linuxUSER

Knoppix: Exklusive Medialinx-Edition S. 14

linuxUSER
04.2014

KNOPPIX • MAGEIA • MINECRAFT • SYSTEMD • TRIPWIRE • PORTABLES LINUX

Optimale Live-Distris und Multiboot-Installer für das Linux-to-go auf dem USB-Stick

PORTABLES LINUX

Desktops maßschneidern mit der Baukasten-Distri Tiny Core Linux S. 44

SD-Cards und USB-Sticks: Performance optimieren und die Lebensdauer erhöhen S. 22

Komfortable Werkzeuge für das Multiboot per Mausklick, die besten Live-Systeme für unterwegs im Vergleich S. 28, 36

Systemd bringt Einheit unter die Linux-Haube S. 80

Wie das neue Init-System alte Zöpfe abschneidet und für rasantes Booten sorgt

Quirliger Web-Neuling S.54

Ergonomischer Webbrowser Qupzilla

Penibler Einbruchschutz S.74

HIDS Tripwire schlägt bei Attacken Alarm

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

Top-Distris auf zwei Heft-DVDs

EUR 8,50 Deutschland | EUR 9,35 Österreich | sfr 17,00 Schweiz | EUR 10,85 Benelux | EUR 11,05 Spanien | EUR 11,05 Italien

4 196067 008502 04

www.linux-user.de

04

Eine neue Hoffnung?

Andreas Bohle
Stellv. Chefredakteur

Sehr geehrte Leserinnen und Leser,

kaum ein Ereignis hat die Community in letzter Zeit so bewegt, wie die Diskussion des Debian-Projekts um die Frage, ob Systemd zum neuen Standard-Init-System avancieren solle. Dass die Streitfrage sich zu einer Existenzfrage entwickelte, liegt daran, dass der einzige ernst zu nehmende Gegenkandidat Upstart hieß.

Upstart markierte einen weiteren Meilenstein in Canonicals Eigenbrötelei in Bezug auf die Hausmarke Ubuntu. Die Tatsache, dass die Mitarbeit an dem Projekt an einen saftigen Knebelvertrag gekoppelt war, machte es quasi per Definition zu einem No-Go für freie Entwickler. Entsprechend stark fielen die Anstrengungen von Canonical aus, die wegweisende Entscheidung des Debian-Projekts zugunsten der Eigenentwicklung zu beeinflussen. Mehr dazu lesen Sie in einem umfassenden Artikel in dieser Ausgabe ab Seite 80.

Am Ende fiel die Entscheidung durch ein Votum von Bdale Garbee. Der steht dem Debian Technical Committee vor und darf in Pattsituationen eine Lösung vorschlagen. Mark Shuttleworth gratulierte und sagte schmallippig zu, dass Ubuntu Systemd übernähme, „sobald die Software stabil sei".

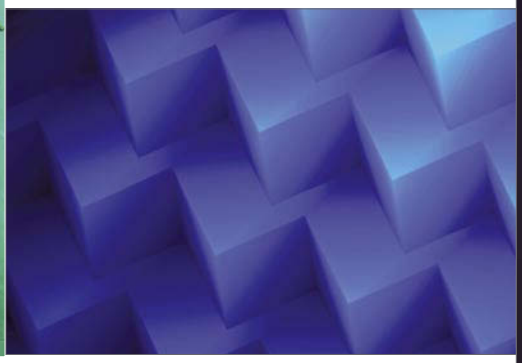
Trägt die Gemeinschaft der Debian-Entwickler den Entschluss des Technical Committee mit, dann schließt die Distribution damit zu einer Reihe von Systemen auf, die schon auf das alternative Init-System setzen oder dies planen. Damit bestünde die nicht unbegründete Hoffnung, dass die freie Entwicklergemeinde in einer essenziellen Frage endlich einmal wieder an einem Strang zöge und sich so Synergien nutzen ließen.

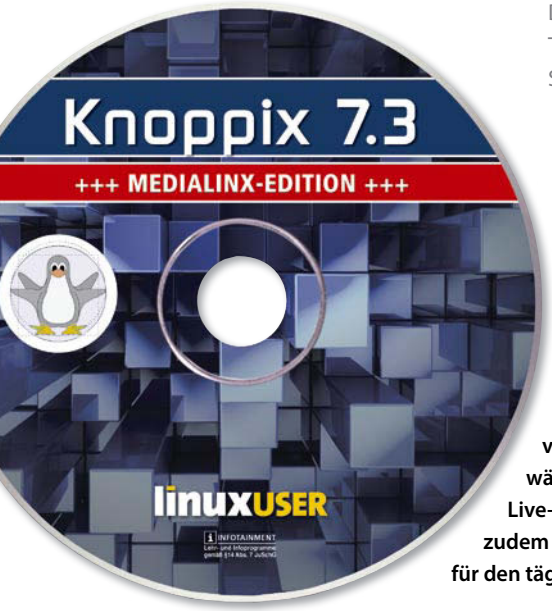
Das dürfte auch dringend notwendig sein, denn schon jetzt entwickelt sich Systemd zu einem ausufernden Projekt: Neben der Kontrolle über den Boot-Prozess ersetzt es auch das traditionelle Protokollieren via Syslog – und geht es nach dem Willen der Entwickler, dann übernimmt der neue Daemon zudem als Zwischenschicht die Kontrolle über weite Teile des Systems.

Wer das Votum aber als eine Absage an eine Monokultur Marke Canonical interpretiert, der sei gewarnt: Die Hauptentwickler von Systemd stehen im Wesentlichen auf der Gehaltsliste von Red Hat. Nicht ohne Grund sehen daher einige die Gefahr, dass auf diese Weise letztlich doch ein einzelnes Unternehmen einen erheblichen Einfluss auf das Linux-Ökosystem gewinnt.

Bevor sich aber solche dunklen Mächte erheben, hege ich erst einmal die Hoffnung, dass sich die Ereignisse für Linux insgesamt zum Vorteil auswirken. Sollte das nicht der Fall sein, bleibt immer noch die Möglichkeit, die Software zu forken und unabhängig weiterzuentwickeln – der freien Lizenz sei Dank.

Herzliche Grüße,





14 Die exklusive Knoppix-Edition vereint alle Vorteile des bewährten Originals unter den Live-Distributionen und bringt zudem wichtige Zusatzsoftware für den täglichen Bedarf direkt mit.

80 Das Init-System Systemd sorgt seit seiner Geburtsstunde gleichermaßen für Furore und Protest. Es bricht mit alten Konventionen, bringt aber zugleich einige innovative Konzepte mit. Wir machen eine Bestandsaufnahme.

22 Die Installation von Linux auf einem Flashspeicher birgt einige Fallstricke. Wir zeigen, was Sie beim Einrichten unbedingt beachten sollten, damit Ihr Linux-to-go allzeit optimal funktioniert.

28 Mehrere Distris auf einen USB-Stick zu installieren, erfordert Handarbeit – oder clevere Werkzeuge, die Ihnen hilfreich unter die Arme greifen.

Praxis

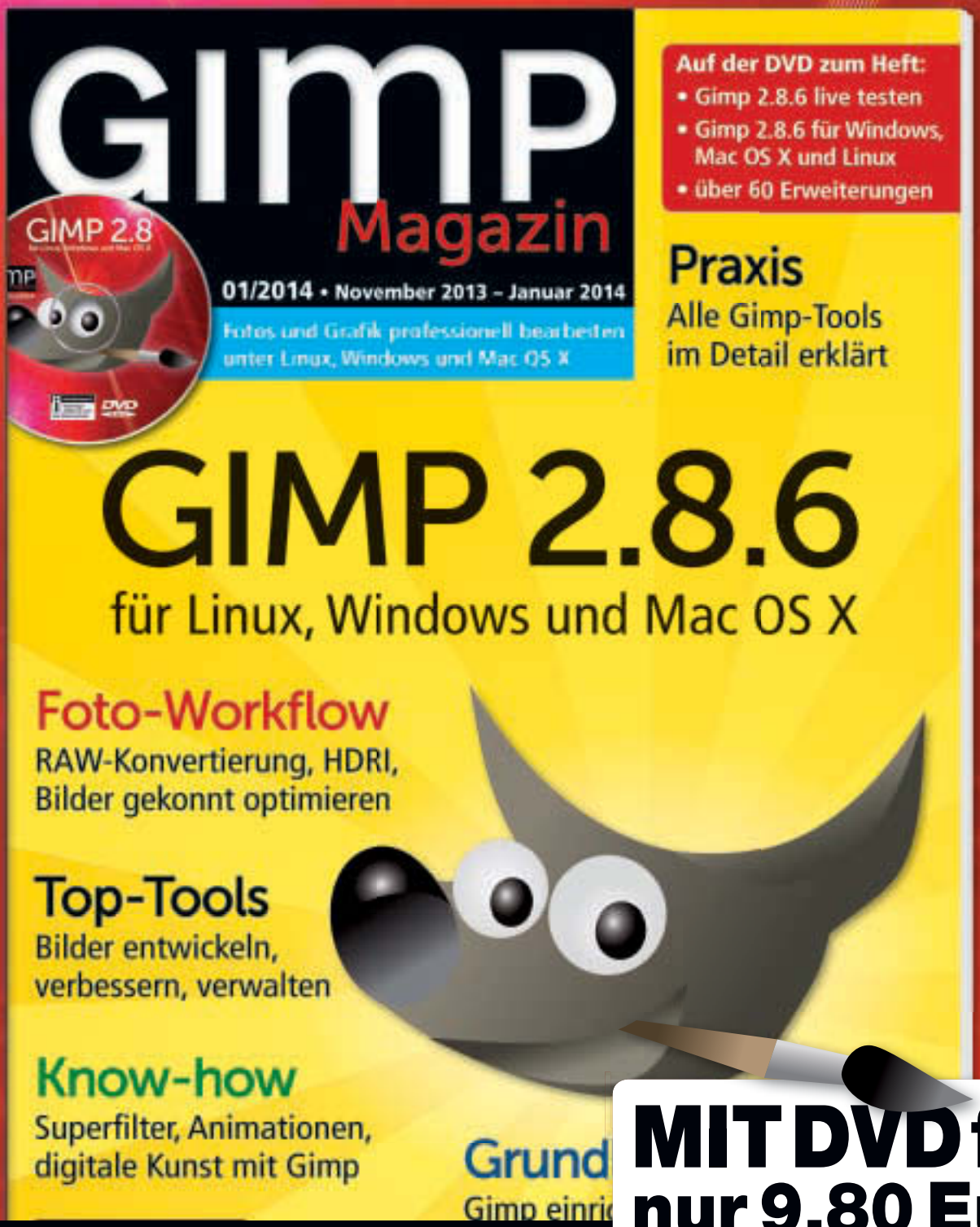
Netz&System

Know-how

74 **Mit Tripwire hält ein harter Hund an der Schwelle zum Rechner Wache, dessen empfindliche Sinne sofort Alarm schlagen, sobald ein Angreifer versucht, sich Einlass zu verschaffen.**

Service

JETZT NEU AM KIOSK!



MIT DVD für nur 9,80 Euro

Hier gleich bestellen:

medialinx-shop.de/gimp-magazin

Neues auf den Heft-DVDs

Knoppix 7.3 Medialinx-Edition

Knoppix 7.3 basiert wie üblich auf einem Mix von Debian „Stable“ und einigen Paketen – in erster Linie Grafiktreibern und Desktop-Programmen – aus dem „Testing“- und „Unstable“-Zweig. Um möglichst viel neue Hardware zur Mitarbeit zu bewegen, dienen als Basis der Kernel 3.13.0 mit Cloop und AUFS sowie X.org 7.7 Core 1.15.0. Das hybride Bootmedium bedient 32- und 64-Bit-Rechner (Bootoption `knoppix64`).

Das wichtigste Highlight dieses Knoppix-Releases stellt die Update-Funktion dar, mit deren Hilfe Sie bei Bedarf einen bereits mit Knoppix geflashten Stick auf eine neue Version aktualisieren, ohne dabei die persönlichen Daten und Einstellungen zu verlieren. Darüber hinaus bietet Knoppix die Möglichkeit, bei einer Installation auf USB-Sticks die persönlichen Daten zu verschlüsseln.

An neuen und aktualisierten Programmen bietet Knoppix unter anderem LibreOffice 4.1.4 und Gimp 2.8.6, die beiden Webbrowser Chromium 31.0.1650.63 und Firefox/Iceweasel 26.0 – den Letzteren samt Adblock Plus 2.4.1 und Noscript 2.6.8.14. Wine in der Version 1.5 hilft Windows-Programme zu integrieren, Virtualbox 4.3.2 sowie Qemu-kvm 1.7.0 übernehmen die Virtualisierung fremder Systeme. Als Standard-Desktopumgebung dient LXDE, optional stehen sowohl KDE 4.8.4 (Bootoption `knoppix desktop=kde`) als auch Gnome 3.8.4 (Bootoption `knoppix desktop=gnome`) bereit.

Sie finden Knoppix auf der Rückseite der ersten Heft-DVD. Einen ausführlichen Artikel zur erweiterten Medialinx-Edition der Distribution aus der Feder des Projekt-Maintainers Klaus Knopper lesen Sie ab Seite 14.

Sechs Mini-Distros auf einen Streich

Ein wahres Potpourri kleiner Distributionen enthält Seite A der ersten Heft-DVD. Mit von der Partie sind 4M Linux 8.0 All-in-One (siehe Artikel ab Seite 10), Puppy Linux 5.6 „Slacko“, Slax 7.0.8, SystemRescueCD 4.0.1 und Tiny Core Linux 5.2. Neben den bootbaren Version stehen sämtliche Distributionen auch als ISO-Images auf Seite A der ersten Heft-DVD bereit.

Vor allem Bastlern dürfte Tiny Core Linux entgegenkommen: Es versteht sich weniger als gebrauchsfertiges System denn als Kern eines solchen. Damit bietet es eine vergleichsweise einfach zu bedienende Grundlage, um ein System ganz nach Ihren Wünschen zu gestalten. Wie das funktioniert, zeigt ein Artikel ab Seite 44.

Ganz auf die Systemrettung spezialisiert hat sich SystemRescueCD 4.0.1. Das Gentoo-Derivat nutzt als Desktop XFCE 4 und bietet fast ausschließlich Werkzeuge zur Datenrettung oder Manipulation von Datenträgern an. So gibt es unter anderem Gparted zum Partitionieren von Festplatten, Partimage zum Sichern von Partitionen und Photorec zum Wiederherstellen von gelöschten Dateien. Neben zahlreichen Netzwerktools liegt auch noch der Virenscanner ClamAV bei. Weitere Details zur SystemRescueCD finden Sie in einem Artikel ab Seite 18.

Dreh- und Angelpunkt der auf Ubuntu basierenden Live-Distribution Multisystem LTS Precise r8 stellt das gleichnamige Werkzeug Multisystem dar. Es besteht aus einer Reihe von Shell-Skripten, die es erlauben, ausgewählte Linux-Distributionen auf einen USB-Stick zu befördern. Welche Vorteile Multisystem bietet, zeigt ein Artikel ab Seite 28.

Mageia 4

Die Entwickler des Mandriva-Abkömmlings Mageia bleiben in der Version 4 dem Motto treu, die Distribution für Um- und Einsteiger einfach zu gestalten, ohne erfahrenen Benutzern die Vielfältigkeit von Linux vorzuenthalten. An Kommunikationssoftware stehen unter anderem die Instant-Messenger Pidgin und Kopete sowie die IRC-Clients Quassel, X-Chat und Irssi bereit, an VoIP-Nutzer richtet sich Ekiga. Den Grafik-Bereich bestücken Gimp, Krita, Inkscape und Blender, der Multimedia-Fundus umfasst unter anderem verschiedene Xine-, Mplayer- und Gstreamer-basierte Software sowie den beliebten VLC. Die 32-Bit-Version starten Sie von Seite A der zweiten Heft-DVD, die 64-Bit-Variante von Seite B. Einen ausführlichen Artikel zu Mageia 4 lesen Sie ab Seite 64 (tle)

Bei der DVD-Edition von LinuxUser ist an dieser Stelle der zweite Heft-Datenträger eingeklebt. Bitte wenden Sie sich per E-Mail an `cdredaktion@linux-user.de`, falls es Probleme mit der Disk gibt.

Neue Programme

Das Werkzeug **Cryptcat 1.2.1** arbeitet wie das klassische Netcat, baut aber verschlüsselte Verbindungen auf. Daher lässt sich das praktische Tool weit über seinen ursprünglichen Zweck hinaus im Alltag einsetzen. Die Möglichkeiten reichen vom simplen Benachrichtigungssystem für das LAN bis zu einem verschlüsselten Chat auf der Konsole.

Anders als Festplatten und SSDs schenken die meisten Anwender USB-Sticks und Speicherkarten kaum Beachtung. **F3 2.2** prüft mittels eines Schreib- und Lesetests die Integrität der Speicherzellen von Flash-Medien und beugt somit unangenehmen Überraschungen wie beispielsweise einem Datenverlust vor.

Finden Sie Firefox zu behäbig, Chromium zu geschwätzig und Opera zu extravagant, dann empfehlen wir einen Blick auf **Qupzilla 1.6.3**. Die enorme Geschwindigkeit des Webbrowsers ist der Rendering-Engine Webkit geschuldet, die auch auf leistungsschwächerer Hardware das Surfen angenehm flüssig gestaltet.

Beim aktuellen **LibreOffice 4.2.1** haben Entwickler der Document Foundation unter anderem die Tabellenkalkulation Calc gründlich überarbeitet. Insbesondere das Verarbeiten großer Datenmengen und der Import umfangreicher und komplexer XLSX-Tabellen bewältigt die freie Büro-Suite nun schneller. Dazu rechnet die Software jetzt per OpenCL auf dem Grafikprozessor.

Hostbasierte IDS wie **Tripwire 2.5.22** spüren mögliche unerwünschte Änderungen auf zu schützenden Rechnern auf. Sie informieren dann die verantwortlichen Administratoren zeitnah und können so die mit einem (gelungenen) Angriff einhergehenden Schäden eindämmen oder gar verhindern.

Das **Disk Information Utility 4.35**, kurz Di, bietet eine flexible Alternative zum klassischen `df` für die Anzeige von Informationen über die Dateisysteme. Das Tool ermöglicht beim Anpassen der Ausgabe einen großen Gestaltungsspielraum.

Das auf Gtk+ basierende Tool **Gwakeonlan 0.6** verwaltet zu startende Systeme in einer übersichtlichen Liste und ermöglicht das parallele Aufwecken mehrerer Rechner mit wenigen Mausklicks.

Das Programm **Socat 1.7.2.2** dient zur bidirektionalen Datenübertragung. Es unterstützt alle gängigen Protokolle und eignet sich als Wrapper für SSL-Verbindungen oder zur Integration in eigene Skripte.

You can leave your hat on!

LINUXTAGE Grazer

4. + 5.4.2014, Graz

Eintritt frei!

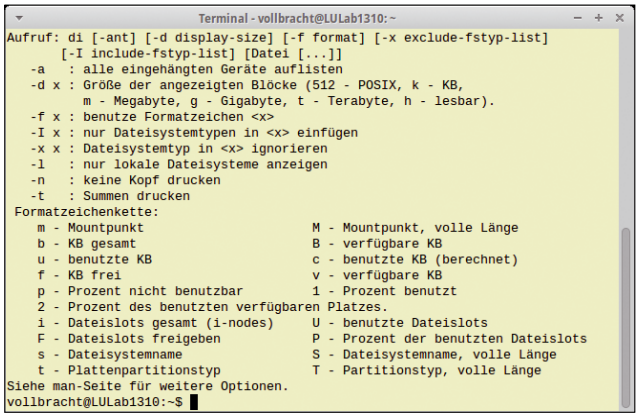
http://linuxtage.at

save the date

Füllstandszeiger

Möchten Sie den Füllstand einer Partition in eigenen Skripten verarbeiten, bietet die Df-Alternative Di 4.35 dazu alle notwendigen Fähigkeiten.

Die Belegung einer Partition ermitteln erfahrene Anwender mit dem GNU-Tool Df. Will man das Ergebnis aber in Skripten weiterverarbeiten, stellt das Di die bessere Alternative dar. Das Tool besticht durch eine frei formatierbare Ausgabe, die Ihnen aufwendige Nacharbeiten mit Sed, Awk und Co. erspart. So blenden Sie damit beispielsweise die Kopfzeile der Ausgabe über den Parameter `-n` aus und unterdrücken so die Spaltenbeschriftungen. Der Parameter `-t` summiert die Werte in jeder Spalte zu einem Gesamtwert auf. Anders als Df stellt Di die ausgegebenen Werte in MByte statt in Byte dar. Darüber hinaus beherrscht es auch eine Darstellung in KByte, GByte oder TByte. Um die Ausgabe nach Ihrem Gusto zu gestalten, geben Sie mit dem Parameter `-f` eine Ausgabeformatierung vor. Darin definieren Sie, welche Werte Di in welcher Reihenfolge anzeigt. Über den Parameter `-I` begrenzen Sie die Ausgabe außerdem auf bestimmte Dateisysteme. Dabei unterstützt Di im Gegensatz zu Df auch virtuelle Systeme wie Cgroups oder Sysfs. Um bestimmte Dateisysteme in der Gesamtausgabe zu ignorieren, verwenden Sie den Parameter `-x`. Benötigen Sie detaillierte Informationen zu den eingehängten Partitionen, lassen Sie Di diese über den Parameter `-A` ausgeben. Dies geht allerdings zu Lasten der Übersichtlichkeit. Brauchen Sie noch umfangreichere Informationen, schalten Sie Di mittels `-X` in den Debugging-Modus. Eine umfangreiche Beschreibung aller Parameter sowie einige Anwendungsbeispiele liefert die aussagekräftige Manpage des Tools.

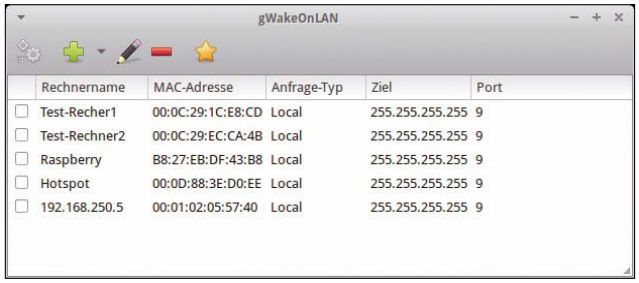


Lizenz: Zlib/Libpng
Quelle: http://www.gentoo.com/di/

Fernstarter

Mit dem intuitiv bedienbaren Gwakeonlan 0.6 starten Sie per Knopfdruck aus der Ferne einen oder gleich mehrere Rechner.

Bei der Fernadministration bieten Tools wie SSH oder VNC eine echte Hilfe – vorausgesetzt, der Zielrechner läuft auch. Tut er das nicht, müssen Sie ihn erst einmal per Wake-on-LAN (WoL) aus dem Dornröschenschlaf wecken. Genau dazu dient Gwakeonlan. Vor seinem Einsatz müssen Sie die entsprechende Funktion im BIOS des Zielsystems aktivieren. Das in Python geschriebene Gwakeonlan stellt Ihnen eine übersichtliche, GTK-basierte Oberfläche zur Verfügung, in der Sie die zu startenden Rechner verwalten und von dort aus mit „Magic"-Paketen aufwecken. Um neue Rechner einzubinden, fügen Sie entweder per Knopfdruck den aktuellen Inhalt des ARP-Caches hinzu oder tragen die Systeme manuell ein. Jeder Rechnereintrag enthält einen eindeutigen Namen und die MAC-Adresse des Zielsystems. Außerdem legen Sie fest, an welchen UDP-Port Gwakeonlan das „Magic"-Paket senden soll. Normalerweise funktioniert WoL nur im eigenen Netzwerk, einige moderne Router unterstützen jedoch das Einschalten von Rechnern via Internet, indem sie das „Magic"-Paket an das Zielsystem weiterreichen. Dazu müssen Sie in Gwakeonlan den Anfragetyp *Internet* wählen und die Zieladresse des Routers eingeben. Seine Konfiguration legt das Tool im Verzeichnis `~/.config/` ab. Alle verwalteten Rechner listet Gwakeonlan übersichtlich auf. Sie wählen dann einen oder mehrere Rechner an und lassen das Programm ans Werk gehen. Übersetzen Sie das Tool aus dem Quellcode, müssen Sie beim Installieren den Parameter `--prefix=/usr` angeben, da Gwakeonlan seine Bibliotheken im Verzeichnis `/usr/share/` erwartet.



Lizenz: GPLv2
Quelle: http://www.muflone.com/gwakeonlan/english/

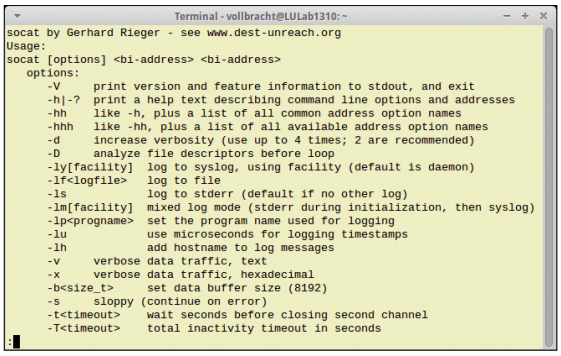
Datenumleiter

Die Fähigkeiten des mächtigen Relay-Tools Socat 1.7.2.2 reichen vom Umleiten der Standardausgabe bis hin zum Aufbau verschlüsselter Verbindungen.

Socket Cat oder kurz Socat ermöglicht das Einrichten bidirektionaler Verbindungen zwischen zwei Systemen. Dabei reicht das Spektrum von der einfachen Datenübertragung bis hin zum Streamen großer Datenmengen. So eignet sich das Tool beispielsweise für schlichte TCP-Weiterleitungen ebenso wie als Relaying-Lösung zwischen IPv6 und IPv4. Auch als SSL-Wrapper auf Server- oder Client-Seite kommt Socat infrage, wenn der umzuleitende Dienst nicht SSL-fähig ist. In Kombination mit Chroot lassen sich so sichere Umgebungen gestalten. Sowohl die umfangreiche Manpage als auch die Webseite des Projekts bieten dafür inspirierende Beispiele. Der Verbindungsaufbau erfolgt bei Socat in vier Stufen, beginnend mit dem Auswerten der übergebenen Kommandozeilenparameter. Es folgt der Verbindungsaufbau, dessen erfolgreichen Abschluss Socat abwartet. Dann fährt es mit der Verarbeitung fort. Steht die Verbindung, lassen sich Daten in beide Richtungen übertragen. Sobald eines der Systeme ein EOF-Signal sendet, baut Socat die Verbindung ab. Die gesamte Konfiguration erfolgt über Parameter, eine Konfigurationsdatei kennt das Tool nicht. Da es neben den Verbindungsoptionen zahlreiche weitere Einstellungen unterstützt, wie etwa Blöckgröße, Timeout oder Debugging, empfiehlt es sich, Socat via Skript aufzurufen.

Lizenz: GPLv2

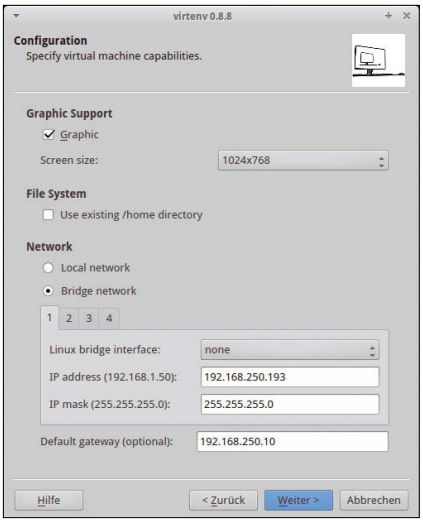
Quelle: http://www.dest-unreach.org/socat/



LXC-Frontend

Dank Virtenv 0.8.8 erstellen und starten Sie virtuelle Maschinen mit LXC im Handumdrehen und bauen so im Handumdrehen Testumgebungen für kritische Anwendungen auf.

Mit der GUI Virtenv erzeugen oder starten Sie in wenigen Schritten eine neue LXC-Umgebung. Der Virtenv-Assistent listet dazu nach dem Programmstart alle konfigurierten virtuellen Maschinen auf. Sie klicken lediglich den Namen einer Maschine an, um sie zu starten. Um eine neue VM zu erzeugen, benennen Sie diese erst einmal. Im Konfigurationsmenü legen Sie fest, ob und in welcher Auflösung die VM eine grafische Oberfläche bereitstellt. Außerdem wählen Sie zwischen einem nur auf dem Host verfügbaren Netz und der Bridged-Variante. Hier können Sie bis zu vier Netzwerkschnittstellen konfigurieren. Damit ist die virtuelle Maschine bereit zum Start. Bei VMs mit grafischer Oberfläche startet Virtenv den Window-Manager Openbox in einer Xephyr-Server-Sitzung. Beim Start der virtuellen Maschine bindet Virtenv das Root-Verzeichnis des Wirtssystems via Copy-on-Write in das dortige Verzeichnis `rootdir/` ein. So ist das Gastsystem sofort ohne Installation lauffähig.



Lizenz: GPLv2

Quelle: http://virtenv.sourceforge.net/

Allerdings erfordert dieser Schritt administrative Rechte. Änderungen in der eingebundenen Verzeichnisstruktur gelangen nicht ins Wirtssystem, sondern landen im Verzeichnis `rootdiffs/` der VM. Damit trennt Virtenv alle Systeme sauber. (jlu)

Die Mutter aller Live-Distributionen wartet in ihrer jüngsten Inkarnation Knoppix 7.3 mit Neuerungen wie UEFI-Boot, Desktop-Export und einfachem Upgrade auf. Unsere exklusive Medialinx Edition bringt außerdem den Adobe Reader und das Flashplayer-Plugin mit. Klaus Knopper

README

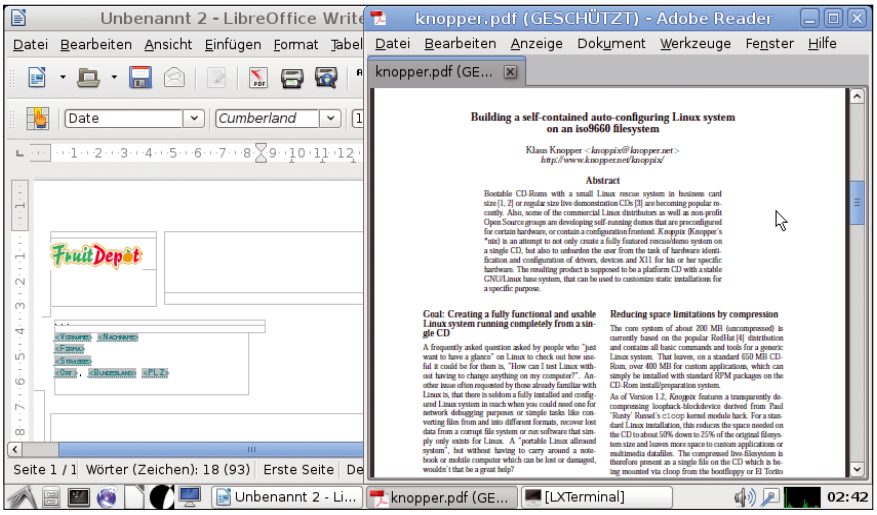
Klaus Knopper stellt zur CeBIT 2014 die Knoppix 7.3 Medialinx Edition vor. In diesem Beitrag gibt er Einblicke in Distributions-Interna und rückt die blitzgescheite Update-Funktion für USB-Sticks sowie das UEFI-Booten ins rechte Licht.

Seit über einem Jahrzehnt erscheinen unter dem Namen Knoppix („Knoppers Unix System") jährlich etwa zwei Zusammenstellungen von Linux-Software. Knoppix bootet von DVD oder USB-Stick und läuft ohne Installation sofort los. Die Software eignet sich zum Arbeiten, Surfen im Internet, Spielen, Unterrichten, Lernen, Programmieren und Retten von Daten defekter Betriebssysteme.

Die pünktlich zur CeBIT 2014 erschienene Version 7.3.0 basiert wie bei Knoppix üblich auf einem Mix von Debian „Stable" und einigen Paketen – in erster Linie Grafiktreibern und Desktop-Programmen – aus „Testing" und „Unstable". Um möglichst viel neue Hardware zur Mitarbeit zu bewegen, dienen als Basis der Kernel 3.13.0 mit Cloop und AUFS sowie X.org 7.7 Core 1.15.0.

Für Systeme mit mehr als 4 GByte Hauptspeicher startet mit der Bootoption `knoppix64` alternativ ein 64-Bit-Kernel. Das ermöglicht zusätzlich Systemreparaturen auf 64-Bit-Rechnern per Chroot-Umgebung. Hier eine sehr kurz gefasste Liste mit den Highlights, die die neue Version mitbringt:

- Experimentell unterstützter UEFI-Boot (32 und 64 Bit) von USB-Sticks.
- LXDE, der schlanke Knoppix-Standarddesktop mit dem Dateimanager Pcmanfm 1.1.2
- KDE 4.8.4 (Bootoption `knoppix desktop=kde`).
- Gnome 3.8.4 (Bootoption `knoppix desktop=gnome`).
- Einfacher Desktop-Export via VNC und RDP für Remote Desktop Viewing unter Linux und Windows.



1 Der proprietäre Adobe Reader (rechts) gehört normalerweise nicht in Knoppix, Libre Office (links) dagegen schon.

Knoppix 7.3 Medialinx Edition bootfähig auf Heft-DVD

- Smbmount-knoppix, das Such- und Mount-Utility zum Einbinden von Netzlaufwerken mittels Samba.
- Chromium 31.0.1650.63, Iceweasel 26.0 mit Adblock Plus 2.4.1 und Noscript 2.6.8.14, aktualisierter Textbrowser Elinks.
- LibreOffice 4.1.4 und Gimp 2.8.6.
- Wine 1.5.
- Virtualbox 4.3.2 und Qemu-kvm 1.7.0.
- Mutt-Vorlagen zur Mailkonfiguration.
- Automatische Blattlageerkennung im Scanprogramm Adriane-ocr und Tastaturlernprogramm Karl im Adriane Audio Desktop.
- Adobe Reader 1 und Flashplayer-Plugin (auf Wunsch der Redaktion).

Die meisten anderen enthaltenen Programme tragen zwar ebenfalls neue Versionsnummern, allerdings fallen die Änderungen dort nicht so spektakulär aus.

Für USB prädestiniert

Heutzutage installieren die meisten Anwender Knoppix eher auf einem USB-Stick (8 GByte) als es von DVD zu starten – nicht zuletzt, weil viele moderne Notebooks kein entsprechendes Laufwerk mehr besitzen. Noch von DVD gestartet, präsentiert Knoppix 7.3 auf dem Desktop das Icon *KNOPPIX auf Flash kopieren*. Ein Doppelklick startet das Knoppix-nach-Flashdisk-Installationstool 2.

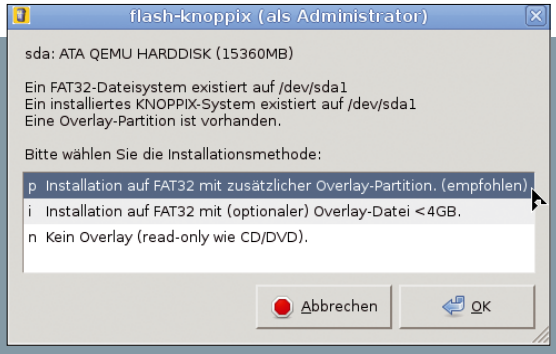
Obwohl die DVD-Version durch eine Sortlist schon fürs Lesen optimiert wurde, beschleunigt Flash-Speicher als Medium den Startvorgang und das Arbeiten mit Knoppix um mindestens den Faktor fünf. Das ermöglicht Startzeiten vom Laden des Kernels bis hin zum kompletten Desktop inklusive Compiz von unter 15 Sekunden – einigermaßen moderne Computer-Hardware und einen schnellen USB-Stick vorausgesetzt.

Eines der am häufigsten nachgefragten neuen Features war die Aktualisierbarkeit: Flash-knoppix untersucht nun das Zielmedium auf eine alte Knoppix-Installation hin und bietet an, nur das komprimierte Dateisystem und den Kernel auszutauschen, statt alles komplett neu zu installieren.

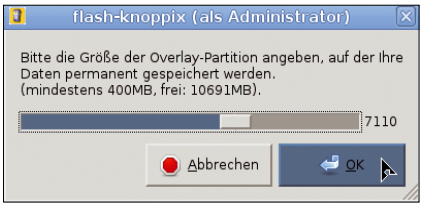
Da Softwarepakete, die Sie selbst installiert haben, mit dem neuen System inkompatibel sein könnten, gibt es die Option, nur die persönlichen Daten und Einstellungen in `/home/knoppix` zu behalten. Alternativ können Sie auch alles nachträglich Installierte behalten – meist nicht empfehlenswert, spart das manchmal Nacharbeit.

EFI und hybrides Booten

Damit das Update auf dem USB-Stick funktioniert, müssen Sie bei der Knoppix-Installation für die erste Partition mehr Platz einkalkulieren, damit Platz für spätere Aktualisierungen bleibt – 4,5 GByte erweisen sich als sichere Bank. Die beschreibbare Partition, die es seit Knoppix 7.1 gibt, kann sich dann über den Rest des entsprechenden Mediums ziehen 3. Optional lassen sich auf der Datenpartition schutzwürdige Benutzerdaten wie zum Beispiel Passwörter stark verschlüsseln.



2 Der Flash-Installer erlaubt es, einen großen USB-Stick so umzupartitionieren, dass er neben der FAT32- eine Linux-Partition anlegt.



3 Die beschreibbare Partition darf sich über den Rest des Sticks ziehen.

Das Starten direkt von USB-Flashdisk klappt schnell und komfortabel, da Knoppix getätigte Konfigurationsänderungen und angefallene Benutzerdateien automatisch auf die Datenpartition schreibt. Allerdings gibt es sehr alte und sehr neue Computer, die nicht von USB booten: Bei den einen unterstützt dies das BIOS nicht, bei den anderen erschwert oder verbietet EFI das Starten von externen Datenträgern.

EFI-Boot

Grundsätzlich startet Knoppix im EFI-Modus von USB-Sticks, da der Ordner `efi` auf der ersten Partition die notwendigen Startdateien enthält. Wurde auf dem Rechner jedoch die EFI-Firmware auf *Secure Boot* gesetzt, so unterbindet diese den Start von anderen Betriebssystemen als den vom Hersteller signierten. In diesem Fall hilft die BIOS-Einstellung *CSM* („Compatibility Support Module"), das einen „traditionellen" Start per Boot Record und Bootloader realisiert.

Für jene Fälle, bei denen ein Start von USB-Flashdisk grundsätzlich nicht klappt, enthält Knoppix 7.3 im Verzeichnis KNOPPIX das ISO-Image einer gerade mal 12 MByte großen Boot-Only-CD. Dieses brennen Sie auf einen Rohling und starten den Computer anschließend bei eingestecktem Knoppix-7.3-Stick von diesem Medium. Der Bootprozess beginnt auf der CD und wechselt nach kurzer Zeit auf den USB-Stick. Dieser Workaround funktioniert bei den meisten Problem-PCs sehr gut.

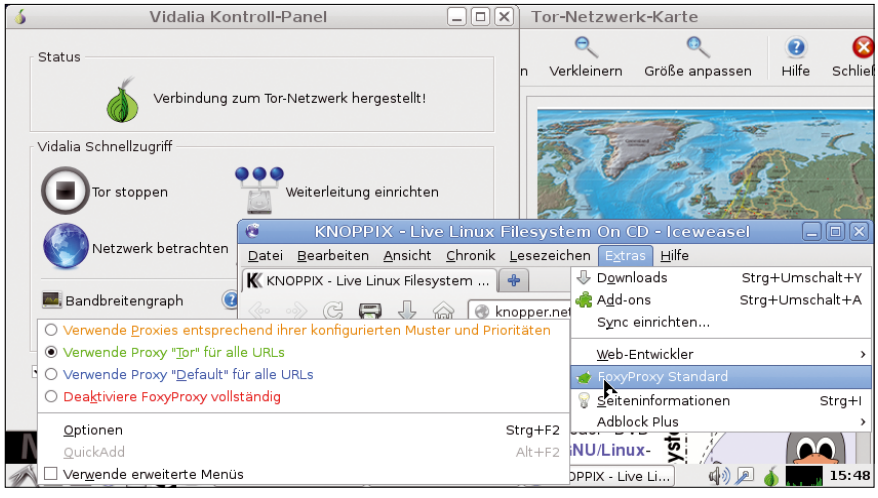
Nicht erst seit Ed Snowdens Enthüllungen besitzen Sicherheit und Schutz der Privatsphäre Priorität in der Knoppix-Architektur. Firefox, der in Debian und deswegen auch in Knoppix Iceweasel heißt, bringt das scharfgeschaltete Noscript-Plugin mit.

Noscript vermutet bei Javascript- oder Flash-Inhalten oder beim Start von Plugins, welche die Kamera, das Mikrofon oder andere Komponenten aktivieren, negative Auswirkungen auf die Sicherheit und Stabilität des Browsers. Es blendet dann am unteren Rand des Browsers oberhalb des Statusbalkens gelbe Benachrichtigungen ein.

Sie können nun entscheiden, ob Sie die Webseite permanent, nur für die aktuelle Session oder gar nicht für aktive Inhalte freischalten. Noscript macht zudem Banking und Bezahltransaktionen beim Einkaufen im Internet viel sicherer, da es viele Cross-Site-Scripting-Attacken erkennt und davor warnt.

Privatsphäre

Bei Tor handelt es sich um eine Privacy-Erweiterung, welche die Privatsphäre schützen soll. Über ein Netz von Gateways erschwert Tor IP-Adress-gestützte Sammelaktivitäten. Aber Vorsicht: Es ist nicht für den Zugriff auf Dienste ausge-



4 Chromium und Firefox haben die Tor-Proxys schon passend eingebunden.

Der Autor

Knoppix-Erfinder Klaus Knopper (knoppix@knopper.net, Jahrgang 1968 und Dipl.-Ing. der Elektrotechnik, arbeitet als selbstständiger IT-Berater und Entwickler, ist Professor für Softwaretechnik und Software-Engineering an der FH Kaiserslautern und gibt Kurse zu freier Software.

Weitere Infos und interessante Links

www.linux-user.de/qr/32352

legt, die einen autorisierten und authentifizierenden Zugang erfordern, wie das Anmelden bei Webdiensten.

Tor lässt sich durch ein Startprogramm im Knoppix-Menü in Gang setzen. Danach müssen Sie einen Proxy im Webbrowser Ihrer Wahl einrichten. Eine Ein-Klick-Aktivierung des Proxys ist in Chromium und Firefox voreingestellt 4.

Regelmäßig fragen Anwender nach einer Firewall für Knoppix – vermutlich, weil sich bei anderen Betriebssystemen Dienste von außen erreichen und damit angreifen lassen, was ein Portfilter zu reglementieren versteht.

Die „unnötige“ Firewall

Ein Standard-Knoppix ist allerdings so konfiguriert, dass es gar keine Dienste startet, die Ports nach draußen öffnen (außer, jemand startet Samba oder den Remote Desktop Server VNC aus dem Menü). Lassen Sie einen Portscanner auf ein laufendes Knoppix-System los, wird dieser daher auch ohne Firewall keinerlei offene, angreifbare Ports feststellen.

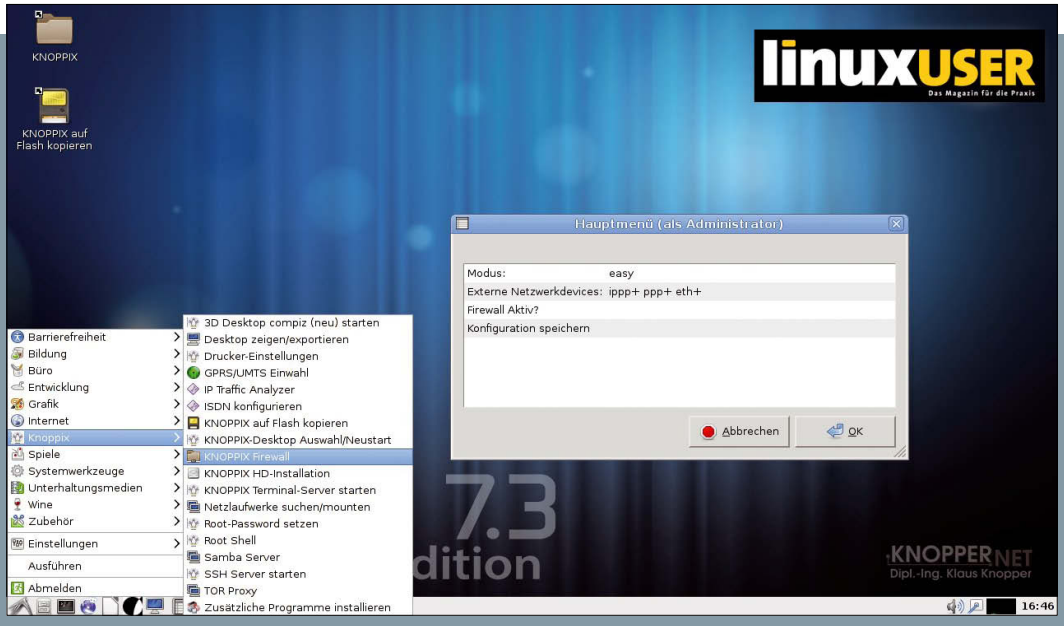
Dennoch besitzt Knoppix eine einfach zu konfigurierende Firewall, die Sie bei Bedarf aus dem Menü *Knoppix* heraus starten 5. Sie bietet drei Komplexitätsstufen von *Easy* bis *Experte* an, wobei Experten eigene Iptables-Regeln einstellen dürfen. Für die normale Benutzung als sicherer Internet-Client benötigen Sie die Firewall nicht. Sie kann sogar kontraproduktiv wirken, wenn es um die Nutzung von Streaming geht (etwa bei Videokonferenzen) – das hängt aber stark von der dafür verwendeten Software ab.

Troubleshooting

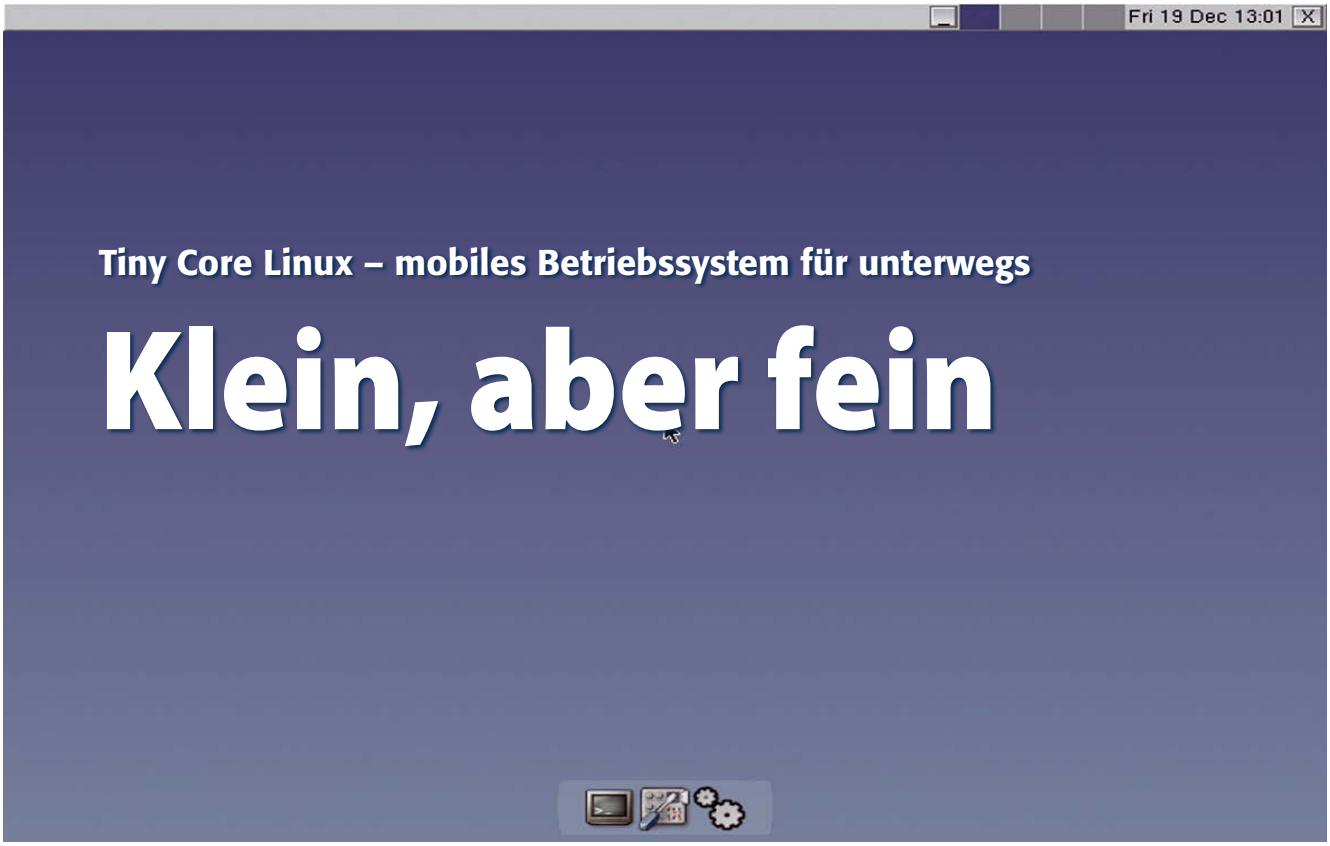
Sämtliche Benutzerzugänge in Knoppix sind übrigens gesperrt – es gibt keine Hintertüren oder Standardpasswörter, nicht einmal für den unprivilegierten Benutzeraccount *knoppix*. Daher klappt auch kein Login – starten Sie einen Screenlocker, dann sperren Sie sich praktisch aus, denn es gibt kein gültiges Passwort zum Entsperren. Daher verzichtet Knoppix auch auf das bei vielen anderen Distributionen übliche Absperren des Bildschirms beim Schließen des Notebook-Displays oder bei Inaktivität.

Normalerweise benötigt Knoppix keinerlei Boot-Optionen, um die vorgefundene Hardware inklusive Grafikkarte zu erkennen und das System optimal zu konfigurieren. Mit einer zunehmenden Anzahl verschiedener Chipsätze und Kombinationen derselben erweist es sich aber manchmal doch als notwendig, das eine oder andere Feature oder eine einzelne Komponente (vorübergehend) abzuschalten, um zum regulären Desktop durchzustarten.

Häufige Boot-Optionen nennt die Boot-Hilfe, die Sie über [F2] und [F3] abrufen. Weitere listet die Textdatei `KNOPPIX/knoppix-cheatcodes.txt` auf. Klemmt beispielsweise der Desktop an der Stelle, an der eigentlich Compiz starten müsste, helfen meist die Boot-Optionen `knoppix nocomposite` oder `knoppix no3d` weiter. Die eine schaltet die Composite-Erweiterung des Grafik-Subsystems ab, die andere verhindert den Compiz-Start. (jlu) ■



5 In Knoppix gibt es eine Firewall, deren Konfiguration in Komplexitätsstufen eingeteilt ist.



Tiny Core Linux – mobiles Betriebssystem für unterwegs

Klein, aber fein

Ein Linux-System stets dabeizuhaben, bringt Vorteile: Auf Fremdrechnern unterwegs startet stets die gewohnte Arbeitsumgebung, alle benötigten Tools und Dokumente sind an ihrem Platz. Ferdinand Thommes

README

Abseits der Mainstream-Distributionen tummelt sich Tiny Core Linux mit einem eigenwilligen, aber sinnvollen Ansatz: Es stellt ein aufs Notwendigste reduziertes System bereit, das Sie nach eigenen Wünschen mit Funktionen und Programmen ausstatten.

Das kürzlich in Version 5.2 erschienene Tiny Core Linux (TCL) präsentiert sich als minimales, modulares Betriebssystem, das sich selbst nicht als gebrauchsfertige Distribution versteht, sondern als der Kern einer solchen. Drei Installations-Images in Größen zwischen 9 und 72 MByte sprechen unterschiedlich fortgeschrittene Anwender an, die sich ein kleines und schnelles System nach eigenen Vorlieben zu bauen wollen, das von einem USB-Stick oder einer CD selbst auf der ältesten Hardware läuft. Als Minimalvoraussetzungen nennt das Projekt eine 486DX-CPU und 64 MByte RAM.

Prinzipiell läuft TCL immer komplett im Hauptspeicher, wobei die Erweiterungen ebenfalls im RAM oder von einem persistenten Speichermedium eingebunden oder auf diesem installiert sein können. Dabei entpackt das System den Kern und die Erweiterungen bei jedem Neustart und lädt sie. Somit bleibt Viren und anderen Schädlingen kaum eine Chance, sich zu etablieren, da sich jede neue Sitzung von TCL wie eine frisch gestartete Live-CD verhält.

Facettenreich

Das Projekt stellt TCL in drei Varianten zur Verfügung. Wer möglichst viel Freiheit bei der Zusammenstellung seines Systems möchte, für den ist das nur 9 MByte große Core die richtige Wahl. Diese Variante bietet einen angepassten Kernel und eignet sich ausschließlich für die Arbeit auf dem Terminal. Werkzeuge zum Erweitern des Systems bringt sie bereits mit. Ein X-Server fehlt jedoch, lässt sich aber – wie alles andere auch – problemlos nachrüsten. Diese Version setzt voraus, dass Sie es gewohnt sind, auf der Kommandozeile zu arbeiten, und das Linux-Rechtesystem kennen. Core eignet sich für schlanke, maßgeschneiderte Desktops, Server-Anwendungen oder Embedded-Systeme.

Wünschen Sie etwas mehr Komfort, dann greifen Sie zum 15 MByte großen Tiny Core. Hier ergänzen ein X-Server sowie eine grafische Oberfläche in Form des Fltk-GUI-Toolkits samt des Window-Managers Flwm das Core-Paket. Tiny Core benötigt ebenso wie Core eine ka-

belgestützte Verbindung zum Internet; beide unterstützen lediglich die US-amerikanische Tastaturbelegung.

Möchten Sie TCL mit WLAN nutzen und nicht auf die deutsche Tastaturbelegung verzichten, dann steht Ihnen dazu die dritte Variante namens Core Plus mit 72 MByte Umfang zur Verfügung. Sie bringt neben Flwm noch sechs weitere Fenstermanager mit, darunter Fluxbox, Blackbox und Openbox sowie ein Remastering-Werkzeug 1.

Alle Images basieren derzeit auf x86; darüber hinaus arbeitet das Team an Versionen für die Architekturen ARMv6 und ARMv7. Die als piCore 5.1 im Januar veröffentlichte Version für ARMv6 ist für den Raspberry Pi vorbereitet.

Cloud-Modus

Die Installation gestaltet sich für alle drei Varianten gleich. Es gibt wiederum drei Möglichkeiten, TCL für verschiedene Anwendungsfälle auf CD oder USB-Stick zu bannen.

Im sogenannten Cloud-Modus brennen Sie das ISO-Image auf eine CD. Nach dem Start in die Desktop-Umgebung entfernen Sie die CD aus dem Laufwerk, der Rest der Sitzung spielt sich im Arbeitsspeicher ab. Somit bleibt das Laufwerk für andere Anwendungsfälle frei. Dieser Modus eignet sich zum Testen von Applikationen oder für Sitzungen, in denen Sie nichts speichern möchten. Nach dem Herunterfahren des Systems bleiben sowohl die CD als auch der Rechner unverändert.

Alternativ transferieren Sie das ISO-Image per Konsolen-Befehl (Listing 1) direkt bootfähig auf einen USB-Stick. Welches Device der USB-Stick belegt, zeigt der Befehl `# fdisk -l`. Alternativ verwenden Sie das Tool Unetbootin.

Die zweite Möglichkeit nennt sich USB Stick Mode und erfordert neben der bereits vorbereiteten CD einen USB-Stick.

Listing 1

```
# dd if=/Pfad/zur/ISO-Datei of=
/dev/sdX
```

Dieser Modus eignet sich für Nutzer, die genutzte Anwendungen sowie die Ergebnisse der Sitzung speichern wollen und TCL auch an Rechnern verwenden, die nicht von USB booten. Dazu stecken Sie einen USB-Stick am Rechner an und booten TCL von einer CD.

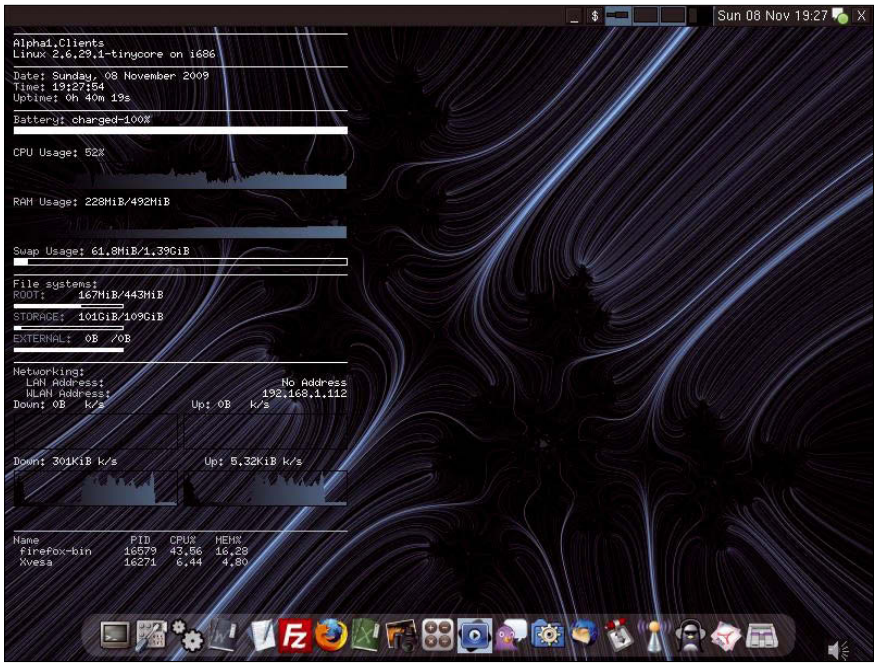
Boot-Prozess

Sobald beim Start die Bootparameter erscheinen, drücken Sie [Tab] und hängen an das Bootkommando den Parameter `tinycore waitusb=10` an. Das hält den Bootprozess für 10 Sekunden an, um langsameren USB-Sticks Zeit zu geben, sich am Systembus zu registrieren. Per [Eingabe] fährt das System weiter hoch. Bei älteren USB-Sticks genügt ein Wert von 10 eventuell nicht, und Sie müssen auf 20 oder mehr Sekunden erhöhen.

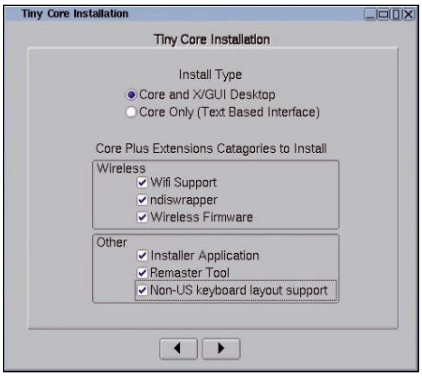
Nach dem Start des Desktops rufen Sie in der Leiste am unteren Bildschirmrand den Dateimanager auf und navigieren darin zum Verzeichnis `/mnt`. Durch einen Klick auf das Plus-Zeichen davor sehen Sie nun den verbundenen USB-Stick. Sind an den Rechner mehrere Festplatten und/oder USB-Sticks angeschlossen, ergibt es Sinn, dem USB-Stick vor-

Tiny Core Linux 5.2 (Core Plus)
bootfähig auf Heft-DVD

Tiny Core Linux 5.2
(Core, Tiny Core, Core Plus als ISO)
`LU/tinycore/`



1 Die Distribution Tiny Core Linux erlaubt es, aus einer einfachen Basis alles vom minimalen Embedded-System bis hin zum maßgeschneiderten Desktop zu bauen.



2 Der Installer erlaubt es Ihnen, die Distribution mühelos mit Ihren Vorgaben auf einem USB-Stick zu installieren.

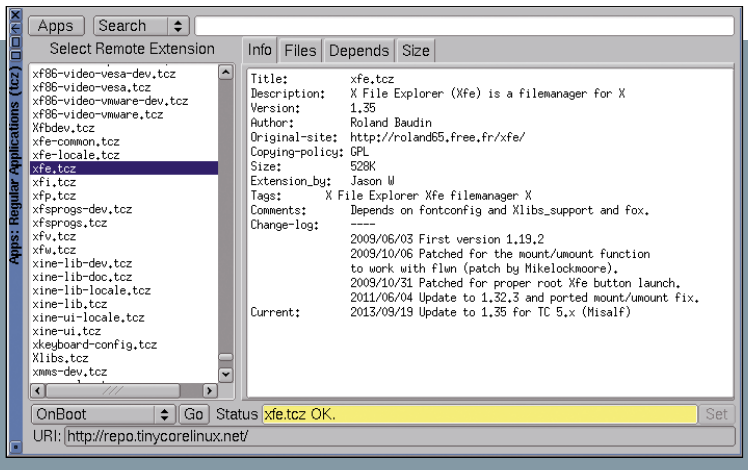
her einen eindeutigen Namen zu geben, sodass er sich leichter identifizieren lässt. Ansonsten hilft wieder der Befehl `fdisk -l`, um sicherzustellen, dass Sie auf das richtige Device schreiben.

Ein Rechtsklick auf das USB-Device öffnet die Option *Create Directory*, mit der Sie nun das Verzeichnis `/tce` erstellen. In diesem Ordner legt TCL zukünftig alle Anwendungen, Konfigurationen und gespeicherte Daten ab. Beim nächsten Start erkennt das System das Verzeichnis automatisch und stellt alle dort abgelegten Anwendungen zur Verfügung.

Vor dem Herunterfahren müssen Sie zum Speichern in der Leiste unten das Icon ganz links benutzen, um dann *Backup Options | Backup* auszuwählen. Nach Anwahl von *sda1/tce* oder der entsprechenden Bezeichnung des USB-Sticks und dem Bestätigen via *OK* speichert TCL alle Daten der Sitzung auf dem Stick. Lassen Sie diesen Schritt aus, gehen die Daten dieser Sitzung verloren.

USB-Stick-Bootmodus

Der USB-Stick-Bootmodus speichert TCL und die Daten direkt auf dem USB-Stick und erspart somit das Booten von CD. Voraussetzung dafür ist allerdings, dass der Rechner das Booten von USB-Geräten auch unterstützt. Nach dem Start des Desktops klicken Sie unten in der Leiste auf das Icon mit den beiden Halbkugeln und wählen im neuen Fenster den Punkt *HD/USB Install* 2.



3 Der App-Browser erlaubt es, zusätzliche Software zu installieren.

Danach öffnet sich ein weiteres Fenster, in dem Sie *USB-HDD* aktivieren. Steht dort in der obersten Zeile bereits `/mnt/sr0/boot/core.gz` und im Fenster darunter der USB-Stick als *Removable Device*, wählen Sie diesen aus. Ist die obere Zeile leer, tragen Sie dort `/mnt/sr0/boot/core.gz` manuell ein. Im nächsten Fenster wählen Sie ein Dateisystem, wobei Ext2 für einen USB-Stick am sinnvollsten erscheint, da das fehlende Journal Schreibzugriffe einspart.

Im darauf folgenden Fenster konfigurieren Sie die Boot-Optionen. Hier tagen Sie `lang=de` ein. Die weiteren angebotenen Optionen hängen Sie bei Bedarf durch Leerstellen voneinander getrennt an. Im nächsten Fenster aktivieren Sie die Optionen gemäß Ihren Wünschen. Wichtig ist wiederum die unterste Option, das Umschalten auf die deutsche Tastaturbelegung. Eine Anleitung, wie Sie diese permanent einrichten, finden Sie im TCL-Forum.

Die Boot-Optionen lassen sich auch später noch beim Hochfahren des Systems jeweils über [F2] bis [F4] anzeigen und auswählen. Der abschließende Dialog gibt einen Überblick über die Optionen; nach einem Klick auf *Proceed* startet die Setup-Routine mit dem Formatieren des USB-Sticks und überträgt danach das Abbild auf den USB-Stick. Von nun an startet der Rechner direkt vom Stick.

Ein weiterer Weg, TCL ohne CD zu nutzen, besteht darin, das Image in einer virtualisierten Umgebung wie Virtualbox oder KVM zu starten. Dabei gilt es lediglich, sicherzustellen, dass die VM die Daten an den USB-Stick im Gastsystem durchreicht. Dazu müssen Sie bei Virtualbox die Gasterweiterungen installieren und den USB-Modus in den Einstellungen auf *USB 2.0* umstellen.

Anwendungen einbinden

Je nachdem, welchen Fenster-Manager Sie nutzen, weicht die Bedienung der Oberfläche und der Menüs leicht voneinander ab. Diese Beschreibung bezieht sich auf den Standard-Manager Flwm, die Alternativen wie Fluxbox oder Openbox arbeiten sehr ähnlich.

Zuerst müssen Sie sich entscheiden, ob Sie die Apps im vorher erstellten Verzeichnis `/tce` ablegen wollen oder eher ein traditionelles Home-Verzeichnis bevorzugen. Die Ablage in `/tce` stellt sicherlich die Norm dar, jedoch lässt sich ein konformes Heimatverzeichnis über die Boot-Option `home=sdX` einrichten.

In Flwm öffnet ein Klick auf den Desktop ein Menü, in dem Sie *System Tools | Apps* auswählen. Im sich daraufhin öffnenden Fenster stellen Sie unten links im Ausklappmenü entweder *OnDemand* oder *OnBoot* ein. Damit entscheiden Sie, ob das System ein Programm mit der Option *OnBoot* beim Hochfahren starten soll oder mit *OnDemand* bei jedem Programmstart frisch auspackt.

Die Art der Anwendung des USB-Sticks sollte hauptsächlich über diese Optionen entscheiden. Setzen Sie TCL etwa an einem öffentlichen Rechner ein, ergibt die Entscheidung *OnDemand* Sinn. Rechts daneben in der Eingabezeile sollte `/mnt/sdbX/tce/optional` angezeigt werden, was auf den USB-Stick verweist. Nun wählen Sie oben unter *Apps* den Eintrag *Cloud Browse* aus, alternativ definieren Sie zunächst den am nächsten gelegenen Spiegelserver.

Möchten Sie ein Programm einrichten, lassen Sie es markiert und klicken unten im Fenster auf *Go*, woraufhin die Installation startet. Beim Markieren eines Programms in der Auswahl zeigt der Paketmanager rechts davon Informationen über das Paket, dessen Größe und Abhängigkeiten an 3. Sollten Upgrades bereitstehen, finden Sie hier Informationen zu den Änderungen.

Eigenes Paketformat

Um seine Philosophie verwirklichen zu können, verwendet Tiny Core ein eigenes Paketformat namens TCZ. Neben den im App-Browser angebotenen Programmen stehen auf den Servern von

TCL viele weitere bereit. Diese laden Sie zum Beispiel mit dem Downloader Wget von dort herunter.

Dabei ist es oft sinnvoll, nicht unbedingt nur in den aktuellsten Archiven zu suchen, sondern auch in deren Vorgänger. Derzeit bietet das Repository für Version 4.x beispielsweise mehr Apps als jenes für das relativ neue 5.x. Falls Sie das gewünschte Paket unter *5.x* nicht finden, müssen Sie in der Repo-URL die Version *5.x* gegen *4.x* austauschen, um das ältere Archiv zu durchstöbern.

Maßgeschneidert

Bei TCL handelt es sich um ein waschechtes Community-Projekt, die meisten in den Archiven vorrätigen Programme wurden von der Gemeinschaft erstellt und gepflegt. Dementsprechend freuen sich die Helfer im Forum, wenn sie Rückmeldungen bekommen, ob etwa Pakete aus 4.x etwa in 5.x funktionieren. Sofern allgemeines Interesse besteht, ist es auch durchaus möglich, dass die Community-Mitglieder auf Nachfrage ein spezielles Programm im kompatiblen TCZ-Format basteln.

Möchten Sie selbst Hand anlegen, sollten Sie sich mit dem Werkzeug Tztools auseinandersetzen, das bereits im TCZ-Format vorliegt. Eine weitere interessante Möglichkeit, mit TCL zu einem maßgeschneiderten System zu kommen, bietet das Remastering-Werkzeug Ezremaster, mit dem Sie eigene Kombinationen von Core, Kernel und Erweiterungen zu einem neuen ISO-Image zusammenstellen 4.

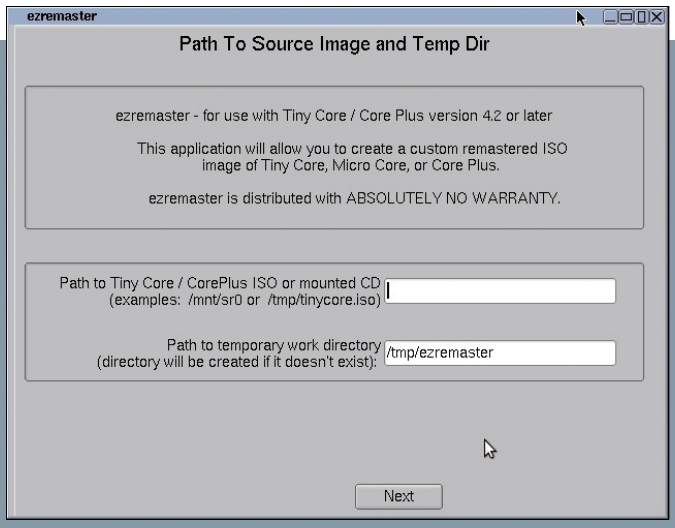
Fazit

Tiny Core Linux fordert zwar vom Anwender etwas Einarbeitung, bietet dafür aber auch weitestgehende Freiheit. Selbst gestandene Linux-Anwender sollten sich zuerst etwas in die Philosophie von TCL einlesen, da die Distribution doch einiges anders handhabt als gewohnt. Dafür erwecken Sie mit TCL bei entsprechender Sorgfalt hinsichtlich der Paketauswahl auch alte Hardware-Schätzchen aus den Neunzigern wieder zu neuem Leben.

Die Dokumentation von TCL erscheint insgesamt als etwas veraltet und für Neueinsteiger nicht immer sinnvoll geordnet. Neben der Dokumentation auf der Webseite gibt es ein gut besuchtes Forum, ein Wiki und eine FAQ. Für die dringliche Frage zwischendurch an die Entwickler bietet sich der IRC-Kanal `#tinycorelinux` auf dem Freenode-Server an. (tle)

Weitere Infos und interessante Links

www.linux-user.de/qr/31431



4 Das Remastering-Werkzeug Ezremaster ermöglicht es Ihnen, ein ISO-Image mit Ihren eigenen Vorgaben von TCL anzufertigen.

Ähnliche Projekte

Neben TCL gibt es weitere Projekte mit ähnlicher Zielsetzung. Dazu zählen unter anderem Puppy Linux und dessen experimenteller Ableger Quirky, das etwas komfortablere Slitaz sowie das sich mit 8 MByte Hauptspeicher begnügende und in den Kernkomponenten in Assembler geschriebene KolibriOS. Somit dürfte in der Szene der kleinen portablen Betriebssysteme für jeden Geschmack etwas dabei sein.

Der Autor

Ferdinand Thommes lebt und arbeitet als Linux-Entwickler, freier Autor und Stadtführer in Berlin.

Basics. Projekte. Ideen. Know-how.

NEU!

Mini-Abo

zwei Ausgaben

nur 9,80 €

Jetzt bestellen!

www.medialinx-shop.de/raspberry-pi-geek

Mageia 4 verbessert den Ablauf der Installation und erweitert das Angebot an Software. Oliver Burger

Das Mageia-Projekt entstand im September 2010 mit dem Ziel, die Distribution Mandriva Linux unabhängig von dem ins Trudeln gekommenen Unternehmen weiterzuführen. Seit der Veröffentlichung des ersten Releases im Mai 2011 erfreut sich Mageia wachsender Beliebtheit und hat sich mittlerweile einen festen Platz in den Top Five des Rankings auf Distrowatch erobert.

Mit der Veröffentlichung von Mageia 4 bleibt das Projekt seinem Ziel treu, eine Distribution zu erstellen, die für Um- und Einsteiger einfach zu handhaben ist, ohne erfahrenen Benutzern die Vielfältigkeit eines Systems vorzuenthalten.

Wie üblich gibt es Mageia 4 in verschiedenen installierbaren Live- sowie dedizierten Installer-Varianten für 32- und 64-Bit-Systeme (siehe Tabelle Mageia-Installationsmedien). Sie haben also schon vor dem Download eine breite Auswahl vor sich. Bei allen Mageia-Medien handelt es sich um sogenannte Hybrid-ISOs, die sich einfach mittels des Kommandozeilen-Befehls `dd` auf einen USB-Stick kopieren lassen, um sie dann von dort aus zu installieren.

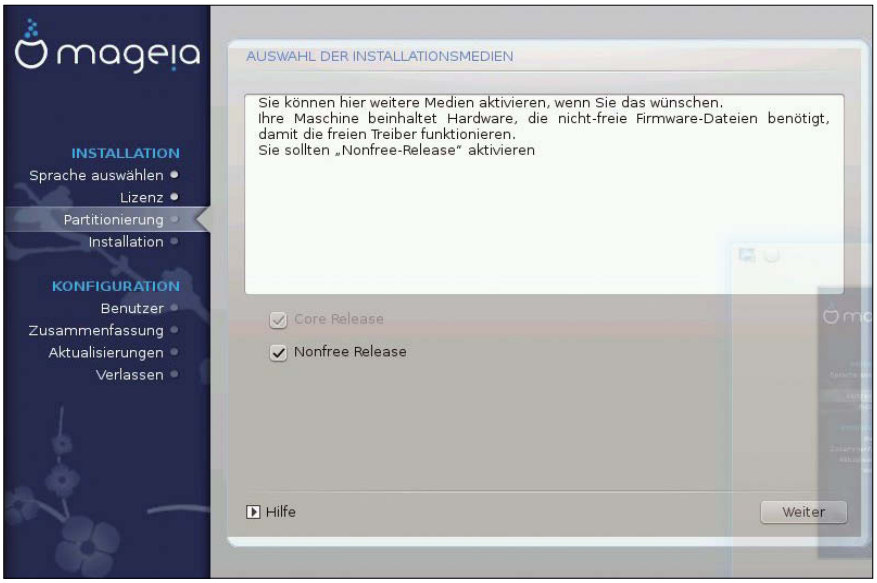
Bei Mageia müssen Sie sich vor dem Herunterladen nicht auf einen Desktop festlegen: Mittels der bereitgestellten Meta-Pakete lässt sich jederzeit ein anderer Desktop nachinstallieren. Hierbei entspricht ein Gnome-Desktop, der mittels Meta-Paket *task-gnome* einer installierten KDE-Live-DVD hinzugefügt wurde, jenem Desktop, der auf einer installierten Gnome-Live-DVD zu sehen wäre.

Mageia-Installationsmedien

Typ	Umfang	32 Bit	64 Bit	Anmerkung
Installationsmedien				
DVD	4,2 GByte	●	●	viele Desktops, breite Software-Auswahl
Dualarch-DVD	1 GByte	●	●	32+64 Bit, nur XFCE
Netzwerk-CDs	23 bis 74 MByte	●	●	mit / ohne unfreier Firmware
Live-Medien				
CD	700 MByte	●	❍	nur Englisch, KDE oder Gnome
DVD	1,4 GByte	●	●	alle Sprachen, KDE oder Gnome

README

Anfang Februar veröffentlichte das Mageia-Projekt die vierte Version seiner Distribution. Besonders angenehm sind die Neuerungen am Installer.



Mageia 4
(Install-DVDs 32+64 Bit)
bootfähig auf Heft-DVD 2

1 Während der Installation geben Sie direkt an, welche der vorhandenen Repositories Sie beim späteren Betrieb der Distribution vewenden möchten.

Den Installer haben die Entwickler für Mageia 4 etwas überarbeitet, wobei jedoch das gewohnte Look & Feel erhalten blieb. Bereits im Bootmenü des Installers treffen Sie verschiedene Einstellungen, etwa mittels [F2] die Auswahl der Sprache für die Installation.

Installation

In den weiteren Schritten partitionieren Sie die Festplatte und wählen dann die zu benutzenden Software-Quellen, wobei sich weitere Medien einrichten lassen wie etwa ein FTP-Server. Danach legen Sie fest, welche der auf den angegebenen Medien verfügbaren Repositories Sie nutzen möchten 1. Vorgegeben sind hier die Repos *Core* und *Non-free* der Installations-DVD.

Anschließend können Sie eine Auswahl der zu installierenden Software treffen. Wie bei den früheren Mageia-Versionen haben Sie in Sachen Desktop die Auswahl zwischen KDE, Gnome oder einem selbst definierten Desktop. Bei der benutzerdefinierten Variante zeigt der Installer eine Übersicht der einzelnen Paketgruppen, aus der Sie anschließend nach eigenem Ermessen auswählen. Daneben besteht die Möglichkeit zur individuellen Auswahl an Paketen, um das System zu erweitern.

Der Installer von Mageia 4 gliedert die Paketgruppen grob in *Arbeitsplatzrechner*, *Server* und *Graphische Arbeitsoberfläche* 2. Diese neue Einteilung erhöht die Übersichtlichkeit – insbesondere, weil die letzte Sektion nach dieser Änderung eine bei Weitem größere Anzahl an Möglichkeiten bietet.

Nach dem Einrichten der Pakete treffen Sie noch einige Einstellungen wie die Wahl des zu installierenden Bootloaders sowie Benutzernamen und Passwörter. Zum Abschluss liefert der Installer einen Überblick über alle Einstellungen und erlaubt noch einmal Anpassungen. Während des gesamten Installationsablaufes haben Sie die Möglichkeit, die zum jeweiligen Schritt gehörende Hilfe-Seite zu öffnen.

Eine weitere Neuerung in Mageia 4: Ein Willkommens-Bildschirm 3 bietet nach dem ersten Login einen Überblick über wichtige Werkzeuge und die zentralen Anlaufstellen für das neue System.

2 Die Anordnung der Paketgruppen in Tabs verbessert die Übersicht im neuen Installer.

3 Der Mageia-Willkommens-Bildschirm bietet beim ersten Login einen Überblick über die wichtigsten Werkzeuge sowie die Anlaufstellen der Mageia-Community.

Zu den herausragenden Merkmalen von Mageia zählt das noch von Mandriva geerbte Mageia-Kontrollzentrum 4. Hier nehmen Sie an zentraler Stelle die gesamte Konfiguration des Systems vor. Dabei lassen sich alle Werkzeuge auch einzeln aufrufen. Die meisten Tools bieten außerdem eine Ncurses-basierte Schnittstelle und lassen sich daher auch ohne X-Server nutzen.

Die Desktops

Neben den bisher schon vorhandenen Desktops bietet Mageia 4 nun außerdem Cinnamon und Maté an, die beide aus dem Mint-Umfeld stammen. Beide Desktops gab es schon für Mageia 3 in inoffiziellen Repositories. Deren Betreiber ist nun aber offizieller Mageia-Packager und hat beide Desktops in die Distribution eingebracht.

Die Installer-DVDs beherbergen somit nun acht vollständige Desktop-Umgebungen. Dazu zählen neben den beiden Platzhirschen KDE und Gnome nun XFCE, LXDE, Razor-Qt, E17, Cinnamon und Maté. Des Weiteren stehen in den Repositories des Projektes zusätzlich schlanke Windowmanager wie Fvwm2, i3 oder Scrotwm bereit.

(U)EFI

Mageia 4 unterstützt standardmäßig noch kein UEFI. Das Mageia-Wiki liefert aber eine Anleitung, wie man Mageia mit UEFI nutzen kann. Mageia 5 soll nativen UEFI-Support erhalten, eine Unterstützung von Secure Boot ist allerdings auch in Zukunft nicht vorgesehen.

Mageia hat an den Desktops und Window-Managern nur wenige Anpassungen vorgenommen, hauptsächlich kleine optische Änderungen wie ein einheitlicher Hintergrund oder ein einheitlicher Menü-Button. So verfügbar, setzen auch alle Oberflächen auf das Oxygen-Theme, um ein einheitliches Look & Feel zu bieten. All dies lässt sich beliebig anpassen.

Desktop-Software

Für den täglichen Bedarf stellt Mageia einen umfänglichen Software-Fundus bereit. Bei Büro-Software haben Sie die Auswahl zwischen LibreOffice, Calligra und einem Gnome-Office-Subset samt Gnumeric und Abiword. Als Webbrowser dienen wahlweise Firefox, Chromium oder Opera. Der oft benötigte Flashplayer lässt sich über die Paketverwaltung nachinstallieren.

Ebenso reichhaltig fällt das Angebot an Kommunikationssoftware aus. Hier finden sich die Instant-Messenger Pidgin, Kopete, Empathy und Telepathy ebenso wie die IRC-Clients Quassel, X-Chat und Irssi. Für VoIP-Nutzer steht Ekiga zur Verfügung, Skype lässt sich über die Paketverwaltung nachinstallieren.

Den Grafik-Bereich bestücken Gimp, Krita, Inkscape und Blender, der Multimedia-Fundus umfasst unter anderem verschiedene Xine-, Mplayer- und Gstreamer-basierte Software sowie den beliebten VLC. Die üblicherweise benutzten Codecs finden sich in den Repositories. Eine vollständige Auflistung der vorhandenen Software findet man in der Anwendungsdatenbank MADB.

Server-Software

Auch für den Server-Einsatz bietet Mageia 4 eine breite Software-Auswahl. Als Webserver stehen Apache, Nginx oder Lighttpd zur Verfügung, als FTP-Server Heimdal-ftpd oder Proftpd.

Für Mailserver haben Sie die Wahl zwischen Postfix oder Sendmail als MTA sowie Dovecot oder Cyrus als POP/IMAP-Server. Den Viren- und Spam-Schutz decken ClamAV, Amavisd-new und Spamassassin ab.

Als Datenbank-Backend dienen MariaDB (als Ersatz für MySQL), PostgreSQL oder SQLite auf relationaler sowie CouchDB und MongoDB auf der Seite der nicht-relationalen Systeme.

Für Entwickler

Auch Entwickler finden bei Mageia 4 reichlich Futter. Neben geläufigen Sprachen wie C/C++, Java, Python, Perl, Ruby und PHP kommen auch Exoten wie Google Go, Haskell und Prolog nicht zu kurz. Mit von der Partie sind außerdem diverse Versionskontrollsysteme sowie die Entwicklungsumgebungen Eclipse, Anjuta und Kdevelop.

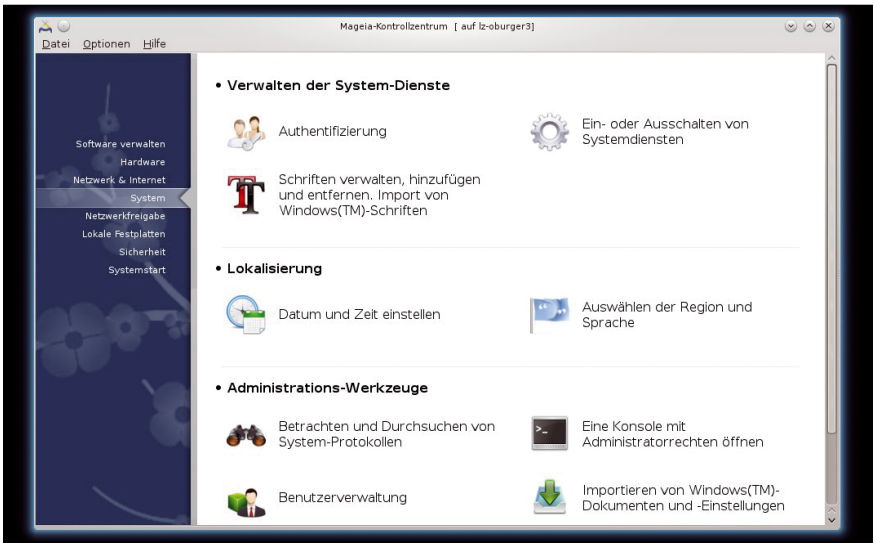
Die Repositories

Die offiziellen Mageia-Repositories gliedern sich in die drei Hauptzweige *Core*, *Tainted* und *Non-free*. Das Core-Repository enthält ausschließlich Open-Source-Programme, die nach Wissen der Mageia-Packager nicht durch Patente oder Lizenzen belastet sind.

Auch im *Tainted*-Repository findet sich Open-Source-Software, allerdings solche, bei der es unter Umständen patent- oder lizenzrechtliche Probleme geben kann. Dazu zählen etwa Audio- und Video-Codecs, die zum Abspielen von DVDs meist notwendige Libdvdcss2 oder der MP3-Encoder Lame. Das *Non-free*-Repository umfasst sämtliche unfreie Software, die das Projekt anbietet wie etwa Nvidia- und AMD-Grafiktreiber sowie manche Spiele.

Die Aufteilung der Software in die drei Zweige gestaltet sich so, dass *Core*-Software nie Pakete aus einem der anderen Repositories benötigt. Umgekehrt hängt aber Software aus einem der anderen Repositories unter Umständen von einem oder mehreren *Core*-Paketen ab.

Das Projekt versorgt alle drei Zweige mit Sicherheitsaktualisierungen und Fehlerkorrekturen. Standardmäßig bindet Mageia die drei Repos zwar ein, aktiviert allerdings nur *Core*. Möchten Sie auch *Tainted* und *Non-free* nutzen, müssen Sie diese im Mageia-Kontrollzentrum aktivieren.



4 **Das Mageia-Kontrollzentrum bietet alle Konfigurationswerkzeuge auf einen Blick.**

Bekannte Probleme

Nicht immer lassen sich bis zur Veröffentlichung einer Distributionsversion alle Fehler finden und beheben – das gilt auch für Mageia. Deswegen sollten Sie die Errata im Blick behalten und die Release Notes nachlesen. Dort finden Sie alle bestätigten Fehler der Distribution samt möglicher Problemlösungen.

Die momentan zur Verfügung stehenden ISO-Abbilder enthalten insbesondere zwei Fehler: Der erste liegt an Isolinux und führt dazu, dass gebrannte CDs und DVDs auf mancher Hardware nicht funktionieren. Der zweite hängt mit dem proprietären Nvidia-Treiber zusammen und hindert einige Programme am Start. Momentan erstellt das Projekt gerade neue ISOs, welche diese Probleme beheben sollen.

Fazit

Abgesehen von solchen unvermeidlichen Problemen präsentiert sich auch Mageia 4 wieder als „runde Sache“. Mit zunehmender Reife der Distribution füllen sich außerdem immer mehr Lücken in den Paket-Repositories, sodass der Paketumfang von Mageia inzwischen in Bezug auf die Software für die alltägliche Arbeit kaum noch irgendwelche Wünsche offenlässt. (jlu) ■

Weitere Infos und interessante Links

www.linux-user.de/qr/32205

Der Autor

Oliver Burger arbeitet als Übersetzer und Packager im Mageia-Projekt mit. Von 2011 bis 2013 war er im Council des Projekts vertreten, seit 2012 sitzt er im Board der Organisation Mageia.org.

Einbrüche mit dem IDS Tripwire erkennen

Stiller Wächter

Im hostbasierten Intrusion-Detection-System Tripwire finden Sie ein mächtiges Werkzeug, um Ihre Rechnersysteme vor ungewollten Änderungen zu schützen Falko Benthin

README

Was für die Regierung noch Neuland ist, entdeckten Ganoven schon längst für sich: das Internet und seine Möglichkeiten. Die Rechner ahnungsloser Bürger und Unternehmen mutieren zu Spam-Schleudern, verteilen Schadprogramme oder spähen Anwender aus. Das hostbasierte Einbruchserkennungssystem Tripwire überwacht still und leise das Dateisystem und informiert zeitnah bei festgestellten Änderungen.

Hinterlistige Trojaner, die Überweisungsdaten beim Online-Banking manipulieren oder Computernutzer ausspähen; ferngesteuerte Webcams, die ihre Umgebung abfilmen, oder versteckte Hintertürchen, die Unbefugten Zugriff auf fremde Rechner gewähren – das Verbrechen ist schon lange in der digitalen Welt angekommen.

Intrusion-Detection-Systeme, kurz IDS, erkennen potenzielle Angriffe auf Rechner und Netzwerke, indem sie den Datenverkehr überwachen und dabei typische Angriffsmuster und eventuelle Anomalien erkennen. Hostbasierte IDS hingegen spüren womöglich unerwünschte Änderungen auf zu schützenden Rechnern auf. Sie informieren dann die verantwortlichen Administratoren zeitnah und können so die mit einem Angriff einhergehenden Schäden eindämmen oder gar verhindern.

Für das freie Betriebssystem gibt es zahlreiche Intrusion-Detection-Systeme, sowohl für komplette Netzwerke („Network-based Intrusion Detection System“,

NIDS) als auch für einzelne Hosts („Host-based Intrusion Detection System", HIDS). Zur ersten Kategorie gehören beispielsweise Programme wie Snort, Suricata oder Prelude, die im Idealfall Angriffe auf gesamte Netzwerke erkennen. In die zweite Kategorie fallen etwa Anwendungen wie Portsentry, Logcheck, Samhain, OSSEC oder Tripwire, um das es in diesem Artikel geht.

Bei Tripwire (deutsch: „Stolperdraht") handelt es sich um einen Datei-Integritätschecker. Das System wurde 1992 von Gene Kim und Dr. Eugene Spafford an der Purdue University in West Lafayette (USA, Indiana) aus der Taufe gehoben. Seit 1999 entwickelt das Unternehmen Tripwire Inc. die Anwendung als Tripwire Enterprise weiter.

Das Tripwire-Open-Source-Projekt wurde 2002 ins Leben gerufen und nutzte als Grundlage die Tripwire-Quelltexte aus dem Jahr 2000. Das Projekt eignet sich laut Tripwire Inc. für eine kleine Anzahl von Servern, die weder eine zentralisierte Administration noch Berichtsfunktionen benötigen.

Funktionsweise

Angreifer versuchen in der Regel, ein gekapertes System mit Trojanern, Backdoors und veränderten Dateien zu kontaminieren, um jederzeit zurückkehren zu können und den Rechner in ihre Machenschaften zu involvieren.

Tripwire wirkt dem entgegen, indem es Informationen (Prüfsummen, Dateigröße, Mtime, Ctime, Inode etc.) wichtiger Verzeichnisse und Dateien verschlüsselt in einer Datenbank ablegt. Damit vergleicht es später die Eigenschaften der zu überwachenden Dateien und teilt Abweichungen dem verantwortlichen Administrator mit. Im Idealfall ist alles in Ordnung und der Bericht fällt kurz und knapp aus. Etwas längere Berichte entstehen, wenn Dateien gewollt oder ungewollt geändert wurden – dann muss der Admin handeln.

Das Prinzip bietet den Vorteil, dass Sie den Vergleich diskret periodisch oder bei Verdacht eines Einbruchs ausführen können. Da das Intrusion-Detection-System nicht permanent im Hintergrund läuft und so meist auch nicht als laufender Prozess auffällt, beansprucht es kaum Systemressourcen. Auch Fehlalarme kommen relativ selten vor. In der Regel wissen Administratoren, wann Tripwire ihre Server überwacht, und können so schnell die Datenbanken aktualisieren beziehungsweise sehen, ob sie eventuell selbst für eine gemeldete Änderung verantwortlich zeichnen.

Als klarer Nachteil wäre zu nennen, dass das System nicht sofort warnt, wenn ein mutmaßlicher Angriff stattfindet, sondern erst dessen Folgen protokolliert. Sobald Tripwire eine Meldung mit einer unberechtigten Änderung an einen Administrator versendet, darf dieser getrost von einer gelungenen Attacke ausgehen.

Tripwire 2.4.2.2
`LU/tripwire/`

Installation

In den Haupt-Repositories der gängigen Distributionen findet sich Tripwire in der Regel nicht. So stellt beispielsweise Ubuntu im *Universe*-Zweig nur für Saucy Salamander (13.10) die aktuelle Version zu Installation bereit, und auch OpenSuse hält Tripwire lediglich im *Security*-Repository vor, das Sie nachträglich manuell einbinden müssen.

Das Programm erfüllt seine Aufgaben bereits sehr gut, sodass die Entwickler nicht permanent neue Versionen nachle-

Listing 1

```
# twadmin --generate-keys --site-keyfile /etc/tripwire/site.key
# twadmin --generate-keys --local-keyfile /etc/tripwire/
$HOSTNAME-local.key
```

Reportlevel

Level	Beschreibung
0	Zusammenfassung auf einer Zeile, listet Anzahl der Änderungen, Hinzufügungen und Löschungen auf.
1	Parsbare Liste aller Verletzungen.
2	Zusammenfassung, Auflistung der Verletzungen nach Sektion im Polfile und Regelname.
3	Standardlevel, zeigt erwartete und erkannte Eigenschaften für überwachte Objekte, die geändert wurden.
4	Kompletter Bericht, der bis ins kleinste Detail geht.

gen. Aktuell ist die Version 2.4.2.2, die Sie mit dem Dreischritt aus den Quellen übersetzen:

```
# ./configure && make && make ins?
tall
```

Während der Installation legt Tripwire einen Site- und einen Local-Key an. Der Erstere dient dazu, um die Konfigurations- und Policy-Dateien zu signieren, der Letztere zur Absicherung der Tripwire-Datenbank. Haben Sie die Schlüsselgenerierung bei der Installation aus irgendeinem Grund ausgelassen, holen Sie sie mit den Befehlen aus Listing 1 nach.

Für die Passphrase gilt hier dasselbe wie für gute Passwörter: Mehr als acht Zeichen Länge, gemischte Groß- und Kleinschreibung sowie Sonderzeichen erhöhen die Sicherheit.

Eventuell müssen Sie auch noch die Datei `/etc/tripwire/twcfg.txt` anpassen. Dort hinterlegen Sie die Pfade zu den Schlüsseldateien, den Richtlinien, der Datenbank und den Berichten. Über weitere Variablen legen Sie den Standard-Editor (`EDITOR`) fest und geben an, ob Tripwire so lange wie möglich wartet, bis es eine Passworteingabe vom Nutzer verlangt (`LATEPROMPTING`). Auch Doppelmeldungen (Datei, Verzeichnis) bei Veränderungen einer überwachten Datei lassen sich an dieser Stelle unterbinden (`LOOSEDIRECTORYCHECKING`).

Da Tripwire auf entfernten Servern oft via Cronjob startet, kann es sich als sinnvoll erweisen, Mails auch dann zu versenden, wenn alles in Ordnung ist (`MAILNOVIOLATIONS=true`). Bleibt dann eine Nachricht aus, darf der Admin schon einmal in Alarmstellung gehen.

Die Reportlevel geben an, wie umfangreich Berichte ausfallen sollen (siehe Tabelle Reportlevel). Weiterhin könnten Art (SMTP oder Sendmail) und die für den Mailversand nötigen Server Aufmerksamkeit verlangen.

Stolperdrähte spannen

Sind die Keys vorhanden und die Konfigurationsdatei im Klartext angepasst, spannen Sie die Stolperdrähte in Form von Policies auf dem Server. In Tripwires Konfigurationsverzeichnis befindet sich mit hoher Wahrscheinlichkeit bereits eine kommentierte Datei `twpol.txt` mit Standard-Richtlinien, das Polfile. Da jedes System anders ist, bietet sie naturgemäß nicht den Schutz, den der individuelle Rechner benötigt. Vielmehr bietet sie eine gute Basis für eigene Anpassungen.

Die Policy-Datei nutzt einige Schlüsselwörter, denen ein `@@` vorsteht (siehe Tabelle Direktiven). Mit den Direktiven unterteilen Sie die Richtlinien in Bereiche mit spezifischen Bedingungen und individuellen Meldungen.

Regeln im Polfile beginnen mit dem zu überwachenden Objekt, bei dem es sich um eine Datei oder ein Verzeichnis handeln kann, gefolgt von –>, den zu überwachenden Eigenschaften („Properties“) und optionalen, in Klammern gesetzten Regelattributen. Häufig benötigte Properties fassten die Entwickler bereits in einigen Variablen zusammen.

Direktiven

Direktive	Beschreibung
`@@section`	Leitet Bereich im Polfile ein, OS-abhängig.
`@@ifhost`	Fallunterscheidungen, falls ein Polfile auf verschiedenen Hosts zum Einsatz kommt.
`@@else`	Siehe `@@ifhost`.
`@@endif`	Siehe `@@ifhost`.
`@@print`	Gibt folgenden String auf der Standardausgabe aus.
`@@error`	Gibt folgenden String auf der Fehlerausgabe aus.
`@@end`	Ende Polfile, alle folgenden Einträge werden ignoriert.

Regelattribute

Attribut	Beschreibung
`rulename`	Vergibt einen Namen für eine Regel. Standard ist das letzte Element des Objektnamens.
`severity`	Schärfe, Werte von 0 bis 1 000 000. Wird die Severity beim Integritätscheck angegeben, werden nur Regeln ab diesem Level geprüft.
`emailto`	E-Mail des Verantwortlichen, den Tripwire bei Unstimmigkeiten informiert.
`recurse`	Rekursion für Verzeichnisse, mögliche Werte sind `True`, `False` und Zahlen von -1 bis 1 000 000.
`onviolation`	Führt bei Unstimmigkeiten das angegebene Kommando aus.
`match`	Wildcard-Muster für Dateitypen, welche die Integritätsprüfung berücksichtigt

Eigenschaften

Property	Beschreibung
`a`	Atime
`b`	von Objekt belegte Blöcke
`c`	Zeitstempel, wann Inode erstellt oder modifiziert wurde
`d`	Device ID
`f`	Flags (betriebssystemabhängig)
`g`	Group-ID des Besitzers
`i`	Inode-Nummer
`l`	wachsende Datei
`m`	Mtime
`n`	Anzahl der Links
`p`	Dateirechte
`s`	Dateigröße
`u`	User-ID des Besitzers
`A`	ACL-Einstellungen
`C`	CRC-32
`G`	Inode Generation Number
`H`	HAVAL-Hash
`M`	MD5-Hash
`S`	SHA-Hash
Vordefinierte Variablen	
`ReadOnly`	`+pinugsmdbfCMAG`
`Dynamic`	`+pinugdfAG`
`Growing`	`+pinugdlfAG`
`IgnoreAll`	prüft nur, ob ein Objekt vorhanden ist
`IgnoreNone`	prüft alle Properties
`Device`	`+pugsdrfA`

Daneben erlaubt es das Regelset, eigene Variablen zu definieren, die Sie in der Datei mit `$(Variable)` aufrufen. Eine Regel erstreckt sich meist auf eine per Semikolon abgeschlossene Zeile. Regeln lassen sich zudem zu Gruppen zusammenfassen, um sie später leichter zu verwalten.

Tripwire kann zahlreiche Kriterien einer Datei im Blick behalten. Dazu gehören unter anderem Atime und Mtime, die von einem Objekt belegten Blöcke, die ID der Festplatte, Inode-Nummer, Dateigröße, User- und Group-ID sowie die Rechte. Ferner wählen Sie über die Properties das Hashverfahren aus. Einen Überblick über die wichtigsten Properties und die oben erwähnten vordefinierten Variablen gibt die Tabelle Eigenschaften.

Die Regelattribute erlauben es, Regeln mit berichtsfreundlichen Namen zu versehen, die Schärfe einer Regel einzustellen, eine E-Mail-Adresse und ein auszuführendes Kommando für den Fall eines Angriffs anzugeben oder Wildcard-Muster für zu berücksichtigende Dateitypen festzulegen. Weiterhin lässt sich die Tiefe der Rekursion angeben, mit der Tripwire die Inhalte eines Verzeichnisses berücksichtigt (siehe Tabelle Regelattribute).

Mittels der E-Mail-Adressen informiert die Software bei einem Angriff verschiedene Verantwortliche, beispielsweise Webmaster über geänderte PHP-Dateien und Administratoren bei Auffälligkeiten im Verzeichnis `/etc` oder `/sbin`. Dabei dürfen Sie mehrere Adressen durch ein Semikolon getrennt angeben. Das ausführende Kommando (`onviolation`) erlaubt es, beispielsweise Dienste sicherheitshalber anzuhalten.

Bei der Rekursion sind –1 und `True` identisch. In beiden Fällen berücksichtigt das Tool den gesamte Inhalt eines Verzeichnisses. Bei `0` oder `False` prüft Tripwire nur der Inode eines Verzeichnisses, wohingegen 1 bedeutet, dass das Tool auch die in einem Verzeichnis ent-

Listing 2

```
(
  rulename = "64 Bit Libs",
  severity = 100,
  emailto = "falko@mail.de;chef@
mail.de"
)
{
  /lib64     -> $(ReadOnly) ;
  /usr/lib64 -> $(ReadOnly) ;
}

/opt/nginx   -> $(ReadOnly)
(rulename = "Nginx", severity =
100, emailto = falko@mail.de) ;
```

```
• falko@zebra409: ~

  Rule Name                    Severity Level    Added    Removed  Modified
  ---------                    --------------    -----    -------  --------
  Invariant Directories        66                0        0        0
  Tripwire Data Files          100               0        0        0
  Other binaries               66                0        0        0
  Tripwire Binaries            100               0        0        0
  Other libraries              66                0        0        0
  Root file-system executables 100               0        0        0
  System boot changes          100               0        0        0
  Root file-system libraries   100               0        0        0
  (/lib)
  Critical system boot files   100               0        0        0
* Other configuration files    66                0        0        3
  (/etc)
  Boot Scripts                 100               0        0        0
  Security Control             66                0        0        0
* Root config files            100               0        0        2
  Devices & Kernel information 100               0        0        0
  (/dev)

Total objects scanned:  12253
Total violations found:  5
```

1 Tripwire gibt beim Integritätscheck eine kurze Zusammenfassung auf der Standardausgabe aus. Die zugehörigen Berichte zeigen meist deutlich mehr Details.

```
• k[redacted]: ~
[redacted]de-20131125-062558.twr
[redacted]de-20131126-062559.twr
[redacted]de-20131127-062743.twr
[redacted]de-20131128-062601.twr
[redacted]de-20131129-062625.twr
[redacted]de-20131130-062622.twr
[redacted]de-20131201-062623.twr
[redacted]de-20131202-062618.twr
[redacted]de-20131203-062622.twr
[redacted]de-20131204-060101.twr
[redacted]de-20131205-060101.twr
[redacted]de-20131206-060101.twr
[redacted]de-20131207-060101.twr
[redacted]de-20131208-060101.twr
[redacted]de-20131209-060101.twr
[redacted]de-20131210-060101.twr
[redacted]de-20131210-094355.twr
[redacted]de-20131211-060101.twr
[redacted]de-20131212-060101.twr
[redacted]de-20131213-060101.twr
[redacted]de-20131214-060101.twr
[redacted]de-20131215-060101.twr
[redacted]de-20131216-060101.twr
[redacted]:~$
```

2 Pro Cronjob und manuellem Integritätscheck ein Bericht: Wenn Sie diese nicht löschen, erzählen sie eine lange Geschichte von gewollten oder ungewollten Dateimanipulationen.

haltenen Dateien auf ihre Integrität prüft (nicht aber die Inhalte in dessen Unterverzeichnissen).

Eine besondere Regel definieren Stop-Points der Form *Objekt*; – dabei handelt es sich um von der Prüfung ausgeschlossene Verzeichnisse oder Dateien. Mit Stop-Points legen Sie entsprechend innerhalb eines zu prüfenden Verzeichnisses Ausnahmen fest.

Jeder Server ist anders und bedarf anderer Schutzmaßnahmen, sodass Sie das Policy-File für jeden Rechner individuell anpassen müssen. Die Default-Policy-Datei sollte bereits einen Mindestschutz bieten, der sich auf die Verzeichnisse `/boot`, `/bin`, `/sbin`, `/usr/bin`, `/usr/sbin`, `/usr/local/bin`, `/usr/local/sbin`, `/usr/lib`, `/usr/local/lib` und `/etc` erstreckt.

Listing 2 zeigt eine Erweiterung mit Regeln, die den Schutz auf 64-Bit-Bibliotheken und eine Nginx-Installation im Verzeichnis `/opt` ausweiten. Die Regel für die 64-Bit-Libs zeigt auch, wie Sie mehrere Objekte gruppieren. Zudem sind E-Mail-Adressen hinterlegt, sodass der Verantwortliche bei Vorfällen Mails erhält.

Nach dem Erstellen der Konfigurations- und Policy-Dateien gilt es, diese zu verschlüsseln, bevor Sie die Tripwire-Datenbank initialisieren. Die beiden Klartext-Dateien legen Sie auf der Kommandozeile mit den Befehlen aus Listing 3 an. Nach dem Verschlüsseln liegen Konfigurations- und Policy-Datei in einer nicht mehr ohne Weiteres lesbaren Form vor.

Im Anschluss an das erfolgreiche Anlegen der Tripwire-Datenbank sollten Sie die Klartext-Dateien entfernen. Falls Sie später noch einmal einen Blick darauf werfen möchten, dann dechiffrieren dazu die Befehle `twadmin --print-polfile` repektive `twadmin --print-cfgfile` die Dateien wieder.

Die Tripwire-Datenbank legen Sie mit dem Befehl `tripwire --init` an. Sie findet sich standardmäßig als Datei mit der Endung `.twd` im Verzeichnis `/var/lib/tripwire/` wieder. Eventuell meldet Tripwire ein paar Fehler, weil die Policy-Datei ungültige Einträge enthält – etwa nicht vorhandene Dateien. In dem Fall passen Sie die Policy-Datei an und generieren sie neu, bis Tripwire die Datenbank ohne Beanstandungen erstellt.

Prüfen und berichten

Bevor Sie Tripwire in einen Cronjob verpacken, sollten Sie prüfen, ob die Software anstandslos E-Mails versendet. Dazu dient folgender Befehl:

```
# tripwire --test --email Mailadresse@Domain.de
```

Anschließend führen Sie mit `tripwire --check` die erste richtige Integritätsprüfung durch 1. Tripwire gibt die Berichte in Kurzform auf der Konsole aus und schreibt sie parallel dazu etwas ausführlicher in die Datei `/var/lib/tripwire/report/$HOSTNAME-timestamp.twr` 2.

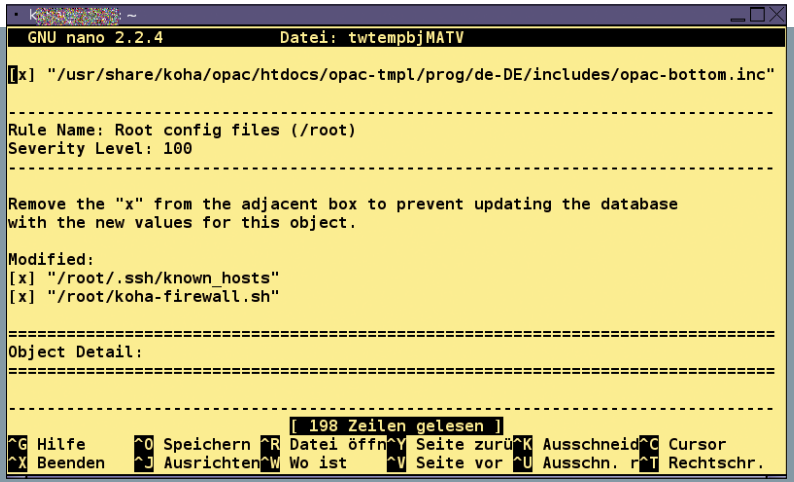
Sollen die Reports auch gleich per E-Mail versandt werden, geben Sie zusätzlich den Schalter `--email-report` an. Die Berichte gehen dann an die Empfänger, die Sie im Policy-File in den jeweiligen Regeln hinterlegt haben.

Hin und wieder kommt es vor, dass Admins die ein oder andere Kleinigkeit am System ändern. Da Tripwire nicht weiß, dass es sich um erlaubte Modifikationen handelt, strotzen dann die Berichte von Regelverletzungen nur so. Um das zu vermeiden, passen Sie die Tripwire-Datenbank auf Basis des Berichts an. Mittels des Kommandos:

```
# tripwire --update -twrfile /var/lib/tripwire/report/$HOSTNAME-timestamp.twr
```

öffnen Sie einen Editor, der alle Regelverstöße auflistet 3. Alternativ übernimmt die Software mit `tripwire --check --interactive` Änderungen auch sofort.

Tun Sie nun durch Nichtstun Ihr Einverständnis kund, passt Tripwire die Datenbank entsprechend an, und die Meldungen zu Integritätsverletzungen tre-



3 Nachvollziehbare und legitime Änderungen übernehmen Sie schnell und unkompliziert in die Tripwire-Datenbank.

ten bei zukünftigen Prüfungen nicht mehr auf. Ist eine Regelverletzung nicht genehmigt und soll bei jeder Prüfung wieder vorgelegt werden, entfernen Sie lediglich das Kreuzchen in der zur Regelverletzung gehörigen Checkbox.

Um einen Blick in die Tripwire-Datenbank zu werfen, nutzen Sie den Befehl `twprint --print-dbfile`. Ähnlich funktioniert es für eine eine binäre Berichtsdatei 4 mit folgendem Kommando:

```
# twprint --print-report --twrfile /var/lib/tripwire/report/$HOSTNAME-timestamp.twr
```

Laufen alle manuellen Checks zufriedenstellend, übernimmt ein Cronjob das Delegieren der Integritätsprüfung. Dazu öffnen Sie mit `crontab -e` als Root die Cron-Tabelle und erweitern sie um die Zeile:

```
00 5 * * * /usr/sbin/tripwire --check --email-report
```

Damit weiß das System, dass es täglich um 5:00 Uhr einen Check starten und per Mail darüber berichten soll.

Sicherheitstipps

Tripwire richten Sie am besten auf einem frisch aufgesetzten System ein, da nur in dem Fall sichergestellt ist, dass alle Dateien noch im Originalzustand vorliegen. Schlüssel, Policy-File und Konfigurationsdatei darf nur der Nutzer *root* lesen und schreiben, was folgendes Kommando sicherstellt:

```
# chmod 600 site.key $HOSTNAME-local.key tw.*
```

Auch auf die Verzeichnisse `/etc/tripwire` und `/var/lib/tripwire/` darf nur *root* zugreifen (`chmod 700 ...`).

Sofern irgend möglich, sollten Sie die Tripwire-Datenbank besonders schützen, sodass ein Angreifer keine Chance hat, sie zu ändern. Bei einem Desktop-Rechner bietet sich dazu ein externes Speichermedium an. Ein Server kann die Datenbank vor jedem Test via SSH und Public-Key-Verfahren von einem anderen Rechner herunterladen oder von einem nur lesbaren Medium beziehen.

```
k[redacted] ~
--------------------------------------------------------------------------------
Rule Name: Root config files (/root)
Severity Level: 100
--------------------------------------------------------------------------------
  ---------------------------------------
  Modified Objects: 2
  ---------------------------------------

Modified object name:  /root/.ssh/known_hosts

  Property:            Expected                  Observed
  -------------        -----------               -----------
* Size                 1326                      1768
* Modify Time          Mon Dec  9 12:25:54 2013  Tue Dec 10 12:53:21 2013
* Change Time          Mon Dec  9 12:25:54 2013  Tue Dec 10 12:53:21 2013
* CRC32                C22e8G                    Cl9aWO
* MD5                  AihWs1J+C8uA4yWNHL7Uhy    Bpz8hem9DoB8wRMX8+hmEy


Modified object name:  /root/koha-firewall.sh

  Property:            Expected                  Observed
  -------------        -----------               -----------
:
```

4 **Der Tripwire-Report zeigt recht ausführlich, wo Unstimmigkeiten auftreten.**

Fazit

Tripwire macht seinem Namen alle Ehre. Das einfache, aber wirkungsvolle Werkzeug ist schnell eingerichtet und versieht seinen Dienst still und diskret. Das HIDS wehrt zwar keine Angriffe ab, kann aber dazu beitragen, Unstimmigkeiten zeitnah zu erkennen. Normalerweise haben Admins nur eine geringe Chance, von Angreifern eingeschmuggelte, kontaminierte Dateien aufzuspüren. Tripwire serviert solche Kandidaten per E-Mail, was den Aufwand für Suche und Entfernung spürbar verringert.

Regeln lassen sich auch nachträglich noch gut anpassen. Die Berichtsdateien fallen meist recht klein aus, sodass die Gefahr einer langsam zulaufenden Festplatte kaum existiert. Erfolgten gewollte Änderungen, etwa durch ein Update oder geänderte Konfigurationsdateien, aktualisieren Sie die Datenbank ohne großen Aufwand. (tle) ■

Weitere Infos und interessante Links
www.linux-user.de/qr/31567

Listing 3

```
# twadmin --create-cfgfile --cfgfile tw.cfg --site-keyfile site.key twcfg.txt
# twadmin --create-polfile --polfile tw.pol --cfgfile tw.cfg --site-keyfile site.key twpol.txt
```

Vorschau auf 05/2014

Die nächste Ausgabe erscheint am 17.04.2014

Private Cloud aufsetzen und optimal nutzen

Nach der Datenhunger der Geheimdienste immer deutlicher zutage tritt, beginnt landauf, landab der Rückzug aus den vernetzten Systemen. In erster Linie betrifft das die Dateien in der Cloud, also den weltumspannenden Online-Speichern. Wir zeigen, wie Sie eine private Wolke in Hardware oder Software aufsetzen, um wichtige Daten vor dem unbefugten Zugriff zu schützen. Dabei haben wir maßgeschneiderte Lösungen im Angebot, die vom Einzelplatz bis zum kleinen Netzwerk alles bedienen.

Dateisystem ZFS

Trotz der nicht ganz freien Lizenz ist ZFS häufig unter Linux im Einsatz. Es punktet mit ausgefeilten Funktionen und einer gigantischen theoretischen Speicherkapazität. Beim Setup auf dem Heim-PC gibt es aber einiges zu beachten.

Flyer-Design mit Scribus

Wer seine Info-Broschüren noch auf klassische Weise erstellen möchte, der hat mit dem freien DTP-Programm Scribus das richtige Werkzeug an der Hand. Wir führen Sie Schritt für Schritt von der ersten Linie bis zum druckreifen PDF.

Heft als DVD-Edition

- 108 Seiten Tests und Workshops zu Soft- und Hardware
- Multiboot-DVD-10 mit Top-Distributionen sowie der Software zu den Artikeln, DVD-5 mit exklusiver LinuxUser-Edition einer aktuellen Distribution

Heft als No-Media-Edition

- Preisgünstige Heftvariante ohne Datenträger für Leser mit Breitband-Internet-Anschluss
- Artikelumfang identisch mit der DVD-Edition: 108 Seiten Tests und Workshops zu aktueller Soft- und Hardware

Community-Edition-PDF

- Über 30 Seiten ausgewählte Artikel und Inhaltsverzeichnis als PDF-Datei
- Unter CC-Lizenz: Frei kopieren und beliebig weiter verteilen
- Jeden Monat kostenlos per E-Mail oder zum Download

Für nur 8,50 Euro (DVD-Edition) bzw. 5 Euro (No-Media-Edition) am Kiosk oder bestellen unter:

http://www.linux-user.de/bestellen

Jederzeit gratis herunterladen unter:

http://www.linux-user.de/CE

Impressum

LinuxUser ist eine monatlich erscheinende Publikation der Linux New Media, eines Geschäftsbereichs der Medialinx AG.

Anschrift
Putzbrunner Str. 71
81739 München
Telefon: (089) 99 34 11-0
Fax: (089) 99 34 11-99

Homepage http://www.linux-user.de
Artikel und Foren http://www.linux-community.de
Abo/Nachbestellung http://www.linux-user.de/bestellen/
E-Mail (Leserbriefe) <redaktion@linux-user.de>
E-Mail (Datenträger) <cdredaktion@linux-user.de>
Abo-Service <abo@linux-user.de>
Pressemitteilungen <presse-info@linux-user.de>

Chefredakteur Jörg Luther (jlu, v. i. S. d. P.) <jluther@linux-user.de>
Stellv. Chefredakteur Andreas Bohle (agr) <abohle@linux-user.de>
Redaktion Thomas Leichtenstern (tle) <tleichtenstern@linux-user.de>
Linux-Community Andreas Bohle (agr) <abohle@linux-community.de>
Datenträger Thomas Leichtenstern (tle) <tleichtenstern@linux-user.de>
Ständige Mitarbeiter Erik Bärwaldt, Falko Benthin, Mario Blättermann, Florian Effenberger, Karsten Günther, Frank Hofmann, Peter Kreußel, Hartmut Noack, Tim Schürmann, Dr. Karl Sarnow, Vincze-Áron Szabó, Ferdinand Thommes, Uwe Vollbracht, Harald Zisler

Grafik Elgin Grabe (Titel und Layout)
Bildnachweis: Stock.xchng, 123rf.com, Fotolia.de u. a.
Sprachlektorat Astrid Hillmer-Bruer
Produktion Christian Ullrich <cullrich@medialinx-gruppe.de>
Druck Vogel Druck und Medienservice GmbH & Co. KG 97204 Höchberg

Geschäftsleitung Brian Osborn (Vorstand, verantwortlich für den Anzeigenteil) <bosborn@medialinx-gruppe.de>
Hermann Plank (Vorstand) <hplank@medialinx-gruppe.de>

Mediaberatung
D / A / CH Petra Jaser <pjaser@medialinx-gruppe.de>
Tel.: +49 (0)89 / 99 34 11 24
Fax: +49 (0)89 / 99 34 11 99
USA / Kanada Ann Jesse <ajesse@linuxnewmedia.com>
Tel.: +1 785 841 88 34
Darrah Buren <dburen@linuxnewmedia.com>
Tel.: +1 785 856 3082
Andere Länder Penny Wilby <pwilby@linuxnewmedia.com>
Tel.: +44 1787 21 11 00

Es gilt die Anzeigenpreisliste vom 01.01.2014.

Pressevertrieb MZV Moderner Zeitschriften Vertrieb GmbH & Co. KG
Ohmstraße 1
85716 Unterschleißheim
Tel.: (089) 3 19 06-0
Fax: (089) 3 19 06-113

Abonnentenservice D / A / CH Gudrun Blanz (Teamleitung) <abo@linux-user.de>
Postfach 1165
74001 Heilbronn
Telefon: +49 (0)7131 27 07-274
Fax: +49 (0)7131 27 07 -78-601

Abo-Preise LinuxUser	Deutschland	Österreich	Schweiz	Ausland EU
No-Media-Ausgabe (ohne Datenträger [1])	€ 5,95	€ 6,70	Sfr 11,90	(siehe Titel)
DVD-Ausgabe (mit 2 Datenträgern)	€ 8,50	€ 9,35	Sfr 17,00	(siehe Titel)
Jahres-DVD (Einzelpreis)	€ 14,95	€ 14,95	Sfr 18,90	€ 14,95
Jahres-DVD (zum Abo [2])	€ 6,70	€ 6,70	Sfr 8,50	€ 6,70
Mini-Abo (3 Ausgaben)	€ 3,00	€ 3,00	Sfr 4,50	€ 3,00
Jahres-Abo (No-Media-Ausgabe)	€ 60,60	€ 68,30	Sfr 99,90	€ 81,00
Jahres-Abo (DVD-Ausgabe)	€ 86,70	€ 95,00	Sfr 142,80	€ 99,00
Preise Digital	**Deutschland**	**Österreich**	**Schweiz**	**Ausland EU**
Heft-PDF (Einzelausgabe)	€ 5,95	€ 5,95	Sfr 7,70	€ 5,95
Digi-Sub (12 Ausgaben)	€ 60,60	€ 60,60	Sfr 78,70	€ 60,60
Digi-Sub (zum Abo [2])	€ 12,00	€ 12,00	Sfr 12,00	€ 12,00
HTML-Archiv (zum Abo [2])	€ 12,00	€ 12,00	Sfr 12,00	€ 12,00
Preise Kombi-Abos	**Deutschland**	**Österreich**	**Schweiz**	**Ausland EU**
Mega-Kombi-Abo (LU plus LM [3])	€ 143,40	€ 163,90	Sfr 199,90	€ 173,90

(1) Die No-Media-Ausgabe erhalten Sie ausschließlich in unserem Webshop unter http://www.medialinx-shop.de, die Auslieferung erfolgt versandkostenfrei.
(2) Ausschließlich erhältlich in Verbindung mit einem Jahresabonnement der Print- oder Digital-Ausgabe von LinuxUser.
(3) Das Mega-Kombi-Abo umfasst das LinuxUser-Abonnement (DVD-Ausgabe) plus das Linux-Magazin-Abonnement inklusive DELUG-Mitgliedschaft (monatliche DELUG-DVD) sowie die Jahres-DVDs beider Magazine.

Informationen zu anderen Abo-Formen und weiteren Produkten der Medialinx AG finden Sie in unserem Webshop unter http://www.medialinx-shop.de.
Gegen Vorlage eines gültigen Schülerausweises oder einer aktuellen Immatrikulationsbescheinigung erhalten Schüler und Studenten eine Ermäßigung von 20 Prozent auf alle Abo-Preise. Der Nachweis ist jeweils bei Verlängerung neu zu erbringen.
Bitte teilen Sie Adressänderungen unserem Abo-Service (<abo@linux-user.de>) umgehend mit, da Nachsendeaufträge bei der Post nicht für Zeitschriften gelten.

ISSN: 1615-4444