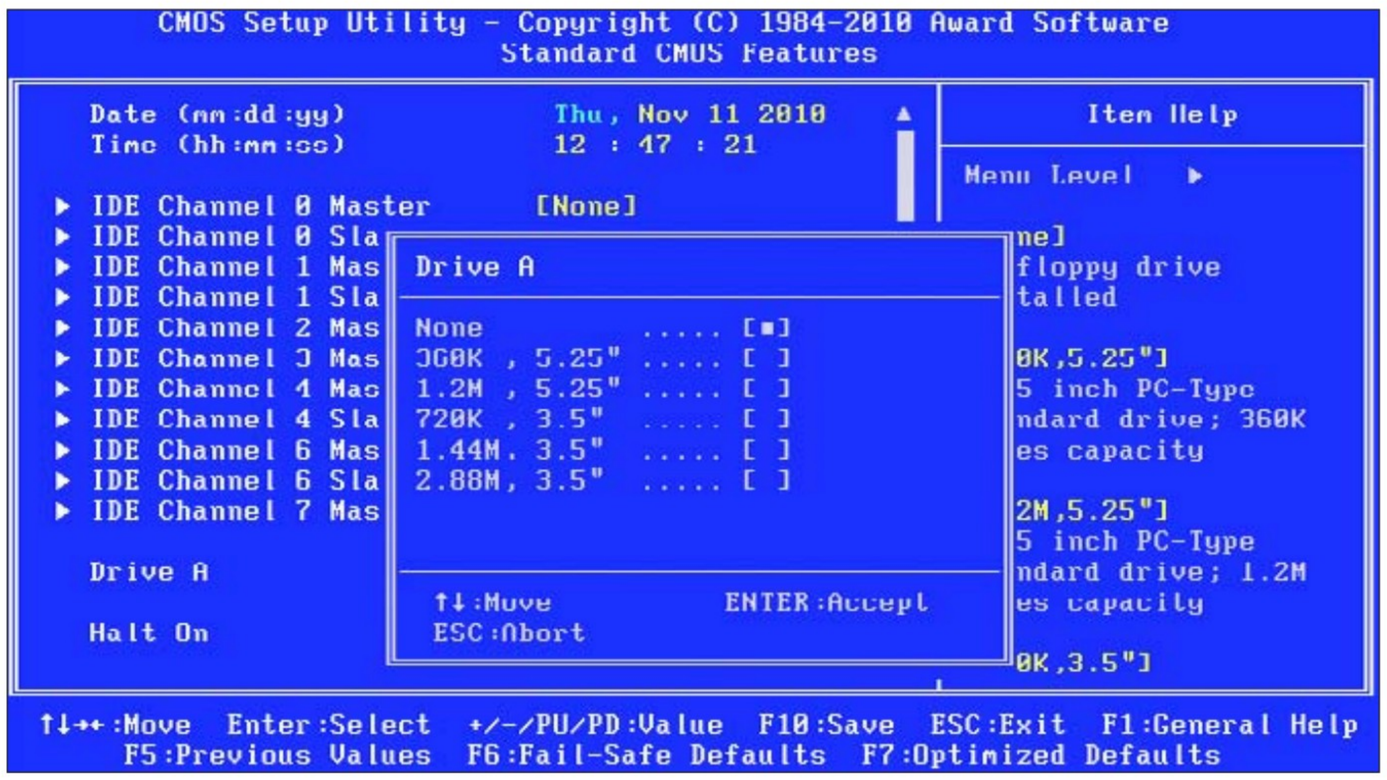
Sicherheits-Tool Syskey

Syskey verschlüsselt die Kennwortdatenbank auf Ihrer Festplatte. Das Passwort hierfür kann bis zu 128 Zeichen lang sein. Knack-Tools wie Ophcrack können aus einer so verschlüsselten Kennwortdatenbank nur noch mit extrem hohem Aufwand Passwörter auslesen. Für Sie bedeutet das, dass Sie bei jedem PC-Start noch vor der eigentlichen Windows-Anmeldung ein zusätzliches Kennwort eingeben müssen.

Wer ganz auf Nummer sicher gehen will, der schützt den Schlüssel für die Kennwortdatenbank nicht mit einem Passwort. Er deponiert den Schlüssel vielmehr auf einem USB-Stick. Knack-Tools ist damit jede Angriffsmöglichkeit entzogen. Ein Schlüssel auf dem USB-Stick benötigt deshalb auch gar kein Passwort mehr.

Für Sie bedeutet das, dass Sie bei jedem PC-Start den USB-Stick einstecken müssen (Bild A).

Dieser Artikel beschreibt zunächst, wie Sie ein zusätzliches Passwort für den Systemstart einrichten. Anschließend erklärt er, wie Sie den Schlüssel für die Kennwortdatenbank auf einem USB-Stick deponieren.



Laufwerk „A:" freigeben: Syskey speichert den Schlüssel für die Kennwortdatenbank grundsätzlich auf Laufwerk „A:". Falls bei Ihnen ein Diskettenlaufwerk diesen Buchstaben besetzt, deaktivieren Sie es im BIOS. Dann ist „A:" frei für Ihren USB-Stick (Bild C)

Zusätzliches Passwort für den PC-Start

Sie erstellen mit Hilfe von Syskey einen Schlüssel für die Kennwortdatenbank. Den Schlüssel schützen Sie mit einem Passwort.

Passwort einrichten

Starten Sie Syskey mit [Windows R] und **`syskey`**. Klicken Sie auf „Aktualisieren". Wählen Sie die Option „Kennwort für den Systemstart" und tragen Sie das Passwort ein (Bild B). Klicken Sie auf „OK".

www.books-2.0

PC-Schlüssel auf dem USB-Stick

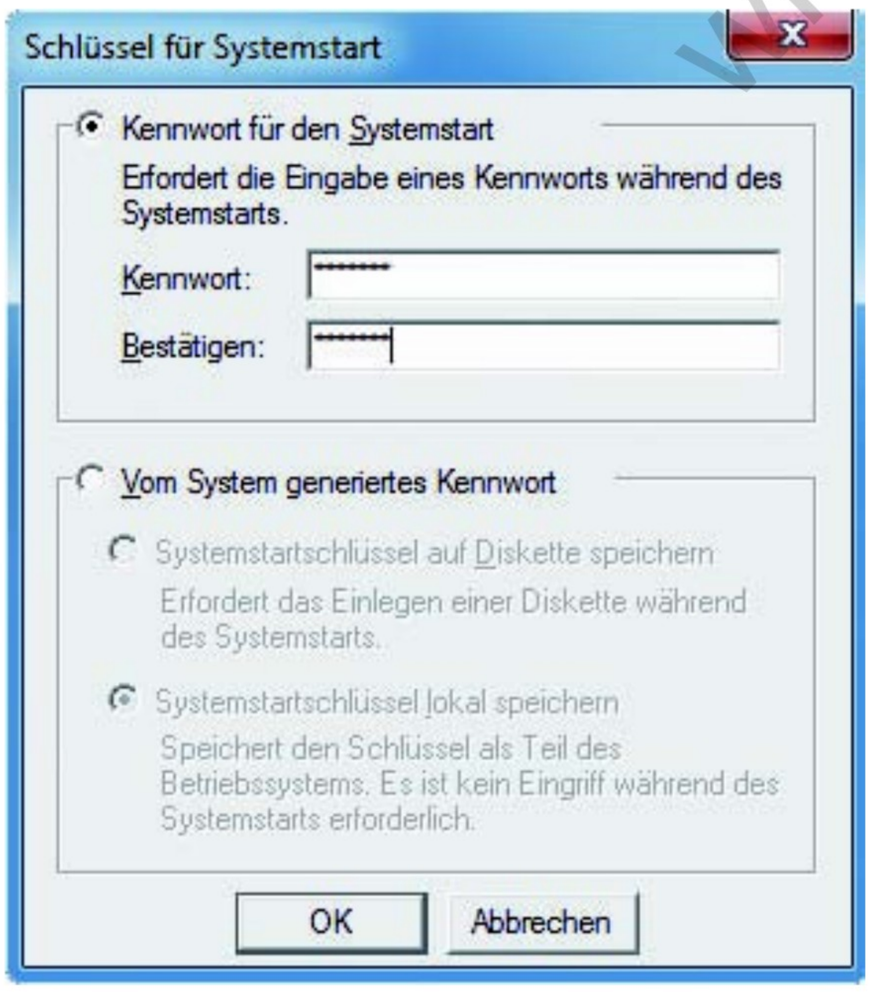
Sie speichern den Schlüssel für die Kennwortdatenbank auf Ihrem USB-Stick.

Floppy deaktivieren

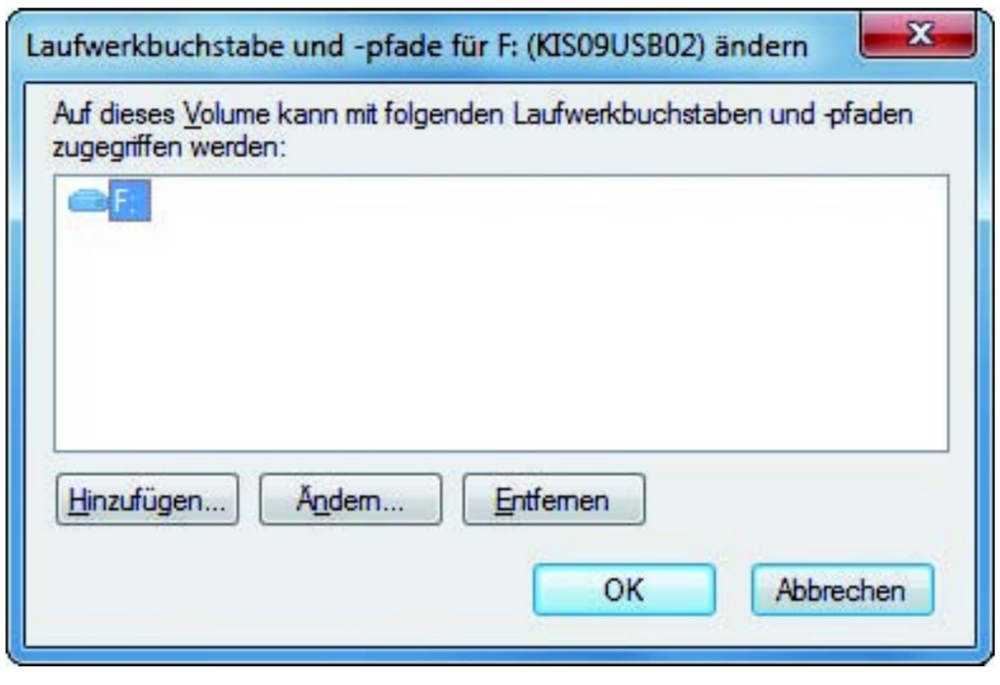
Das Tool Syskey stammt aus einer Zeit, als es noch keine USB-Sticks gab. Zu dieser Zeit arbeiteten alle Anwender noch mit Disketten. Das Diskettenlaufwerk trägt üblicherweise die Bezeichnung „A:“. Syskey erwartet den Schlüssel folglich auf Laufwerk „A:“. Sorgen Sie also dafür, dass Ihr USB-Stick als Laufwerk „A:“ erscheint.

Falls Sie in Ihrem PC noch ein Diskettenlaufwerk haben, müssen Sie es im BIOS zuerst deaktivieren, damit der Laufwerkbuchstabe „A:“ frei wird.

Rufen Sie dazu das BIOS-Setup auf: Drücken Sie beim Start mehrmals die Taste [Entf] oder [F1]. Welche Taste es bei Ihrem Rechner ist, steht im Handbuch Ihres Mainboards oder PCs. Die Option zum Deaktivieren des Floppy-Laufwerks finden Sie im BIOS im Menü „Main“ oder unter „Standard CMOS Features“ (Bild C). Deaktivieren Sie hier das Floppy-Laufwerk. Verlassen Sie das BIOS über „Save & Exit Setup“. Starten Sie den PC ganz normal.



Passwort für den PC-Start einrichten: Schützen Sie den Schlüssel für die Kennwortdatenbank mit einem Passwort. Syskey unterstützt Passwörter mit bis zu 128 Zeichen (Bild B)



Laufwerkbuchstaben zuweisen: Windows hat Ihrem USB-Stick automatisch einen Laufwerkbuchstaben zugewiesen, hier zum Beispiel „F:“. Weisen Sie dem Stick stattdessen das Laufwerk „A:“ zu (Bild D)

USB-Stick vorbereiten

Weisen Sie dem USB-Stick den Laufwerkbuchstaben „A:“ zu. Stecken Sie den USB-Stick ein und starten Sie die Datenträgerverwaltung mit [Windows R] und `diskmgmt.msc`. Unten in der Liste erscheint der USB-Stick. Klicken Sie mit der rechten Maustaste darauf und wählen Sie „Laufwerkbuchstaben und -pfade ändern …“. Klicken Sie auf „Ändern …“ und weisen Sie dem Stick den Buchstaben „A“ zu (Bild D). Bestätigen Sie alles mit „OK“ und „Ja“. Der USB-Stick ist jetzt Laufwerk „A:“.

PC-Schlüssel generieren

Erstellen Sie nun den Schlüssel für die Kennwortdatenbank auf dem USB-Stick. Stecken Sie den USB-Stick ein. Starten Sie Syskey mit [Windows R] und `syskey`. Klicken Sie auf „Aktualisieren“. Wählen Sie „Systemstartschlüssel auf Diskette speichern“ und klicken Sie auf „OK“. Jetzt erstellt Syskey den Schlüssel und speichert ihn unter dem Namen „StartKey.Key“ im Hauptverzeichnis Ihres USB-Sticks.

Ab sofort lässt sich der PC nur noch mit dem Stick starten. Sollten Sie ihn verlieren oder sollte er kaputtgehen, dann müssen Sie Windows neu installieren. Speichern Sie sicherheitshalber „StartKey.Key“ auf einem zweiten USB-Stick, dem Sie ebenfalls den Laufwerkbuchstaben „A:“ zuweisen.

PC-Schutz wieder rückgängig machen

Bitte beachten Sie: Wenn Sie einmal mit Syskey die Kennwortdatenbank verschlüsselt haben, dann lässt sich das nicht wieder zurücknehmen. Es gibt trotzdem zwei Möglichkeiten, den PC-Start wieder zu vereinfachen.

Sie können einmal in Syskey „Kennwort für den Systemstart“ wählen und das Kennwortfeld leer lassen. Dann müssen Sie beim PC-Start nur noch die Eingabetaste drücken.

Eine andere Möglichkeit ist, in Syskey auszuwählen, dass der Schlüssel lokal, also auf der Festplatte, gespeichert wird. Dann läuft der PC-Start ohne Nachfrage durch. Das geht so lange gut, wie die Festplatte nicht defekt ist an der Stelle, an der der Schlüssel gespeichert ist. Sollte das passieren, müssten Sie mit einem Rettungssystem Ihre Daten retten und Windows neu installieren. ■

Oliver Ehm
sonderheft@com-magazin.de

Weitere Infos

- www.microsoft.com/germany/technet/sicherheit/newsletter/securitymanagement.mspx#EQD
  Tipps zu Syskey und weitere Security-Tipps von Microsoft

WinBooks 2.0

Wichtige Kontaktadressen

Fragen zum Abonnement
Neue Mediengesellschaft
Telefon (018 05) 00 25 23
(0,14 Euro/Min. aus dem Festnetz,
Mobilfunk max. 0,42 Euro/Min.)
Fax (018 05) 00 31 73
(0,14 Euro/Min. aus dem Festnetz,
Mobilfunk max. 0,42 Euro/Min.)
aboservice@com-magazin.de

DVD defekt?
Neue Mediengesellschaft
Telefon (018 05) 00 25 23
(0,14 Euro/Min. aus dem Festnetz,
Mobilfunk max. 0,42 Euro/Min.)
aboservice@com-magazin.de

Leserbriefe
Lob, Kritik und Anregungen sind uns jederzeit willkommen. Ihre E-Mail richten Sie bitte an
sonderheft@com-magazin.de

DVD-Redaktion
Vorschläge für Inhalte der Heft-DVD richten Sie bitte an
cd@com-magazin.de

Pressemitteilungen
Wenn Sie uns Pressemitteilungen zukommen lassen wollen, schicken Sie diese bitte an
redaktion@com-magazin.de

Bitte haben Sie Verständnis, dass wir keinen Support für die Software auf der Heft-DVD leisten können. Bei Fragen zu einem Programm wenden Sie sich bitte an den Hersteller.

Impressum

Das Computer-Magazin com!

ISSN 1612-7358
Redaktion, Anzeigen, Vertrieb:
Bayerstraße 16a, 80335 München
Postfach 20 15 52, 80015 München
Telefon (089) 741 17-0
Fax (089) 741 17-132

Mail: redaktion@com-magazin.de
Internet: www.com-magazin.de
Verlag: Neue Mediengesellschaft Ulm mbH, Karlstraße 41, 89073 Ulm
Registergericht Ulm HRB 723869
Sitz der Gesellschaft ist Ulm

Chefredakteur
Roland Bischoff (bif, verantwortlich)

Redaktion
Johann Sedlbauer (hs)
Andreas Dumont (ad)
Oliver Ehm (oe)
Andreas Th. Fischer (afi)
Stefan Kuhn (stk)
Konstantin Pfliegl (kpf)
sonderheft@com-magazin.de

Schlussredaktion
Linda Drasal

DVD-Redaktion und -Produktion
Johann Sedlbauer,
Mahmut Kursun,
Linda Drasal

Art Directorin
Maria-Luise Sailer

Grafik & Bildredaktion
Alfred Agatz, Dagmar Breitenbauch, Catharina Burmester, Harun Hosic, Manuela Keller, Susanna Knevels, Simone Köhnke, Simone Meyer, Petra Reichenspurner, Ilka Rüther, Mathias Vietmeier, Melanie Wallner

Webauftritt com-magazin.de
S2 Intermedia
www.s2intermedia.de

Redaktionsassistenz
Daniela Richter
redaktion@com-magazin.de
Telefon (089) 741 17-302
Fax (089) 741 17-132

Verlag Geschäftsführer
Thomas Perskowitz,
Dr. Günter Götz,
Florian Ebner

Herstellung
Sybille Schreiber (Leitung)
sybille.schreiber@nmg.de

Redaktionstechnik
Tobias Ebner,
Ernst Altmannshofer

Anzeigenberatung

PLZ-Bereich 1, 2, 4, 5, International
Bettina Günther
(verantwortlich für den Anzeigenteil)
Telefon (089) 741 17-801
Fax (089) 741 17-260
bettina.guenther@com-magazin.de

PLZ-Bereich 3, 6, 7, 8, 9, 0
Stefan Bader
Telefon (089) 741 17-668
stefan.bader@com-magazin.de

Key Account Manager Online
Doris Hollenbach
Tel. (089) 741 17-669
doris.hollenbach@com-magazin.de

Anzeigenkoordination
Sybille Schreiber (Leitung)
sybille.schreiber@nmg.de

Anzeigen-Dispo
Susanne Martorana
Telefon (089) 741 17-257
Fax (089) 741 17-115
susanne.martorana@nmg.de

Es gilt die Anzeigenpreisliste vom 1.1.2011

Vertrieb
Rainer Herbrecht
herbrecht@ebnerverlag.de

Vertriebskooperationen
Sybille Schreiber
sybille.schreiber@nmg.de

Heftpreis
com! Sonderheft: Sicherheit mit Heft-DVD
Einzelverkaufspreis:
8,90 Euro

Vertrieb Einzelhandel
asv vertriebs GmbH
Süderstraße 777
20097 Hamburg
Telefon (040) 34 72 40 41

Sonderdrucke
Gerda Uhl
gerda.uhl@nmg.de
Telefon (089) 741 17-338
Fax (089) 741 17-189

Vorstufe
Neue Mediengesellschaft Ulm mbH
Bayerstraße 16a
80335 München

Druck
L. N. Schaffrath GmbH & Co. KG
Marktweg 42-50
47608 Geldern

Dieses com! Sonderheft wird auf chlorfrei gebleichtem Papier gedruckt.

Nachdruck nur mit schriftlicher Genehmigung des Verlags. Die Aufnahme in Online-Dienste und Internet und die Vervielfältigung auf Datenträger wie CD-ROM, DVD-ROM et cetera dürfen nur nach vorheriger schriftlicher Zustimmung des Verlags erfolgen. com! Sonderheft: Sicherheit darf nur mit Verlagsgenehmigung in Lesezirkeln geführt werden.

Haftung Für den Fall, dass in com! Sonderheft: Sicherheit unzutreffende Informationen oder in veröffentlichten Programmen oder Schaltungen Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlags oder seiner Mitarbeiter in Betracht. Verlag und Redaktion haften nicht für unverlangt eingesandte Manuskripte, Fotos und Illustrationen sowie Produkte.

wiwobooks2.0

Die Seite zum Heft

Updates zum Heft

Artikel-Archiv

Security-News

Tipps & Tricks

com!-Tools

www.com-magazin.de

Copyright © 2011 Symantec Corporation. Alle Rechte vorbehalten. Symantec, das Symantec Logo, Norton AntiVirus und Norton Internet Security sind Marken oder eingetragene Marken der Symantec Corporation oder ihrer verbundenen Unternehmen in den USA und in anderen Ländern.

Wobooks 2.0

Cybercrime bereitet realen Schmerz.

Ignorieren

Reagieren

PC Pr@xis Testsieger 02/11

CHIP TESTSIEGER Norton Internet Security 2011 01/2011

PC WELT Test-Sieger Heft 1/2011

Die kriminelle Energie von Online-Gangstern nimmt zu. Sie stehlen Passwörter, dringen in Deine Privatsphäre ein und verschicken Tag für Tag Milliarden infizierter E-Mails. Im Jahr 2009 hat das Bundeskriminalamt (BKA) 207.000 Fälle mit dem „Tatmittel Internet" registriert, die Angriffe auf Bankkonten sind dabei um mehr als 60% gestiegen. Norton schützt Dich vor digitalen Gefahren – intelligent und schnell. www.norton.de