Verschlüsselung von Partitionen unter Linux mit „Hausmitteln“

Beispiel: Die leere/neu zu formatierende Partition /dev/sdb1 soll mit AES verschlüsselt werden, d.h. alle Daten, die dort gespeichert werden, sollen automatisch verschlüsselt sein, und erst nach Eingaben eines Schüssels/Schlüsseldatei transparent (scheinbar unverschlüsselt) benutzt werden.

Verfahren: „Device-Mapper“: Bildet ein Blockdevice auf ein anderes ab, „dm-crypt“ / crypsetup: erzeugt einen „Verschlüsselungs-Tunnel“ zwischen der Anwendersoftware und der physikalischen Speicherung.

Anlegen:

```
/sbin/cryptsetup create --key-size 256 --cipher aes crypto /dev/sdb1
```

(Erzeugt eine virtuelle Partition „crypto“, die zur und von der echten Partition /dev/sdb1 verschlüsselt nach AES-Standard (ohne sichtbaren Header → plausible Abstreitbarkeit für Länder mit Crypto-Verbot). Das „create“ fragt nach einem Schlüssel, den man frei wählen kann und sich aber gut merken sollte!

Neu formatieren (Achtung: Datenverlust!):

```
mkfs.ext4 /dev/mapper/crypto
```

(Während auf der virtuellen Partition /dev/mapper/crypto ein ext4-Dateisystem erzeugt wird, landen auf /dev/sdb1 „zufällig aussehende“ Daten durch die AES-Verschlüsselung.)

```
mount /dev/mapper/crypto /mnt
```

Der verschlüsselte Inhalt der realen Partition `/dev/sdb1` wird unverschlüsselt unter `/mnt` eingeblendet.

Rückgängig (unverschlüsselte Daten ausblenden):

```
umount /mnt
```

```
/sbin/cryptsetup remove crypto
```

Wenn als Container beim „`cryptsetup create`“ per Option Luks angegeben wird, kann das Ver-/Entschlüsselungspasswort später geändert werden.