Sichere Daten

Grundlagen

- Datenverschlüsselung zur persönlichen Sicherheit
- Laufwerksverwendung
  - bei Installation des Systems
  - stark im System eingebunden
- Containerverwendung
  - Nachträglich
  - Der Container kann besser gesichert und transportiert werde

Grundlagen

- Einzelne Datei/Dateien verschlüsseln
  - Mail oder USB Transport
- Jede Datensicherheit hängt vom Passwort ab, mind. 8 Zeichen (a-zA-Z0-9_-.)

Software

- Linux Betriebssystem
- Containerverschlüsselung
  - sudo apt-get install cryptsetup
  - mod_probe dm_crypt
- Dateiverschlüsselung
  - gpg
  - openssl

Beispiel - Datei

- Verschlüsseln
  - gpg -c DATEI
  - openssl enc -e -aes256 -in DATEI -out DATEI.enc
- Entschlüsseln
  - gpg -d DATEI.gpg > DATEI
  - openssl enc -d -aes256 -in DATEI.enc -out DATEI
- Verschlüsselungsmethoden
  - gpg –version
  - openssl -?

Beispiel – gpg Script

```
#!/bin/bash

datei=$1
kommando=$2

if [ -z $datei -o -z $kommando ]
then
	echo „$0 DATEI c|d“
	exit
fi

if [ „$kommando“ = „c“ ]
then
	gpg -c $datei
fi
if [ „$kommando“ = „d“ ]
then
	gpg -d $datei“.gpg“ > $datei
fi
```

Beispiel - Container

- Container anlegen
  - dd if=/dev/urandom of=/home/pi/geheim bs=1M count=250
- Container verschlüsseln
  - sudo cryptsetup -c aes-xts-plain -y -s 512 luksFormat /home/pi/geheim
- Container öffnen (Passwortabfrage)
  - sudo cryptsetup luksOpen /home/pi/geheim usb_crypt
- Container formatieren
  - mkfs.ext4 /dev/mapper/usb_crypt

Beispiel - Container

- Container einhängen
  - sudo mount -t ext4 -o rw,exec,user /dev/mapper/usb_crypt /home/pi/daten
- Container aushängen
  - sync && umount /home/pi/daten && cryptsetup luksClose /dev/mapper/usb_crypt

Beispiel - Container

- Container vergrößern
  - sudo cryptsetup luksOpen /home/pi/geheim usb_crypt
  - dd if=/dev/urandom bs=1M count=100 >> container_file
  - sudo cryptsetup resize /dev/mapper/usb_crypt
  - sudo resize2fs /dev/mapper/usb_crypt

Danke