

Dienstag, 11. August 2015

Wie man Katastrophen abwendet, heute: LÄschen von LUKS-SchlÄsseln

Ich bin deutlich zu experimentierfreudig.

Ich habe vor einiger Zeit meinem Laptop beigebracht, die verschlÄsselte LUKS-Partition nicht nur Äber eine Passphrase, sondern auch Äber eine (andere) Passphrase, gepaart mit meinem Yubikey zu entschlÄsseln.

Das hat sich heute gerÄcht, weil ich den Yubikey fÄr andere Zwecke umkonfiguriert hatte. Ich dachte dann, diesen Slot in LUKS iÄschst Du mal.

DafÄr muss man immer noch ein funktionierendes Passwort angeben.

Dumm nur: Es wurde das Passwort gelÄscht welches ich eingegeben hatte. Ganz dumme Geschichte - damit wÄre beim nÄchsten hochfahren das System nicht mehr hochgekommen, weil kein EntschlÄsselungs-SchlÄssel mehr bereit gewesen wÄre; den initialen hatte ich gerade gelÄscht und der Yubikey hatte andere Werte.

Was tun fragte ich mich, besonders weil eine Suchmaschinen-Suche auf diese Fragestellung keine eindeutige Antwort gab. Ich sah mich schon alles Backuppen, formatieren und restoren (oder - wenn ich gut drauf gewesen wÄre - neues Device mit luks anlegen, dd if.. of ... von A nach B schieben).

Mein GlÄck ist, dass das Laufwerk ja noch online und damit geÄffnet ist. Auch der Master-Key ist (fÄr root) auslesbar.

Zugschlus ist gerade auf der DebConf und hat Margarita ManterolagegenÄber sitzen. Und sie kennt luks sehr gut. Ich weiss nicht ob sie aus Erfahrung spricht, aber sie hat den richtigen Tip gehabt:

```
# cryptsetup luksAddKey $device_name --master-key-file
```

Geschrieben von rince um 17:34

Zum VerstÄndnis:

Luks hat den master key unencrypted und auslesbar im Speicher und ein tool um ihn auszulesen. Als Angreifer der irgendwie temporÄr root bekommt reicht also ein kommando um offline die platte zu decrypten, wenn der Rechner ausgeschaltet wurde.
Anonym am Aug 11 2015, 18:38

Brauchst Du Dir nicht merken, wirst Du nie wieder brauchen.

Anonym am Aug 12 2015, 10:09

Das wird wohl nicht anders gehen wÄhrend das Device aufgeschlossen ist.

Anonym am Aug 12 2015, 10:10