Bild: Timo Lenzen

Verschlüsseldienst

Daten verschlüsselter Linux-Installationen retten

Bei der Installation moderner Linux-Distributionen genügt meist ein Knopfdruck, um alle Dateisysteme mithilfe von LUKS zu verschlüsseln. Das schützt zwar die Privatsphäre beim Verlust des Laptops und verhindert Datendiebstähle bei Einbrüchen in Unternehmen. Schlimmstenfalls genügt ein gekipptes Bit, um Ihnen den Zugriff auf all Ihre Daten zu verwehren. Mit der richtigen Vorbereitung können Sie Ihre Daten dennoch zurückgewinnen.

Von Tim Schürmann und Mirko Dölle

Datenklau passiert nicht nur online. Der Diebstahl von Smartphones und Notebooks oder der Einbruch im Büro sind noch immer ein probates Mittel, um an wertvolle Daten von Unternehmen, Journalisten und Einzelpersonen zu gelangen. Durch vermehrte Heimarbeit im Zuge der Corona-Pandemie hat sich das Risiko für Unternehmen drastisch erhöht, Privatwohnungen sind selten wie ein Unternehmenssitz gesichert. Da hilft auch kein besonders sicheres Anmeldepasswort – ist das Speichermedium nicht verschlüsselt, kommt ein Angreifer mit physischem Zugriff auf einen Datenträger leicht an die Dateien heran.

Verschlüsselte Festplatten und SSDs sind vor solchen physischen Datendiebstählen gefeit. Die Einrichtung eines verschlüsselten Linux-Systems ist leicht. Fast alle aktuellen Distributionen bieten diese Möglichkeit bereits während der Installation, es kostet nur wenige Mausklicks. Das erhöht die Sicherheit zwar deutlich, schafft aber auch Schwachstellen: Wird der Schlüssel versehentlich gelöscht oder kippt etwa infolge eines Lesefehlers auch nur ein einzelnes Bit des Schlüssels, sind gleich sämtliche Daten verloren.

c't Hardcore

Unternehmenseinsatz

Auch organisatorisch will der Einsatz verschlüsselter Dateisysteme in Unternehmen gut überlegt sein: Das vorrangige Ziel ist ja, dass nur der jeweilige Mitarbeiter an die Daten herankommt – damit werden

aber auch die Admins ausgesperrt. Erkrankt der Mitarbeiter oder verlässt er das Unternehmen, ohne das Passwort zu verraten, bedeutet das für das Unternehmen einen vollständigen Datenverlust. Man könnte allenfalls auf die Backups zurückgreifen, sofern diese nicht ebenfalls verschlüsselt sind. Auch können sich nicht mehr ohne Weiteres mehrere Benutzer einen Rechner teilen, schließlich soll niemand sein Passwort weitergeben. Genau hier setzt das Konzept von LUKS (Linux Unified Key Setup) an.

Nachschlüssel

Bei LUKS handelt es sich nicht um ein Verschlüsselungsverfahren, sondern um eine Schlüsselverwaltung. Für die Ver- und Entschlüsselung der Daten ist der Device Mapper (DM) des Kernels zuständig, der auch mehrere physische Blockgeräte eines LVMs oder Software-RAIDs zu einem virtuellen Block Device zusammenfügt, das man dann mit Dateisystemen versehen kann. Weil die Daten zusätzlich verschlüsselt werden, spricht man oft von DM-Crypt.

Den symmetrischen Schlüssel, den sogenannten Master Key (MK), erhält der Device Mapper des Kernels von dem Programm `cryptsetup`. Das wird beim Booten eines verschlüsselten Linux-Systems automatisch aufgerufen und fragt nach dem Passwort. Das funktioniert auch ohne LUKS im sogenannten Plain-Modus, bedeutet aber, dass der Master Key direkt aus dem eingegebenen Passwort abgeleitet wird. Will man das Passwort ändern, ändert sich auch der Master Key und der gesamte Datenträger muss entschlüsselt und neu verschlüsselt werden. Das kann je nach Größe Stunden oder gar Tage dauern. Soll jemand anderes Zugriff auf den Datenträger erhalten, so muss man zwangsweise das Passwort weitergeben. Der Vorteil ist, dass ein solcher Datenträger keine besonders verwundbare Stelle besitzt – gibt es etwa einen Lesefehler, so sind nur die Daten des jeweiligen Blocks betroffen, der Rest bleibt les- und entschlüsselbar.

Mit LUKS zieht `cryptsetup` eine Zwischenebene ein: Der symmetrische Schlüssel für das Laufwerk wird zufällig generiert und anschließend mit dem eingegebenen Passwort des Anwenders und einem zusätzlichen Salt verschlüsselt. Diesen verschlüsselten Schlüssel speichert `cryptsetup` in einem von insgesamt acht Key Slots im LUKS-Header am Anfang des Laufwerks. Damit neben dem Mitarbeiter auch der Admin Zugriff auf den Rechner bekommt, genügt es, in einem zweiten Key Slot eine mit dem Admin-Passwort verschlüsselte Kopie des symmetrischen Schlüssels zu speichern. Auf die gleiche Weise können Sie noch sechs weiteren Personen Zugriff auf Ihre Daten gewähren:

```
sudo cryptsetup luksAddKey /dev/sda3
```

Dabei wird stets der nächste freie Key Slot benutzt. Der Gerätename /dev/sda3 ist Standard bei Debian- und Ubuntu-Installationen. Den korrekten Gerätenamen auf Ihrem System ermitteln Sie mit dem Befehl

```
sudo blkid -t TYPE=crypto_LUKS
```

Welche Slots bereits belegt sind und wie viele Passwörter es somit für Ihre Festplatte gibt, finden Sie mit folgendem Kommando heraus:

```
sudo cryptsetup luksDump /dev/sda3
```

Schlüsselfrage

Dabei wird Ihnen allerdings nicht angezeigt, welches Passwort zu welchem Key Slot gehört. Die Slot-Nummer eines Passworts erfahren Sie, indem Sie die Partition mit `cryptsetup open` von Hand entschlüsseln und zusätzlich den Parameter `-v` verwenden:

```
sudo cryptsetup -v \
open /dev/sda3 sda3_crypt
```

So können Sie alle berechtigten Passwörter ausprobieren und die Key Slots löschen, zu denen Ihnen kein Schlüssel bekannt ist:

```
sudo cryptsetup \
luksKillSlot /dev/sda3 1
```

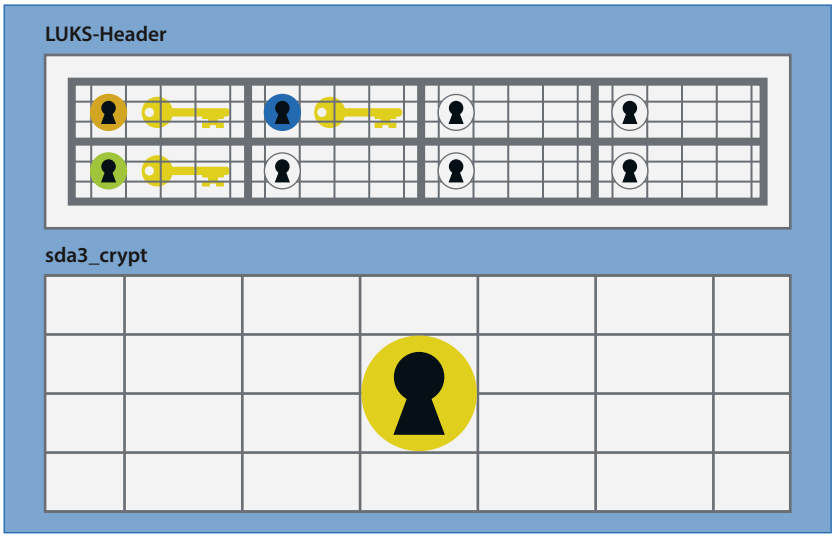
In diesem Fall wäre es Slot 1. Indem Sie anschließend ein neues Passwort einrichten, können Sie so vergessene Passwörter durch neue ersetzen. Wichtig ist nur, dass Sie den Datenträger zuvor mit einem der anderen Passwörter geöffnet haben. So schützt ein zweites, etwa in einem Tresor oder Keypass aufbewahrtes Passwort vor einem vollständigen Datenverlust bei Vergesslichkeit.

Geht es hingegen nur darum, ein Passwort zu ändern, so erledigen Sie dies folgendermaßen:

```
sudo cryptsetup \
luksChangeKey /dev/sda3
```

Schlüsseltresor

Beim Linux Unified Key Setup (LUKS) erhalten bis zu acht Personen einen eigenen Nachschlüssel, also eine Schlüsselkopie. Diese werden im LUKS-Header der Partition abgelegt und mit einem individuellen Passwort gesichert. Wird einer der acht Key Slots beschädigt, entschlüsseln die noch unversehrten Nachschlüssel weiterhin sämtliche Daten.



Dabei geben Sie einfach das zu ändernde und das neue Passwort ein – `cryptsetup` ermittelt den zugehörigen Key Slot automatisch. Auf nahezu gleiche Weise entfernt `cryptsetup luksRemoveKey` ein noch bekanntes Passwort, woraufhin es künftig nicht mehr funktioniert.

Sicher ist sicher

Da jeder Key Slot eine eigene verschlüsselte Kopie des Schlüssels enthält, sinkt mit jedem zusätzlichen Schlüssel die Anfälligkeit: Solange bei einem Defekt auch nur einer der Key Slots unversehrt bleibt, lässt sich das Medium weiter vollständig entschlüsseln. Sie sollten aber auf jeden Fall eine Kopie des Headers speichern und an einem sicheren Ort aufbewahren:

```
sudo cryptsetup \
luksHeaderBackup /dev/sda3 \
--header-backup-file luksheader.bin
```

Indem Sie den Header mittels `cryptsetup luksHeaderRestore` wieder zurückspielen, reparieren Sie etwaige Beschädigungen. Dabei werden jedoch alle Header-Informationen und sämtliche Key Slots überschrieben. Das hat Vor- und Nachteile: Hat ein Anwender sein Passwort zwischenzeitlich geändert, so ist dies nach dem Restore wieder auf den Stand des Backups zurückgesetzt. Wurden zusätzliche Schlüssel für weitere Benutzer eingerichtet, verlieren diese den Zugang. Außerdem könnte sich ein ehemaliger Mitarbeiter, dessen Schlüssel inzwischen entfernt wurde, mithilfe eines alten Backups wieder Zugang verschaffen.

Dafür hat ein Admin aber auch dann Zugriff auf den verschlüsselten Datenträger, wenn ein Benutzer den Admin-Key gelöscht oder etwa per `cryptsetup luksErase` den gesamten LUKS-Header überschrieben hat. Dieser Befehl ist auch das geeignete Mittel, um den LUKS-Header gezielt zu zerstören, etwa bevor man einen Datenträger ausbaut oder verschrottet. Ein Passwort wird für diese Operation nicht benötigt. Für Admins empfiehlt sich deshalb, den LUKS-Header kurz nach der Installation zu speichern. So haben Sie mithilfe eines Live-Linux vom USB-Stick jederzeit Zugang zum Datenträger und können mit dem Befehl

```
sudo cryptsetup \
luksHeaderRestore /dev/sda3 \
--header-backup-file luksheader.bin
```

zunächst den alten LUKS-Header mit dem bei der Installation vergebenen Admin-Passwort wiederherstellen und den Datenträger dann mit dem Befehl

```
sudo cryptsetup \
open /dev/sda3 sda3_crypt
```

entschlüsseln.

Falls in dem verschlüsselten Bereich wie bei Debian, Ubuntu und anderen Distributionen üblich ein LVM steckt und die dort enthaltenen Volumes nicht automatisch im Verzeichnis /dev/mapper auftauchen, aktivieren Sie es mit den Befehlen `sudo vgscan` und `sudo vgchange -ay`. Die Volumes aus /dev/mapper können Sie dann wie gewohnt mittels `mount` einbinden, aber auch Datenrettung etwa mittels `photorec` oder `foremost` betreiben, falls Datenträger oder Dateisystem beschädigt sind. Da die Verschlüsselung blockweise arbeitet, sind nur Datenblöcke verloren, die in einem beschädigten Bereich liegen.

Sind Datenträger und Dateisystem in Ordnung, können Sie ein verschlüsseltes Laufwerk ohne Handarbeit öffnen, indem Sie etwa ein Ubuntu 20.04 LTS booten: Dann genügt ein Klick im Dateimanager Nautilus auf das Laufwerk und schon fragt Ubuntu nach dem Passwort. Anschließend wird das LVM aktiviert und Sie können das entschlüsselte Laufwerk mit einem weiteren Klick einbinden.

Umbenannt

Bei Datenträgern, die wie bei Debian oder Ubuntu üblich ein verschlüsseltes LVM enthalten, gibt es noch einen weiteren Stolperstein: Ubuntu etwa nennt die Volume Group für das Root-Dateisystem und Swap standardmäßig `vgubuntu`. Schließt man zur Datenrettung die verschlüsselte Festplatte eines Ubuntu-Rechners an einen anderen an, auf dem ebenfalls Ubuntu verschlüsselt installiert ist, kann die Volume Group aufgrund der Namensgleichheit nicht aktiviert werden – die Logical Volumes bekämen dieselben Namen wie die des laufenden Ubuntus.

Deshalb müssen Sie die Volume Group umbenennen und, damit es nicht zu Verwechslungen kommt, die UUID der Volume Group angeben. Diese ermitteln Sie mit dem Befehl `sudo vgdisplay`. Zum Umbenennen verwenden Sie `vgrename`, im folgenden Beispiel ist die UUID verkürzt:

```
sudo vgrename mBZq-...-uA4 vgextern
```

Den neuen Namen der Volume Group können Sie sich frei aussuchen – es darf ihn nur noch nicht im System geben. Anschließend können Sie die Volumes des anderen Rechners bequem über den Dateimanager mounten. Vergessen Sie aber nicht, den Namen wieder zurückzuändern, bevor Sie die Festplatte wieder in den anderen Rechner einbauen.

Fazit

Mit der richtigen Vorsorge sind verschlüsselte Linux-Systeme ein probates Mittel, um Datenklau vorzubeugen, ohne die Sicherheit der Daten zu gefährden. Dabei kommt LUKS besonders Unternehmen und Familien entgegen, wo Rechner von mehreren Anwendern benutzt werden oder wo es inakzeptabel wäre, dass nur eine einzelne Person Zugang zu wichtigen Firmendaten hat. *(mid@ct.de)* c't

Mehrfach verkapselt

Bei verschlüsselten Debian- und Ubuntu-Installationen stecken das Root-Dateisystem sowie Swap einer Matrjoschka ähnlich in einem LVM, das innerhalb der verschlüsselten LUKS-Partition liegt.