Tuesday, August 11. 2015

Wie man Katastrophen abwendet, heute: LÃ¶schen von LUKS-SchlÃ¼sseln

Ich bin deutlich zu experimentierfreudig.

Ich habe vor einiger Zeit meinem Laptop beigebracht, die verschlÃ¼sselte LUKS-Partition nicht nur Ã¼ber eine Passphrase, sondern auch Ã¼ber eine (andere) Passphrase, gepaart mit meinem Yubikey zu entschlÃ¼sseln.

Das hat sich heute gerÃ¤cht, weil ich den Yubikey fÃ¼r andere Zwecke umkonfiguriert hatte. Ich dachte dann, diesen Slot in LUKS lÃ¶schst Du mal.

DafÃ¼r muss man immer noch ein funktionierendes Passwort angeben.
Dumm nur: Es wurde das Passwort gelÃ¶scht welches ich eingegeben hatte. Ganz dumme Geschichte - damit wÃ¤re beim nÃ¤chsten hochfahren das System nicht mehr hochgekommen, weil kein EntschlÃ¼sselungs-SchlÃ¼ssel mehr bereit gewesen wÃ¤re; den initialen hatte ich gerade gelÃ¶scht 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 wÃ¤re - neues Device mit luks anlegen, dd if.. of ... von A nach B schieben).

Mein GlÃ¼ck ist, dass das Laufwerk ja noch online und damit geÃ¶ffnet ist. Auch der Master-Key ist (fÃ¼r root) auslesbar.

Zugschlus ist gerade auf der DebConf und hat Margarita ManterolagegenÃ¼ber 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
```

Posted by rince at 17:34

Zum VerstÃ¤ndnis:
Luks hat den master key ungecrypted und auslesbar im Speicher und ein tool um ihn auszulesen. Als Angreifer der irgendwie temporÃ¤r root bekommt reicht also ein kommando um offline die platte zu decrypten, wenn der Rechner ausgeschaltet wurde.
Anonymous on Aug 11 2015, 18:38

Brauchst Du Dir nicht merken, wirst Du nie wieder brauchen.
Anonymous on Aug 12 2015, 10:09

Das wird wohl nicht anders gehen wÃ¤hrend das Device aufgeschlossen ist.
Anonymous on Aug 12 2015, 10:10