



## Eset NOD32 Antivirus 4

Ein Jahr kostenloser Virenschutz

## Knoppicillin 7.0.1

Notfallpaket mit drei Virenscannern

## BackTrack 4

Netzwerke, System und Anwendungen prüfen

## c't Bankix 9.04.1

Sicheres Internet-Banking (s. S. 95)

## Analyse und Kontrolle

### Windows

BareTail 3.50a  
 c't Helper 1.25  
 ChipCardMaster 6.66  
 DebugBar 5.3  
 FileAlyzer 1.6.0.4  
 Gruppenwechsel2.bat  
 Kafu.exe 1.1  
 MachMichAdmin 4  
 MD5 1.1.18  
 Nmap 5.00  
 OllyDbg 1.10  
 PEiD 0.95  
 Personal Software Inspector (PSI) 1.5.0.0  
 RunAlyzer 1.6.1.24  
 Sleuth Kit 3.0.1  
 Sudo for Windows (sudowin) 0.4.2-r208  
 suDown 2.21  
 TestDisk 6.11.3  
 TrackWinstall 1.1.4  
 WebScarab 1631  
 WinPcap 4.0.2  
 WinSecurityGate 1.0.4  
 Wireshark 1.2.1  
 Wireshark Portable 1.2.1

### Mac OS

Nmap 5.00  
 TestDisk 6.11.3  
 WebScarab 1304  
 Wireshark 1.2.1

### Linux

Nmap 5.00  
 WebScarab 1631  
 xstress 0.375 beta  
 Zenmap 5.00

## Antivirus

### Windows

AVG Anti-Virus Free 8.5.409  
 Avira AntiRootkit Tool 1.1.0.1  
 Avira AntiVir Personal – Free Antivirus 9.0.0.407  
 GMER 1.0.15.15077  
 Radix Anti-Rootkit 1.0.0.9  
 RootKit Hook Analyzer 3.02  
 RootkitBuster 2.52.1013 Beta  
 Sophos Anti-Rootkit 1.5.0  
 SpyBot Search & Destroy 1.6.2.46  
 ThreatFire 4.5.0

### Linux

Avira AntiVir Personal – Free Antivirus 3.0.5

### Mobile

SpyBot Search & Destroy Mobile 0.3

## Datenschutz

### Windows

ATA Security Service 1.1  
 backup.bat  
 Eraser 5.8.7  
 Eraser Portable 5.82  
 GnuPT 3.6.6  
 Gpg4win 2.0.0  
 GPGshell 3.73  
 KeePass Password Safe 2.08  
 KeePassX 0.4.0  
 MySQLDumper 1.24  
 Safey 1.0.0.3  
 TrueCrypt 6.2a

### Mac OS

ATA Security Service 1.0.1  
 KeePassX 0.4.0  
 MySQLDumper 1.24  
 TrueCrypt 6.2a

### Linux

ATA Security Service 5.9  
 KeePassX 0.4.0  
 MySQLDumper 1.24

### Mobile

KeePassMobile 0.06

## Online-Banking

### Windows

GnuCash 2.3.4  
 GnuCash Portable 2.2.8  
 Hibiscus 1.10

### Mac OS

Hibiscus 1.10

### Linux

Hibiscus 1.10  
 KMyMoney2 0.9.3

## Sicher surfen

### Windows

Enigmail 0.96.0  
 Enigmail deutsches Sprachpaket 0.96.0  
 Firefox 3.5.2  
 Firefox Portable 3.5.2  
 FlashBlock 1.5.11.2  
 freeSSHd 1.2.5  
 JSView 2.0.5  
 NoScript 1.9.8.4  
 Opera 9.64  
 Sandboxie 3.38  
 Thunderbird 2.0.0.23  
 Thunderbird Portable 2.0.0.23

### Mac OS

DansGuardian 2.10.1.1  
 Enigmail 0.96.0  
 Enigmail deutsches Sprachpaket 0.96.0  
 Firefox 3.5.2  
 FlashBlock 1.5.11.2  
 JSView 2.0.5  
 NoScript 1.9.8.4  
 Opera 9.64.5270  
 Thunderbird 2.0.0.23

### Linux

DansGuardian 2.10.1.1  
 Enigmail 0.96.0  
 Enigmail deutsches Sprachpaket 0.96.0  
 Firekeeper 0.3.1  
 FlashBlock 1.5.11.2  
 JSView 2.0.5  
 NoScript 1.9.8.4

## Tools

### Windows

FileZilla 3.2.7.1  
 FileZilla Portable 3.2.7  
 IMAPSize 0.3.7  
 Pismo File Mount Audit Package build 053  
 PuTTY beta 0.60  
 SQLite Database Browser 1.3  
 SQLiteSpy 1.8.10  
 UNetbootin (Universal Netboot Installer) 357  
 WinSCP 4.1.9  
 WinSCP Portable 4.1.9

### Mac OS

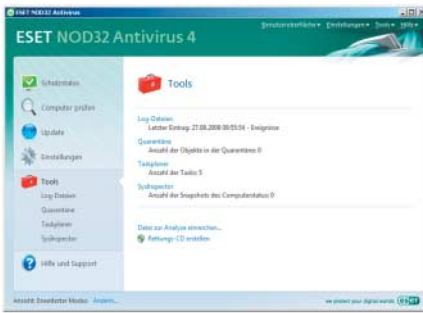
FileZilla 3.2.7.1  
 SQLite Database Browser 1.2  
 TimeMachineEditor 2.2  
 TimeMachineScheduler 2.3.1

### Linux

SQLite Database Browser 1.3  
 UNetbootin (Universal Netboot Installer) 356

### Mobile

PuTTY for Symbian OS S60 3rd 1.5.1



## Eset NOD32 Antivirus

Ohne mitlaufenden Virenschutz sollte man heutzutage keinen Windows-Rechner mehr betreiben. Eset bietet Lesern des *c't kompakt Security* eine einjährige Lizenz von NOD32 Antivirus 4 an, inklusive aller Updates und Signaturen.

Zwar gibt es einige wenige kostenlose Virens Scanner, doch fehlen meist wichtige Komponenten, zum Beispiel Rootkit-Erkennungen. Eset NOD32 Antivirus ist dagegen eine Vollversion, die nach Registrierung ein Jahr lang kostenlos genutzt werden kann.

Den dafür notwendigen Nutzernamen und das Passwort erhält man mit Hilfe des individuellen Berechtigungs-Codes, der auf der Heft-DVD im weißen Feld aufgedruckt ist. Diesen Code gibt man in einem Online-Formular ein (Link auf der Heft-DVD), zusammen mit der Mail-Adresse.

Eine Bestätigungs-Mail folgt mit dem Hinweis, dass innerhalb einer Stunde eine weitere Mail mit Nutzernamen und Passwort kommt. Erst danach sollte das Antivirenpaket von DVD installiert werden. Entweder gibt man nach Aufforderung während der Installation diese Kenndaten ein oder nach der Installation im Eingangs-menü von NOD32 Antivirus („Update“, „Lizenzdaten eingeben“). Nicht nervös werden, wenn die Lizenz nicht überprüft werden kann oder nur wenige Wochen anzeigt: Beim nächsten Update erkennt NOD32 die Lizenz für ein Jahr an. Die Anmelde-Prozedur muss bis zum 28. 10. 2010 erfolgen.

Eset NOD32 Antivirus eignet sich wegen seiner übersichtlichen Bedienoberfläche mit nur wenigen Einstellmöglichkeiten besonders für Einsteiger, die ohne viel Konfiguration sofort loslegen wollen. Zu Optionen wie benutzerdefinierte Scans und Taskplaner gelangt man erst nach Änderung des Standardmodus (kleine Schrift am unteren linken Rand). Einen ausführlichen Test von Antiviren-Software finden Sie im Sonderheft. (jr)



## Knoppicillin

Wenn der installierte Virens Scanner versagt oder von Schädlingen lahmgelegt wird, das Betriebssystem hoffnungslos verseucht ist, dann schlägt die Stunde von Knoppicillin auf der Heft-DVD, einer garantiert virenfreien Umgebung.

Das Notfallsystem bootet direkt von der DVD. Vier Optionen stehen für Knoppicillin zur Verfügung: *Knoppicillin 7*, *HD-Update*, *failsafe* und *Diagnose-Knoppix*. Meist kommt die erste in Frage. Ohne Installation auf der Festplatte startet ein Live-Linux, fragt unter Umständen nach einem Netzwerk (LAN, WLAN, Einwahl per DSL oder Modem) und holt sich Updates. Die sind unbedingt notwendig für die drei integrierten Virens Scanner von Avira, BitDefender und Kaspersky, denn die Signaturen müssen auf dem aktuellen Stand sein.

Wenn die Netzwerkverbindung scheitert, weil etwa die WLAN-Hardware im Notebook nicht erkannt wird, empfehlen wir die LAN-Verbindung per Kabel. Genaues zur Konfiguration, auch für WLAN-Verbindungen, und wie man Knoppicillin auf vielfältige Weise gegen Schädlinge einsetzt, beschreibt ein Artikel im Sonderheft.

Nach den Updates erscheint ein Schnellstart-Menü mit einigen wenigen Fragen zum anstehenden Virens Scan. Auch unerfahrene Anwender kommen damit zurecht und sehen rasch, wie es um ihren Rechner steht. Das Menü enthält auch Tools für ein Backup, falls der Rechner komplett streikt und man Daten auf externe Medien retten möchte.

Die Boot-Option *Diagnose-Knoppix* führt zu einer grafischen Bedienoberfläche, von der aus unter anderem E-Mail-Client, Browser und Editor zu erreichen sind. Damit kann man zum Beispiel unterwegs auch dann mit dem Rechner arbeiten, wenn Schädlinge die Installation zerstört haben, oder man möchte sich online über die von den Virens Scannern gefundene Malware informieren. (jr)



## BackTrack 4

Die Linux-Live-Distribution BackTrack 4 ist rund 1,2 GByte groß und enthält über 300 freie Security-Tools, darunter Netzwerk-analysatoren, LAN-, WLAN-, Bluetooth-Scanner und Passwort-Tester.

Schwachstellen in der eigenen IT-Infrastruktur lassen sich mit BackTrack schnell und ohne Installation aufspüren. Auf dem bootfähigen Teil der DVD sind von den sieben Startoptionen die ersten beiden wichtig, sie unterscheiden sich lediglich in der erforderlichen Bildschirmauflösung (XGA oder SVGA). Option Nummer drei *Backtrack Forensics* ignoriert die Festplatte. Die restlichen Optionen sind Spezialfälle (Infos dazu unter [www.remote-exploit.org](http://www.remote-exploit.org)).

Nach dem Booten führt die Eingabe von *startx* in der Kommandozeile zu einem KDE-Desktop. BackTrack findet erst nach Aufforderung seinen Weg ins Netz, beispielsweise per `dhclient eth0` in einer Shell. WLAN steht nach `ifconfig wlan0 up` bereit. Das Programm-Menü „Backtrack“ listet zahlreiche Haupt- und Untertabellen, um die Hunderte von Tools einigermaßen sinnvoll zu gruppieren.

Viele davon kann man nicht nur als Verteidigungs- oder Diagnose-Tool, sondern auch gegen fremde Systeme einsetzen – durchaus versehentlich. Missbrauch ist strafbar, man sollte ein Tool also erst dann nutzen, wenn man genau weiß, was man tut. Das Sonderheft gibt einen Einstieg in das umfangreiche Programmpaket.

*Ettercap* zum Beispiel leitet den Netzwerkverkehr über den eigenen PC um und attackiert damit als Man-in-the-Middle. Es eignet sich zur Überprüfung von Online-Backup-Diensten, ob diese User-Daten bei der Übertragung tatsächlich verschlüsseln. Unterm Strich bringt BackTrack viele Erkenntnisse und inspiriert, sich mit dem riesigen Funktionsumfang zu beschäftigen, auch wenn für viele Tools eine gehörige Portion Vorwissen und damit meist eine zeitintensive Einarbeitung nötig ist. (jr)