Partitionen Verschlüsseln mit Debian Linux und cryptsetup

Inhalt: Seite:

1. Einleitung

Daten für Mitmenschen unerreichbar machen? Wozu einzelne Daten mit Passwörtern versehen, wenn es doch so einfach ist eine ganze Partition jemand anderen vorzuenthalten? Wie sich das Ganze einrichten lässt werde ich euch nun erklären. Ihr müsst eigentlich nichts anderes machen als den Anweisungen zu folgen. Natürlich sind einige Vorraussetzungen gesetzt. U.A. müsst ihr in der Lage sein, einen Kernel zu kompilieren. Wie das geht, werde ich vielleicht später mal erklären. Heute steht jedoch die Kryptographie auf dem Programm.
Zur Verschlüsselung werden wir cryptsetup mit AES Algorithmen nutzen. Alle AES Algorithmen sind für Schlüssellängen von 128-256 Bit definiert worden und sollten für unsere Verschlüsselung genügen ;)

2. Vorbereitung

a) Kernel

Im Kernel müssen einige neue Module hinzugefügt werden. Diese werden jedoch erst ab 2.6.4 unterstützt. Da Debian von Hause aus einen 2.4er Kernel mitbringt, sind wir gezwungen einen neuen zu kompilieren. Im Kernel müssen folgende Module hinzugefügt werden:

- Code maturity level options →
  - Prompt for development and/or incomplete code/drivers
- General setup →
  - Support for hot-pluggable devices
- Device Drivers →
  - Multi-device support (RAID and LVM) →
    - Device mapper support
    - Crypt target support
- Cryptographic options →
  - AES cipher algorithms

Nach einem erfolgreichen Booten des neuen Kernels, können wir noch überprüfen ob die Module korrekt installiert sind:

1) Wir überprüfen ob die Device Mapper existieren:

```
# ls –L /dev/mapper/control
```

2) Wir überprüfen ob AES unterstützt wird:

```
# cat /proc/crypto
```

b) Pakete

dmcrypt muss natürlich auch noch installiert werden. Dazu führen wir ganz einfach

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

aus. Cryptsetup erleichtert uns das Arbeiten mit dmcrypt und da cryptsetup von dmcrypt abhängt, wird es auch gleich mitinstalliert.

Nach der Installation können wir mit

```
# dmsetup targets
```

überprüfen ob das Paket auch korrekt installiert wurde.

```
crypt        v1.0.0
striped      v1.0.1
linear       v1.0.1
error        v1.0.1
```

3. Partition verschlüsseln und verwenden

Nun beginnt der eigentliche Teil der ganzen Aktion. Wir werden nun eine Partition verschlüsseln. Diesen Vorgang werde ich in drei Unterpunkte teilen:

1) cryptsetup ausführen
2) Ein Filesystem auf dem neuen Device erstellen
3) Das neue Device einbinden

1) Cryptsetup verwenden

Wir führen folgendes Kommando aus:

```
# cryptsetup -y create <label> /dev/hdxy
```

Wobei ‚<label>' eine Beschreibung des neuen Devices ist. ‚/dev/hdxy' muss natürlich entsprechend der Festplatte und Partition angepasst werden. Die Option ‚–y' lässt das Passwort zwei mal abfragen.
Anschließend lässt sich mit

```
# dmsetup ls
```

Überprüfen ob die Aktion geglückt ist.

(Wichtig: merkt euch, was ihr für <label> angegeben habt! Ihr werdet es noch brauchen ;))

2) Dateisystem erstellen

Wir müssen nun ein Dateisystem auf dem neu erstellten Device erstellen. Dazu ist es euch überlassen, welches Dateisystem ihr bevorzugt. Ich nutze das ext3-FS.

```
# mkfs.ext3 /dev/mapper/<label>
```

Wer das ReiserFS bevorzugt, nutzt folgendes Kommando:

```
# mkfs.reiserfs /dev/mapper/<label>
```

3) Device einbinden

Schließlich muss die Verschlüsselte Partition noch eingebunden werden:

```
# mount /dev/mapper/<label> /mnt/cryptodrive
```

4. Automatisieren

Da nun aber nach jedem Neustart des Systems die mit cryptsetup erstellten Devices ‚zerstört' werden, sind wir gezwungen sie jedes Mal neu zu erstellen. Um dem entgegenzuwirken, werden wir uns ein kleines Script schreiben, welches dies für uns übernimmt.

Wir starten also den bevorzugten Editor und schreiben den folgenden Text in die Datei.

```
if [ -b /dev/mapper/<label> ]; then
/sbin/cryptsetup remove <label>
fi
/sbin/cryptsetup create <label> /dev/hdxy
mount /dev/mapper/<label> /mnt/crypto
```

Zu Beachten ist hierbei, dass ihr wieder ‚<label>', ‚/dev/hdxy' sowie euren Mountpunkt ‚/mnt/crypto' anpassen müsst!

Schließlich führen wir es aus das war's schon.

Erstellt am 7. Februar 2006
von ‚Ich mag meinen Nick nicht'
für Spieleplanet.ch -