Tuesday, October 10. 2017

VerschlÃ¼sselte Filesysteme unter Linux: Anlegen und vergrÃ¶ÃŸern

Dies ist primÃ¤r ein Eintrag fÃ¼r mich, damit ich nicht vergesse wie ich Dinge aufgesetzt habe

Ich habe ein Filesystem das verschlÃ¼sselt werden soll - es ist keine Systemplatte sondern Nutzdaten. Damit kann ich mir sparen, groÃŸe Verrenkungen machen zu mÃ¼ssen wegen Root- oder Bootpartition.
Also, einfach nur eine Festplatte, oder besser: ein Volume. Da ich potentiell mit RAID0 arbeiten mÃ¶chte (Stripes) oder Platten konkatenieren mÃ¶chte, bietet sich lvm mit LUKS zusammen an. lvm und LUKS kÃ¶nnen andere Leute viel besser erklÃ¤ren, 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 groÃŸ und heisst dann "Daten-crypt".

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

Hiermit erstelle ich eine verschlÃ¼sselte Partition auf dem Volumen Daten-Crypt. Ich gebe dann das Passwort ein das ich dafÃ¼r nutzen mÃ¶chte. 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 mÃ¶chte, geht das wie folgt:

Ich Ã¶ffne das verschlÃ¼sselte Filesystem und unmounte es, falls es gemounted ist.

Dann vergrÃ¶ÃŸere 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 verschlÃ¼sselte Volumen auch "ordentlich" vergrÃ¶ÃŸern:

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

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

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

Hiermit wird das Filesystem dann wirklich vergrÃ¶ÃŸert.

Ich mache danach Ã¼blicherweise 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 verschlÃ¼sseln ist, dass Dir dann jemand ganz einfach ein cryptsetup-Binary unterschieben kann, das die Passworteingabe mitlogged und das Passwort irgendwo hin schicken kann (oder sich bei der Gelegenheit einen zweiten Keyslot belegen kÃ¶nnte).

Und diese Problematik schlÃ¤gt dann bei VollverschlÃ¼sselung auf Kernel und Initrd durch, was direkt zu secure boot fÃ¼hrt, was dafÃ¼r sorgt, dass Du Deinem Hardwarehersteller trauen musst. Und dass die meisten staatlichen Angriffe Ã¼ber trojanisierte Firmware laufen werden, ist meine feste Meinung.

FÃ¼r 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 durchgefÃ¼hrt wird tut in Scripts weh.
Anonymous on Oct 11 2017, 08:23