Kurztipp: Verschlüsselt installieren

von Bodo Schmitz

Vollverschlüsselung ist seit Debian Etch ohne große Probleme möglich – gewisse Erfahrung in diesem Bereich vorausgesetzt. Dieser Kurztipp soll den Artikel „Ubuntu-Systemverschlüsselung per Alternate-CD“ von Dominik Wagenführ in freiesMagazin 05/2010 [1] ergänzen und so manchem Interessierten verschiedene Stolpersteine aus dem Weg räumen.

Stand der Dinge

Generell ist beim Wunsch einer Vollverschlüsselung eine „richtige“ Installations-CD (sogenannte Alternate- oder Netinstall-CD) notwendig. Eine Live-CD, mit der sich dies bewerkstelligen ließe, scheint bis zum heutigen Tage nicht vorzuliegen. Dies darf auch als Aufruf an die Distributoren verstanden werden, ihre Installer entsprechend anzupassen. Debian-/Ubuntu-seitig ist dies seit Debian Etch fast kein Problem mehr. In der RPM-Welt unterstützt Fedora Core inzwischen auch Vollverschlüsselung, Mandriva aber überraschenderweise nicht. Unter openSUSE fehlen mir entsprechende Erfahrungswerte.

Der Etch-Installer („oldstable“) hat im Modul zur Konfiguration einen defekten „Zurück“-Button, der zum Hängenbleiben des Programms führt. Hat man diesen versehentlich erwischt, bleibt einem nichts anderes als den Rechner durch einen „Affengriff“ Strg + Alt + Entf neu zu starten und von vorne zu beginnen.

Der Hardy-Installer („oldLTS“) hat ein Problem mit verschlüsselten Swap-Partitionen. Der Ladevorgang des zugehörigen Konfigurationsmoduls beginnt, bleibt dann aber reproduzierbar mittendrin hängen. Man behilft sich bei diesem Problem wie folgt: Entweder lässt man die Swap-Partition zunächst weg oder legt sie erst einmal unverschlüsselt an. Nach dem anschließenden ersten Start des neuen Systems kann man entweder die Swap-Partition auf Verschlüsselung umstellen, oder alternativ eine (verschlüsselte) Swap-Datei anlegen. Beides wird im ubuntuusers-Wiki beschrieben [2].

Tipps zum verschlüsselten Swap

Will man eine Swap-Datei zur Laufzeit aushängen, lässt sich dies mit folgendem Kommando machen.

```
# swapoff /Pfad/zur/SWAPDATEI
```

Eine verschlüsselte Swap-Partition macht man dem System folgendermaßen bekannt: In die Datei **/etc/crypttab** fügt man mit entsprechenden Root-Rechten die Zeile

```
sdX1_crypt /dev/sdX1 /dev/urandom ↷
cipher=aes-cbc-essiv:sha256,size↷
=256,swap
```

ein. sdX1 bzw. sdX1_crypt stellt hier die Partitionsbezeichnung der Swap-Partition dar.

In die Datei **/etc/fstab** trägt man mit Root-Rechten ein:

```
/dev/mapper/sdX_crypt none ↷
            swap     sw 0       0
```

In die Datei **/etc/initramfs-tools/conf.d/resume** ist Folgendes einzutragen, auch wiederum mit Root-Rechten:

```
RESUME=/dev/mapper/sdX1_crypt
```

Danach sollte man das initrd-Image mit dem Befehl

```
# update-initramfs -u
```

neu schreiben lassen. Nach dem Neustart des Rechners sollte das System die verschlüsselte Swap-Partition erkennen.

Allgemeine Tipps

Hier noch ein paar zusätzliche Hinweise bzgl. der Hardy-Installation: Die Installation von der Alternate-CD sollte grundsätzlich im – gleich strukturierten – Textmodus durchgeführt werden, da grafisch keine Verschlüsselung möglich ist.

Sollte es aufgrund problematischer Hardware zu Bootproblemen des Installationsmediums kommen, helfen möglicherweise folgende Cheatcodes am Boot-Prompt (eventuell kombiniert man diese): „noapic“, „nolapic“, „acpi=off“, bei Grafikproblemen (z. B. bei verschiedenen Notebooks) kann man „fb=false“ versuchen [3].

Wenn das Netzwerk nicht erkannt wird, sollte man dies einfach ignorieren und trotzdem die Installation durchführen. Nach dem ersten Start des installierten Systems wird es zumeist erkannt.

Manchmal darf sich der Benutzer Root nicht an der grafischen Benutzeroberfläche anmelden. In der Konsole klappt dies dann aber doch über

```
$ sudo -i
```

Nach dem ersten Einloggen sollte man zunächst die Updates via

```
# apt-get update && apt-get upgrade↷
 && apt-get clean && apt-get ↷
autoclean
```

holen. Um (unter K/Ubuntu) dem Benutzer Root das grafische Anmelden zu erlauben, kann man nun mit einem Konsolen-basierten Texteditor (bspw. nano) in der Datei **/etc/kde3/kdm/kdmrc** den Eintrag „AllowRootLogin“ von „false“ auf „true“ ändern – natürlich braucht es dazu Root-Rechte. Nach dem nächsten Neustart wird dem Benutzer Root das Einloggen nicht mehr verwehrt.

GIMP lässt sich durch Installation der Pakete **language-pack-gnome-de** und **language-pack-gnome-de-base** eindeutschen. OpenOffice.org ebenfalls durch **openoffice.org-l10n-de** und eventuell weitere abhängige Pakete.

Achtung: Nach dem ersten Systemupdate und anschließendem Neustart ist einmalig das Dateisystem „dirty“ und sollte daher z. B. via Live-CD (Knoppix, Sidux, Kanotix, grml oder andere) durch eine Überprüfung des Dateisystems mit dem Programm fsck wieder konsistent gemacht werden. Das erledigt man mit Root-Rechten wie folgt, indem man den Container zuerst öffnet:

```
# cryptsetup luksOpen /dev/sdXY ↷
sdXY
```

Hinweis: sdXY stellt die Partitionsbezeichnung dar. Auch sollte man die exakte Schreibweise des Befehls **luksOpen** mit großem „O“ beachten.

Danach folgt die Dateisystemüberprüfung, bei einer Partition mit einem Ext3-Dateisystem zum Beispiel mit dem Befehl

```
# fsck.ext3 /dev/mapper/sdXY
```

Anschließend schließt man den Container wieder durch folgenden Befehl:

```
# cryptsetup luksClose sdXY
```

Auch hier wieder daran denken: **luksClose** mit großem „C“ schreiben! Danach darf man den Rechner neu starten.

Legt man nun noch Wert auf eine erhöhte Sicherheit des Journals, kann man dies mit

```
# tune2fs -o journal_data /dev/↷
mapper/sdXY
```

an ausgehängten Partitionen einstellen. Der obige tune2fs-Befehl bewirkt, dass nicht nur die Metadaten, sondern die eigentlichen Daten selbst ins Journal und anschließend fest ins Dateisystem geschrieben werden. Das führt zwar zu Geschwindigkeitsverlusten bei der Datenrate, erhöht aber die Chancen, im Falle eines Crashs ein konsistentes Dateisystem zu behalten bzw. die Daten fehlerfrei und vollständig restaurieren zu können. Eine Überprüfung der Einstellungen der jeweiligen Partition lässt sich via

```
# tune2fs -l /dev/mapper/sdXY
```

ereichen, womit die Informationen aus dem Superblock der jeweiligen Partition ausgelesen werden.

LINKS

[1] http://www.freiesmagazin.de/freiesMagazin-2010-05

[2] http://wiki.ubuntuusers.de/Swap

[3] http://wiki.ubuntuusers.de/Booten

Autoreninformation

Bodo Schmitz setzt seit ca. 6 Jahren ausschließlich auf Linux und hat dabei viele Erfahrungen mit verschiedenen Systemen gesammelt.

Diesen Artikel kommentieren