

Tuesday, October 10, 2017

Verschlüsselte Filesysteme unter Linux: Anlegen und vergrößern

Dies ist primär ein Eintrag für mich, damit ich nicht vergesse wie ich Dinge aufgesetzt habe

Ich habe ein Filesystem das verschlüsselt werden soll - es ist keine Systemplatte sondern Nutzdaten. Damit kann ich mir sparen, große Verrenkungen machen zu müssen wegen Root- oder Bootpartition. Also, einfach nur eine Festplatte, oder besser: ein Volume. Da ich potentiell mit RAID0 arbeiten möchte (Stripes) oder Platten konkatenieren möchte, bietet sich lvm mit LUKS zusammen an. lvm und LUKS können andere Leute viel besser erklären, daher erspare ich mir das.

Also erstellen wir erst einmal ein logisches Volumen (pv und vg sind bereits angelegt)

```
lvcreate -L 1T -n Daten-crypt Daten
```

Hiermit erstelle ich ein logisches Volumen aus der Volume Group "Daten". Diese ist 1TeraByte groß und heisst dann "Daten-crypt".

```
cryptsetup -y --cipher aes-cbc-essiv:sha256 --key-size 256 luksFormat /dev/Daten/Daten-crypt
```

Hiermit erstelle ich eine verschlüsselte Partition auf dem Volumen Daten-Crypt. Ich gebe dann das Passwort ein das ich dafür nutzen möchte. Das sollte ich tunlichst mir aufschreiben

OpenMediaVault hat netterweise ein gutes GUI, mit dem ich auch solche Filesysteme aufmachen kann. Dann muss ich mir den CLI-befehl nicht unbedingt merken:

```
cryptsetup luksOpen /dev/Daten/Daten-crypt Daten-crypt
```

Wunderbar, das funktioniert.

Wenn ich dies nun erweitern möchte, geht das wie folgt:

Ich öffne das verschlüsselte Filesystem und unmounte es, falls es gemounted ist.

Dann vergrößere ich das Volumen:

```
lvresize -L +500G /dev/mapper/Daten-Daten--crypt
```

dann - weil ich vorsichtig bin - mache ich einen Filesystemcheck:

```
e2fsck -f /dev/mapper/Daten-Daten--crypt-crypt
```

Das sollte sauber durchlaufen, ohne Probleme!

Wenn das geschafft ist, kann man das verschlüsselte Volumen auch "ordentlich" vergrößern:

```
cryptsetup resize /dev/mapper/Daten-Daten--crypt-crypt
```

Damit wird dem Filesystem quasi gesagt, dass sich das darunterliegende Volume geändert hat. Wenn keine Fehlermeldung kommt ist alles gut

```
resize2fs -p /dev/mapper/multimedia-multimedia--crypt-crypt
```

Hiermit wird das Filesystem dann wirklich vergrößert.

Ich mache danach üblicherweise noch einen Filesystemcheck, bevor ich das Filesystem wieder in Benutzung nehme.

Posted by rince at 20:43

cryptsetup resize kannte ich noch nicht.

Die Problematik, nur die Datenpartition zu verschlüsseln ist, dass Dir dann jemand ganz einfach ein cryptsetup-Binary unterschieben kann, das die Passwordeingabe mitlogged und das Passwort irgendwo hin schicken kann (oder sich bei der Gelegenheit einen zweiten Keyslot belegen könnte).

Und diese Problematik schlägt dann bei Vollverschlüsselung auf Kernel und Initrd durch, was direkt zu secure boot führt, was dafür sorgt, dass Du Deinem Hardwarehersteller trauen musst. Und dass die meisten staatlichen Angriffe über trojanisierte Firmware laufen werden, ist meine feste Meinung.

Für den Namen der LV nehme ich meist c_foo und foo, das macht die tab completion in /dev/mapper nicht kaputt. Underscore deswegen, weil dashes in /dev/mapper bereits benutzt werden, das escaping, das dann durchgeführt wird tut in Scripts weh.

Anonymous on Oct 11 2017, 08:23