Kurztipp: Heimcontainer oder Datentresor ohne TrueCrypt

von Bodo P. Schmitz

Auch wenn TrueCrypt derzeit wohl als vertrauenswürdig gelten darf [1], so bietet es sich an, eine Verschlüsselung mit Bordmitteln umzusetzen, um Passwörter, Zugangsdaten oder sonstige Daten sicher aufzubewahren und zu transportieren.

Ein möglicher Weg wäre das dateibasierte EncFS. Eine leicht zu „transportierende“ Möglichkeit ohne dessen Nachteile einer ordnerbasierten Verschlüsselung bietet sich mit dm-crypt an, da dieses nicht nur Partitionen, sondern auch Container-Dateien verschlüsseln kann – allerdings benötigt man dazu root-Rechte!

Zunächst erzeugt man einen Container von z. B. 10MB Größe.

```
# dd if=/dev/zero bs=10M count=1 of=/Pfad/zu/container.crypt
```

Da dm-crypt nicht das Konzept der „Glaubhaften Abstreitbarkeit“ [2] unterstützt, bietet sich alternativ die Wahl eines unverfänglichen Namens wie z. B. urlaub.jpg an.

Der Container wird dann verschlüsselt:

```
# cryptsetup luksFormat -c aes-xts-plain64 -s 512 /Pfad/zu/container.crypt
```

Wie üblich muss die folgende Frage mit großgeschriebenem **YES** quittiert werden. Danach folgt zur Sicherheit die doppelte Eingabe der Passphrase.

Dann wird der Container geöffnet:

```
# cryptsetup luksOpen /Pfad/zu/container.crypt crypt
```

Anschließend wird der Container mit einem Dateisystem formatiert:

```
# mkfs.ext4 /dev/mapper/crypt
```

Es muss natürlich ein Mountpunkt für den Container existieren – diesen ggf. vorher mit

```
# mkdir /media/crypt
```

anlegen. Damit der nicht-privilegierte Benutzer auf den Container zugreifen kann, sind noch die Zugriffsrechte entsprechend anzupassen:

```
# chown Name:Gruppe /media/crypt/
```

Die User-ID (**uid**) und Group-ID (**gid**) können mit dem Befehl **id** abgefragt werden. Der Container kann danach eingebunden werden:

```
# mount /dev/mapper/crypt /media/crypt
```

Anschließend kann der Container (auch als nicht-privilegierter Benutzer) beschrieben werden.

Ausgehängt wird er mit:

```
# umount /media/crypt/
```

Abschließend wird der Container geschlossen:

```
# cryptsetup luksClose crypt
```

Ein Vorteil dieser Methode ist, dass die verschlüsselte Containerdatei **container.crypt** bequem und sicher selbst über einen unverschlüsselten USB-Stick oder das unsichere Internet auf andere Computer übertragen werden kann – vorausgesetzt, die eingesetzten Rechner können mit dm-crypt und dem Dateisystem des verschlüsselten Containers umgehen.

LINKS

[1] http://heise.de/-2035104

[2] https://de.wikipedia.org/wiki/Glaubhafte_Abstreitbarkeit

Autoreninformation

Bodo P. Schmitz (Webseite) hat in den letzten zehn Jahren rund 200 Installationen verschiedener Distributionen durchgeführt.

Diesen Artikel kommentieren