

Wurmkur ohne Nebenwirkung – Virenentfernung mittels Live-CDs

von Bodo Schmitz

Neben den zumeist kostenpflichtigen Virens Scannerlösungen gibt es auch einige – zumeist linuxbasierte – Angebote, die sich wunderbar dazu eignen, digitalem Ungeziefer unter Windows zu Leibe zu rücken. Teilweise basieren sie auf freien Virens Scanner-Engines (z. B. clamav) oder sie stellen freie Varianten ansonsten kostenpflichtiger Lösungen dar.

Es ist vergleichbar zum realen Leben: Die Erkältung erwischt einen immer im falschen Moment! Genau so fällt die Infektion des Windows-PCs immer genau dann auf, wenn ein zeitkritischer Job zu erledigen ist. Dem lässt sich neben einer Gesamtsicherung des Systems mit möglichst mehreren der hier vorgestellten CDs beikommen.

Das Ganze hat aber noch eine Besonderheit: Inzwischen gibt es Schädlinge, die erkennen können, ob ein bestimmter Virens Scanner installiert ist. Finden sie einen Scanner, werfen sie diesen kurzerhand aus dem Speicher, deinstallieren ihn oder manipulieren schlichtweg dessen Scan-Ergebnisse. Somit kann man sich heutzutage nicht mehr auf die Resultate eines installierten Virens Scanners verlassen und sollte seinen Rechner ergänzend mit – garantiert nicht manipulierbaren – Live-CDs überprüfen. Selbst wenn man mit Windows arbeiten muss oder will und keine Ahnung von Linux hat, ist der Einsatz der hier beschriebenen CDs somit sinnvoll, um die Chancen, das lästige digitale Ungeziefer loszu-

werden, beträchtlich zu erhöhen. Vielleicht weckt das dann darüber hinaus noch die Lust auf eine höhere Dosis Linux ...

Die meisten CDs beinhalten inzwischen das Paket **ntfs-3g** [1], welches nahezu perfekten Schreibzugriff auf NTFS-formatierte Festplatten ermöglicht, sodass eine Vielzahl gefundener Viren zuverlässig entfernt, oder zumindest umbenannt bzw. in Quarantäne geschickt werden kann. Da sich Desinfektionsleistung sowie Scan-Ergebnisse der verschiedenen CDs unterscheiden, sollten unbedingt mehrere CDs eingesetzt werden. Der Einsatz mehrerer CDs nacheinander verhindert außerdem, dass sich die verschiedenen Virens Scanner in die Quere kommen.

Nicht alle CDs können große Dateien, Postfächer, Archive oder die Windows-Auslagerungsdatei scannen. Bei einigen lassen sich entsprechende Optionen setzen, einige der anderen quittieren den Versuch lediglich mit einer Fehlermeldung. Dies birgt natürlich ein gewisses Gefahrenpotential aufgrund möglicherweise nicht erkannter Schädlinge. Daher ist ein möglichst zahlreicher Einsatz der hier vorgestellten CDs ratsam.

Die Scan-Geschwindigkeit der einzelnen Programme variiert teilweise sehr stark, sodass für die vollständige Untersuchung des Rechners ein paar Stunden freigehalten werden sollten. Möglichst sollte der Scan-Vorgang auf Zeiten gelegt werden, in denen der Rechner nicht dringend benötigt wird.

Die Bedienung der häufig eingedeutschten CDs ist meist selbsterklärend und graphisch geführt, dennoch sollen hier einige Hinweise zu deren Bedienung und Besonderheiten folgen. Eine Ausnahme stellt die konsolenbasierte OpenDiagnostics-Live-CD dar, die mit ein paar (Debian-)Linux-Kenntnissen aber auch leicht einsetzbar ist.

Bei sämtlichen der hier getesteten CDs funktionieren USB-Tastaturen am Bootprompt nicht. Somit wird eine PS/2-Tastatur bzw. ein passender Adapter benötigt, da sonst am Bootprompt keine Optionen gesetzt werden können. Nach dem Booten des Rechners funktionieren USB-Tastaturen selbstverständlich wie gewohnt.

Obwohl der aktuelle Bootmanager grub2 inzwischen ISOs booten kann, ließ sich keine der hier getesteten CDs auf diesem Wege vom USB-Stick starten. UNetbootin [2] kann laut Herstellerangaben einige der hier behandelten CDs starten, daher bieten sich weitere Experimente mit diesem und ähnlichen Programmen oder Skripten an. Kaspersky bietet ein Windows-Programm zum Download an.

Die Überprüfung verschlüsselter Linux-Partitionen klappt bei keiner der hier vorgestellten CDs out-of-the-box, ist aber prinzipiell möglich, soweit der Anwender den Umgang mit cryptsetup [3] in der Konsole beherrscht und das Paket vorhanden ist oder sich im Live-Betrieb nachinstallieren lässt. Dies darf auch als Aufruf an die



Hersteller verstanden werden, denn dass das automatische Einhängen verschlüsselter Partitionen beim Bootvorgang funktionieren kann, beweist die Finnix-Live-CD [4].

Mit der für Windows geeigneten Variante TrueCrypt [5] ist bei einigen der hier vorgestellten CDs der Zugriff auf verschlüsselte Festplatten per Hand möglich, seitdem der Hersteller das Programm so umgebaut hat, dass die lästige Kernel-Kompilierung nicht mehr nötig ist. Wenn man den Installer anweist, die Programmdateien auszupacken, statt sie zu installieren, kann man diese anschließend via USB-Stick über eine root-Shell ins laufende Live-System kopieren (z. B. per mc) und dann das verschlüsselte Windows-System händisch einbinden. Gegebenenfalls muss dann noch der Virens Scanner neu gestartet werden, damit er das eingebundene Windows-System erkennt. Da bei manchen Virens Scanner-CDs nur Zugriff über die Konsole besteht und das Hauptprogramm den gesamten Desktop ausfüllt, empfiehlt es sich, sowohl die GUI- als auch die Konsolenvariante von TrueCrypt auf dem USB-Stick bereitzuhalten. Grundlagen zur Konsolenvariante sind im Wiki von ubuntuusers.de nachzulesen [6]. Informativ ist auch die TrueCrypt-eigene Hilfe mittels

```
$ truecrypt --help
```

Verschlüsselte Partitionen bzw. Container lassen sich in der Konsole folgendermaßen einhängen; entsprechende Mount-Punkte müssen eventuell vorher manuell angelegt werden:

```
# truecrypt --mount /dev/sda1 /mnt/windows # bzw.
# truecrypt --mount container.tc /mnt/windows
```

Sämtliche verschlüsselte Datenträger werden über

```
# truecrypt -d
```

wieder ausgehängt.

Hinweis: Um bei den Ubuntu-basierten CDs nicht – wie in unzähligen Quellen angegeben – bei jeder Befehlszeile **sudo BEFEHL ...** regelmäßig das Benutzerpasswort eintippen zu müssen, wechselt man lieber direkt per **sudo -i** in den root-Kontext [7]. Verlassen kann man diesen wieder mit dem Befehl **exit** und sich für die Dauer der root-Sitzung das **sudo** sparen.

Achtung: Im BIOS des Rechners muss die richtige Boot-Reihenfolge eingestellt sein, damit die Virens Scanner-CDs starten können. Moderne Rechner können inzwischen per Tastendruck (meist eine der Funktionstasten) ein manuelles Boot-Auswahlmenü aufrufen.

Die Reihenfolge der hier vorgestellten CDs ist alphabetisch und stellt keine Wertung dar. Von Zeit zu Zeit ändern sich die Links der Webseiten, so dass die Quellen der CDs gegebenenfalls neu gesucht werden müssen.

Neben den hier vorgestellten sieben Live-CDs finden sich im Netz weitere Angebote. Außerdem liegt der Computerzeitschrift c't [8] alle sechs Monate die Variante Desinfec't [9] (früher Knoppcillin) bei, die jeweils mit zwei bis drei

Virens Scannern mit zeitlich befristeten Lizenzschlüsseln (die aber den sechsmonatigen Zeitraum abdecken) ausgestattet ist; allerdings ohne Download-Möglichkeit der aktuellen ISO-Datei.

Das Übel an der Wurzel packen – Rootkit-Suche über Live-CDs

Für Linux gibt es zwei Lösungen, um nach diesen perfiden Schädlingen zu suchen. Eine gute Anleitung zu Einrichtung und Betrieb von **chkrootkit** und **rkhunter** findet sich auf Uçk-Anleitungen [10]. Packt man die genannten tar.gz-Archive auf einem USB-Stick aus, lassen sich diese Programme auch bei den Live-CDs, welche eine root-Shell beinhalten, einsetzen. Eine detaillierte Beschreibung zu Installation und Einsatz dieser Werkzeuge passen leider nicht in den Rahmen dieses Artikels.

Avira AntiVir Rescue CD

Die Avira AntiVir Rescue CD (ISO-Image [11]) bootet nach ca. 20 Sekunden selbstständig oder durch Druck auf die Eingabetaste. Sie bindet automatisch die gefundenen Partitionen ein und startet die graphische Oberfläche mitsamt dem Virens Scanner. Sie beinhaltet ntfs-3g, basiert auf einem Standard-Linux-Kernel und bemerkt eine fehlende Netzverbindung sowie eine veraltete Viren-Datenbank. Eine manuelle Einrichtung des Netzwerks, mitsamt anschließender Aktualisierung der Viren-Datenbank ist aber möglich. Die Lokalisierung ist vollständig und kann ohne Neustart des Programms geändert werden. Li-

nuxtypisch kann man per **Strg** + **Alt** + **F1** auf die Konsole wechseln; die Rückkehr zum Hauptfenster erfolgt per **Strg** + **Alt** + **F7**. Die Konfiguration des Programms ist selbsterklärend und auch für Normalanwender verständlich. Nach dem Herunterfahren des Rechners muss man sich beim Entnehmen der CD beeilen, da die Schublade des Laufwerks nach 1-2 Sekunden automatisch geschlossen wird. Der Zugriff auf verschlüsselte Linux-Festplatten ist mangels `cryptsetup` nicht möglich und lässt sich aufgrund eines fehlenden Paketmanagers nicht nachinstallieren. TrueCrypt lässt sich aber nach der oben beschriebenen Vorgehensweise in der Konsolen-Variante ins Livesystem kopieren. Die verschlüsselten Datenträger sollten irgendwo unterhalb von `/media/Devices/` eingebunden werden. Gegebenenfalls müssen die Mount-Punkte händisch angelegt werden.

Bitdefender Rescue CD

Die Bitdefender Rescue CD (ISO-Image [12]) basiert zurzeit auf Ubuntu 9.10 „Karmic Koala“ [13] und lässt somit den Zugriff auf die Konsole zu. Nach dem Start der graphischen Oberfläche müssen zunächst die Lizenzbedingungen abgenickt werden. Ganz ubuntu-typisch wechselt man per

```
$ sudo bash
```

in den root-Kontext. Fehlt die Internetverbindung wird der Anwender darauf hingewiesen. Ansonsten aktualisiert der automatisch gestartete Scanner seine Datenbank und startet an-

schließend selbstständig den Scan-Vorgang. Per **Strg** + **Alt** + **F1** geht es zur Konsolenvariante des Scanners. Diese Variante wird auch gezeigt, falls die graphische Oberfläche nicht gestartet werden kann. Auf den folgenden Funktionstasten liegen die üblichen normalen Textkonsolen. Zurück zur graphischen Oberfläche geht es per **Strg** + **Alt** + **F7**.

Der Bitdefender Rescue CD fehlt das Paket `cryptsetup`; seit Ubuntu 9.10 „Karmic Koala“ lässt es sich aber im Live-Betrieb lauffähig nachinstallieren. Dazu ist als root Folgendes auszuführen:

```
# apt-get update
# apt-get install cryptsetup
```

TrueCrypt lässt sich per root-Shell in der GUI-Variante ins laufende System kopieren. Der zugehörige Startmenü-Eintrag ist direkt vorhanden. Die verschlüsselten Datenträger sollten manuell unterhalb von `/media` eingebunden werden. Anschließend empfiehlt es sich den Virens scanner neu zu starten, damit er die verschlüsselten Datenträger zuverlässig erkennt.

Achtung: Sowohl die Textkonsole, als auch das graphische Terminal unterstützen ausschließlich die amerikanische Tastaturbelegung! Eine manuelle Konfiguration und Aktualisierung ist aber möglich. `ntfs-3g` ist enthalten, sodass ein zuverlässiger Schreibzugriff auf Windows-Systeme möglich ist. Truecrypt lässt sich per USB-Stick ins Live-System übertragen und von Hand „nachinstallieren“.

F-Secure Rescue CD 3.11

Auch diese nur auf englisch laufende MicroKnoppix-basierte CD von F-Secure [14] [15] startet nach 15 Sekunden Wartezeit automatisch mit amerikanischem Tastaturlayout.

`cryptsetup` fehlt ebenfalls, lässt sich aber wie bei der Bitdefender Rescue CD beschrieben zur Laufzeit „nachinstallieren“. `ntfs-3g` ist aber vorhanden.

TrueCrypt lässt sich in der Konsolen-Variante benutzen. Damit der Virens scanner die verschlüsselten Datenträger auch zuverlässig erkennt, müssen diese bis spätestens zum Punkt Lizenzbedingungen manuell unterhalb von `/mnt` eingebunden werden.

Während des Bootvorgangs wird der Anwender auf die Möglichkeit, dass nach einer Desinfektion virenbefallener Systemdateien das installierte System möglicherweise nicht mehr startet, hingewiesen, was mit Druck auf „Next“ zur Kenntnis genommen werden muss. Nach Meldung der evtl. nicht erreichbaren Viren-Datenbank müssen noch die Lizenzbedingungen akzeptiert werden (Druck auf „Next“, „I Agree“). Nach Auswahl der (standardmäßig bereits ausgewählten) zu scannenden Laufwerke und des Master Boot Records (MBR [16]) kann der Scan-Vorgang gestartet werden. Zwar startet diese CD keine graphische Oberfläche, die konsolenbasierte Navigation ist allerdings laientauglich. Mit **Alt** + **F5** wird die Liste der gescannten Dateien angezeigt, **Alt** + **F6** listet die gefundenen Schädlinge und **Alt** + **F1**



führt zum Hauptfenster zurück. Hinter den anderen Funktionstasten-Kombinationen liegen die linux-typischen Konsolen im root-Kontext.

Nach dem Beenden des Scan-Vorgangs kann durch Druck auf die Eingabetaste der Bericht angezeigt werden.

Abschließend kann die Viren-Datenbank aktualisiert und der Rechner erneut gescannt oder neu gestartet werden.

Kaspersky Rescue Disc 10

Am Bootprompt dieser Gentoo-basierten CD von Kaspersky (ISO-Image [17]) kann man innerhalb von zehn Sekunden per Tastendruck zur Sprachauswahl gelangen. Auf dem nächsten Schirm erfolgt die Wahl der Startart. Die Option „Kaspersky Rescue Disk. Grafikmodus“ stellt eine gute Wahl dar. Anschließend werden die Lizenzbedingungen akzeptiert. Der Startvorgang kann recht lange dauern und so erscheinen, als ob

sich der Rechner aufgehängt hat. Daher sollte länger als sonst üblich gewartet werden, bis sich der Rechner wieder meldet und auf Eingaben reagiert. Nach dem Start der graphischen Oberfläche wird – soweit verfügbar – die Netzverbindung eingerichtet und der Scanner wartet auf Anweisungen des Benutzers. Die rote Lampe zeigt, dass noch nicht alle Einstellungen korrekt vorgenommen wurden bzw. die Viren-Datenbank veraltet ist. Daher sollte das Programm zunächst durch Klick auf „Einstellungen“ rechts oben konfiguriert werden. Im Reiter „Update“ wird die Viren-Datenbank aktualisiert und dann der Scan-Vorgang des Rechners durch Klick auf „Untersuchung von Objekten starten“ gestartet.

ntfs-3g ist vorhanden, die Unterstützung für verschlüsselte Laufwerke fehlt dagegen vollständig. Aufgrund

eines fehlenden Paketmanagers lässt sich cryptsetup nicht nachinstallieren. Darüber hinaus fehlt ebenfalls die Unterstützung für Overlay-Dateisysteme wie „UnionFS“ [18] oder „aufs“ [19]. Daher lässt sich TrueCrypt ebenfalls nicht „installieren“.

Die CD wird nach dem Herunterfahren bzw. vor dem Neustart des Rechners nicht ausgeworfen; daher muss sie von Hand entfernt werden.

Unter der o. g. Download-Adresse findet sich übrigens ein Windows-Programm, mit dem man die CD auf einen USB-Stick übertragen kann („Rescue2usb“).

OpenDiagnostics Live-CD

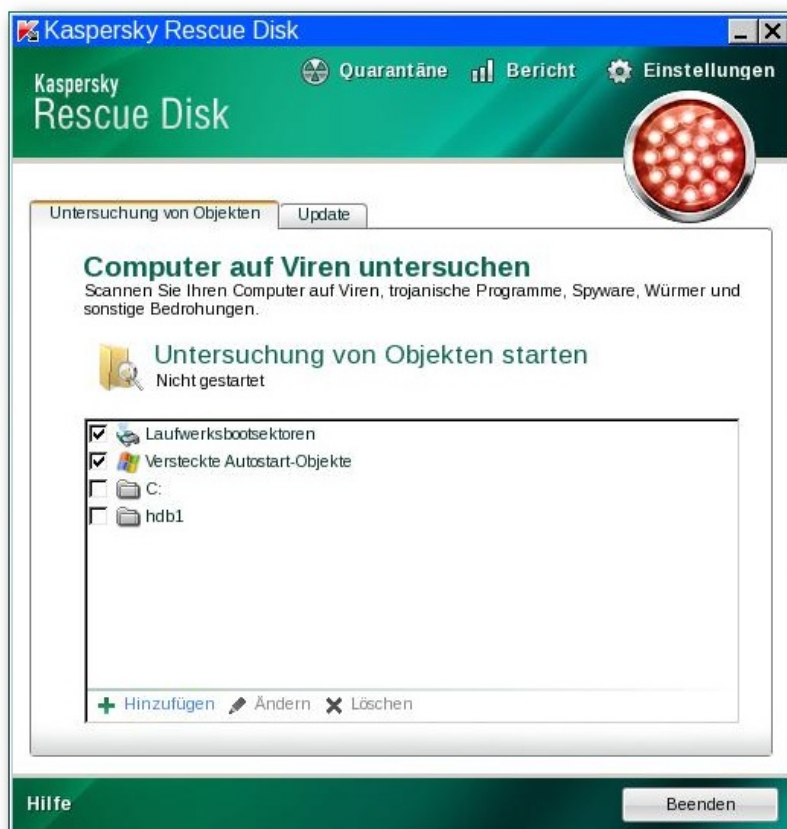
Die OpenDiagnostics Live-CD [20] stellt die Weiterentwicklung der ClamAV-Live-CD dar und wird per Konsole mit amerikanischer Tastenbelegung bedient. Somit ist hier eine etwas ausführlichere Beschreibung nötig, um diese CD auch Linux-Anfängern zugänglich zu machen. Debian- bzw. Ubuntu-Anwendern wird das meiste davon bekannt vorkommen.

Nach dem Booten sollte man zunächst per

```
$ sudo -i
```

in den root-Kontext wechseln. Soweit der Rechner über genügend Arbeitsspeicher verfügt, kann per

```
# apt-get update
# apt-get upgrade
```



Graphische Oberfläche der Kaspersky Rescue Disc. 🔍

die CD virtuell „aktualisiert“ werden. Das betrifft dann auch den Virens Scanner selbst. Unterstützung für NTFS und verschlüsselte Festplatten kann per

```
# apt-get update
# apt-get install ntfs-3g
# apt-get install cryptsetup
```

nachgerüstet werden. Die Konsolen-Variante von TrueCrypt lässt sich ebenfalls per USB-Stick einspielen. Für eine angenehmere Navigation durch die Konsole kommt je nach Wunsch noch der Midnight Commander per

```
# apt-get install mc
```

dazu. Um wieder mehr Arbeitsspeicher frei zu bekommen, kann anschließend per

```
# apt-get clean
```

aufgeräumt werden. Die aktuellen Viren-Datenbanken kommen durch **freshclam** und **clamav-unofficial-sigs** aus dem Netz.

Die Partitionen der Festplatte(n) werden per

```
# fdisk -l
```

aufgelistet, da die Mount-Punkte manuell angelegt werden müssen; z. B. durch

```
# mkdir /mnt/sda1
```

Pro Partition wird je ein Mount-Punkt nach diesem Schema angelegt.

Die Partitionen werden nun wie folgt eingebunden: Linux- und FAT-Dateisysteme werden z. B. per

```
# mount /dev/sda1 /mnt/sda1
```

eingehängt. NTFS-Partitionen dagegen werden per

```
# ntfs-3g /dev/sda1 /mnt/sda1
```

eingehängt.

Anschließend wird der Scanner per

```
# clamscan -r -v /mnt/sda1
```

gestartet. Die Option **-r** steht dabei für rekursives scannen, **-v** macht den Virens Scanner sprachiger („verbose“).

Nach Beendigung der Arbeiten werden alle Partitionen nach dem bekannten Schema per

```
# umount /mnt/sda1
```

wieder ausgehängt. Der „Affengriff“ (**Strg** + **Alt** + **Entf**) startet den Rechner neu; der Befehl **halt** fährt ihn herunter.

Panda SafeDisc

Nach dem Start der Panda SafeDisc (ISO-Images [21] [22]) kommt zuerst die Frage nach der gewünschten Spracheinstellung, allerdings werden nur Englisch und Spanisch angeboten. Im nächsten Fenster werden die Partitionen ermittelt, die Netzverbindung hergestellt und das Programm konfiguriert. Ohne eine stehende In-

ternetverbindung kann der Scanner nur mit den auf der Disk befindlichen Viren-Datenbanken verwendet werden. Alternativ bleibt nur Abschalten oder Neustart des Rechners. Die wenigen Optionen des Programms sind allerdings selbsterklärend. Der Zugriff auf verschlüsselte Dateisysteme ist aufgrund fehlender Konsole weder möglich noch nachrüstbar.

PC Tools Alternate Operating System Scanner (AOSS)

Die AOSS-CD [23] startet sofort und ohne Bootprompt. Nach kurzer Zeit erscheint der Sprachauswahldialog, der bereits mit der Maus bedient werden kann. Im nächsten Fenster sind die Lizenzbedingungen abzusegnen. Anschließend erscheint das Hauptmenü der CD-Oberfläche. Dort finden sich neben dem Virens Scanner weitere Dienste (z. B. die Möglichkeit der Datenwiederherstellung bzw. -löschung, eine Konsole, sowie „Scripting“). Hier soll aber nur der Virens Scanner behandelt werden.

Nach Auswahl der Partitionen legt der Scanner direkt los. Der Virens Scanner selbst bietet nicht viele Optionen. Es lassen sich aber sog. „deaktivierte Dateien“ wiederherstellen. Das bietet sich an, wenn infizierte Systemdateien in die Quarantäne gesteckt wurden, und das installierte System daher nicht mehr hochfährt. Man sollte aber bedenken, dass man damit höchstwahrscheinlich den Schädling ebenfalls wiederherstellt.

Eine Unterstützung für cryptsetup fehlt, TrueCrypt kann man über die Systemshell vom Hauptmenü aus nach der unten bei der VBA-Rescue



CD beschriebenen Methode manuell „installieren“. Zusätzlich muss man noch von Hand Zugriffsrechte per

```
# chmod +x /usr/bin/truecrypt
```

setzen. Die Shell mit amerikanischer Tastenbelegung verlässt man mit **exit**.

VBA Rescue

Die Abbild-Datei [24] der VBA Rescue CD wird nahezu täglich neu erzeugt. Am Grub1-Bootprompt hat der Benutzer fünf Sekunden Zeit, um eine Auswahl zu treffen. Neben der Standard-Bootmethode gibt es auch die Wahl alles in den Arbeitsspeicher zu laden („2ram“; das ist für Rechner mit nur einem Laufwerk interessant, da die CD bei dieser Option nach dem Booten ausgeworfen wird), den Speichertest Memtest86+, sowie das Festplatten-Analyse-Tool mhdd. Nach Auswahl des vba32rescue-Images wird die gewünschte Bildschirmauflösung ausgewählt. Auch hier muss sich der Anwender zügig entscheiden. Als nächstes folgt die Sprachauswahl, gefolgt von Hinweisen zur Navigation per Tastatur. In den graphischen Auflösungen funktioniert die Maus allerdings auch. Anschließend gelangt man ins Hauptfenster des Programms. Die möglichen Optionen sind selbsterklärend und gut voreingestellt. Die CD ist zeitlich befristet lizenziert, der Zeitraum verlängert sich aber durch Herunterladen der häufig erneuerten aktuellen Version. Eine Unterstützung für cryptsetup fehlt. TrueCrypt ist aufgrund fehlender Systembibliotheken nicht direkt lauffähig. Von einem instal-

lierten Linux-System (z. B. Debian 5.0 „Lenny“) lassen sich die benötigten drei Systembibliothek aber möglicherweise per USB-Stick „ausleihen“. Benötigt werden `/usr/lib/libfuse.so.2`, `/usr/lib/libstdc++.so.6` und sowie `/lib/libgcc_s.so.1`. ntf5-3g ist aber mit an Bord. Die per Druck auf **Alt** + **Funktionstaste** erreichbaren Konsolen beinhalten trotz deutscher Lokalisierung englische Tastaturbelegung. Das Hauptfenster liegt auf der sechsten Konsole.

Fazit

Ergänzend zum regulär installierten Duo Virens Scanner und Firewall ist gerade auf den stets infektionsgefährdeten proprietären Betriebssystemen der regelmäßige Einsatz der hier exemplarisch vorgestellten Live-CDs sinnvoll, um dem Problem zugriffsgesperrter infektiöser Dateien, manipulierter Scan-Ergebnisse durch Schädlinge oder gar hinauskatapultiertes Virens Scanner vorzubeugen. Seit der komfortablen Integration von ntf5-3g stellt die zuverlässige Entfernung der Schädlinge auf Windows-Systemen kein wirkliches Problem mehr da. Vorsicht ist nur bei leichtfertiger Entfernung infizierter Systemdateien geboten, da dies in einem nicht mehr lauffähigen System enden kann.

Aufgrund der häufig aktualisierten CD-Abbilder mit jeweils den neusten Versionen von Scanner-Engine und Virendatenbank empfiehlt es sich die ISO-Dateien erst bei Bedarf herunterzuladen und auf wiederbeschreibbare Rohlinge (RW) zu brennen, um erhöhtem „Silberschrott“ vorzubeugen.

Da die Scan-Vorgänge teils sehr lange dauern und der Rechner aufgrund des Bootens vom Live-Medium ohnehin nicht anders eingesetzt werden kann, ist es ratsam die Virensuche auf freie Zeiten zu legen. Beim Einsatz der hier gezeigten sieben CDs würde sich beispielsweise eine pro Nacht anbieten. Da die Scan-Ergebnisse bei den jeweiligen CDs voneinander abweichen, ist der Einsatz mehrerer Datenträger unbedingt zu empfehlen.

Die Untersuchung verschlüsselter Linux-Systeme ist leider nur mit einigen der hier vorgestellten CDs möglich. Hier könnten die Hersteller noch Entwicklungszeit investieren, um dem Normalanwender eine klickbare Lösung anzubieten, denn seit mit dem Debian 4.0 „Etch“ Verschlüsselung fast problemlos einrichtbar geworden ist, dürfte diesbezüglich auch entsprechender Bedarf bestehen.

Auf der anderen Seite ist Windows mit Einführung der Pre-Boot-Authentication [25] in TrueCrypt ebenfalls voll-verschlüsselbar geworden.

Ergänzende Sicherheitshinweise








Durch stetigen Einsatz dieser CDs sollte man sich aber nicht in scheinbarer Sicherheit wiegen. Sicherheit ist ein steter und komplizierter Prozess, in dem diese CDs nur einen Teilschritt darstellen. Zusätzlich sollten weitere mögliche Fehlerquellen ausgeschlossen werden: Wechseldatenträger wie CDs und USB-Sticks legt man unter Windows per Druck auf die **Umschalt**-Taste ein und hält diese bis zum Beenden der Daten-

trägerindexierung fest. Das deaktiviert die sogenannte Autorun-Funktion, die sich zur automatischen Infektion von Windows-Rechnern „zweckentfremden“ lässt. Anschließend „öffnet“ man den Datenträger per rechter Maustaste statt ihn zu „starten“, da sonst die Autorun-Funktion nachträglich ausgeführt würde. Wechseldatenträger sollten generell auf Viren überprüft werden – auch diejenigen von guten Freunden!

Das System sollte sicherheitsbewusst konfiguriert werden, denn Sicherheit geht immer vor Komfort. Die eingesetzten Browser sollten durch Erweiterungen abgedichtet werden (siehe z. B. „Gesunde Datenkekse backen – Firefox mit Erweiterungen absichern“ [freiesMagazin 03/2011 \[26\]](http://www.freiesMagazin.de/03/2011)).

Im Übrigen sind die hier beschriebenen CDs allesamt kostenlos erhältlich, was auch die Linux-Anwender freuen dürfte. Daneben sind die Live-CDs hilfreich, dass man nicht unbemerkt verseuchte Dateien weiter an Dritte gibt und so möglicherweise deren Rechner infiziert, selbst wenn der eigene (Linux-)Rechner nicht befallen ist.

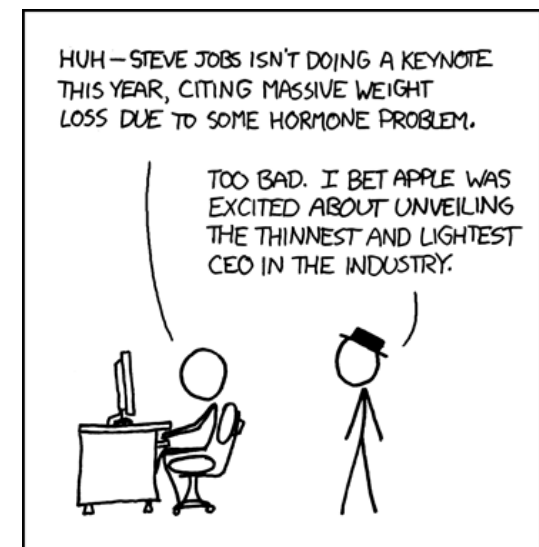
LINKS

- [1] <https://secure.wikimedia.org/wikipedia/de/wiki/NTFS-3G>
- [2] <http://unetbootin.sourceforge.net/> 
- [3] <https://secure.wikimedia.org/wikipedia/de/wiki/Dm-crypt>
- [4] <http://www.finnix.org/> 
- [5] <http://www.truecrypt.org/> 
- [6] <http://wiki.ubuntuusers.de/Archiv/TrueCrypt>
- [7] <http://www.griessler.org/sudo-su-vs-sudo-bash-vs-sudo-i.php>
- [8] <http://www.heise.de/ct/>
- [9] <https://secure.wikimedia.org/wikipedia/de/wiki/Desinfec't>
- [10] <http://uckanleitungen.de/rootkit-scanner-linux/>
- [11] <http://dl.antivir.de/download/vdf/rescuecd/rescuecd.iso>
- [12] http://download.bitdefender.com/rescue_cd/bitdefender-rescue-cd.iso
- [13] http://wiki.ubuntuusers.de/Karmic_Koala
- [14] <http://www.f-secure.com/linux-weblog/2009/09/22/rescue-cd-311/> 
- [15] http://www.f-secure.com/en_EMEA-Labs/security-threats/tools/rescue-cd 
- [16] https://secure.wikimedia.org/wikipedia/de/wiki/Master_Boot_Record
- [17] http://devbuilds.kaspersky-labs.com/devbuilds/RescueDisk10/kav_rescue_10.iso
- [18] <https://secure.wikimedia.org/wikipedia/de/wiki/UnionFS>
- [19] <https://secure.wikimedia.org/wikipedia/de/wiki/Aufs>
- [20] <http://volatileminds.net/node/6/release> 
- [21] <http://www.pandasecurity.com/resources/tools/SafeCD.iso>
- [22] <http://www.pandasecurity.com/resources/sop/SafeCD/PandaSafeCD.iso>
- [23] <http://www.pctools.com/aoss/details/> 
- [24] <http://anti-virus.by/pub/vbarescue.iso>
- [25] https://secure.wikimedia.org/wikipedia/de/wiki/Pre-Boot_Authentication
- [26] <http://www.freiesMagazin.de/freiesMagazin-2011-03>

Autoreninformation

Bodo Schmitz ([Webseite](#)) hat durch seinen Beruf, Zugriff auf eine Vielzahl vireninfiltrierter Windows-PCs und dadurch die Erkenntnis gewonnen, dass man den Scan-Ergebnissen innerhalb eines bereits infizierten Systems nicht wirklich trauen kann.

Diesen Artikel kommentieren 



„Keynote“ © by Randall Munroe (CC-BY-NC-2.5), <http://xkcd.com/527>