Verschlüsseltes Cloud-Backup mit Linux Bordmitteln

Bernd Strößenreuther
clt@stroessenreuther.info

Photo by Jonathan Strößenreuther

Chemnitzer Linux-Tage
11. und 12. März 2023

Lizenz

Disclaimer

- Für Eure Daten, deren Sicherung und Wiederherstellbarkeit seid ausschließlich Ihr selbst verantwortlich.
- Alle Inhalte und Scripts wurden nach bestem Wissen und Gewissen erstellt – sind allerdings ggf. trotzdem nicht frei von Fehlern, die im schlimmsten Fall zu Datenverlust führen können: Dafür übernehme ich keine Haftung.
- Sie können maximal als Anregung dienen, Eure eigene Backup-Strategie zu erstellen und umzusetzen.

Agenda

(1) Brauche ich im privaten Umfeld ein Backup?

(2) Bedrohungen für meine Daten

(3) Welche Daten sollte ich sichern?

(4) Eine sinnvolle Backup-Strategie für zu Hause

(5) Spezielle Herausforderungen bei Cloud-Storage

- Verschlüsselung gewünscht?
- Begrenzte Upstream-Bandbreite bei heimischen Internet-Anschluss

(6) Fragen / Diskussion

Brauche ich ein Backup?

- Jede / jeder von uns erzeugt täglich eigene Daten
  Fotos / Videos (z. B. Urlaubserinnerungen), Texte, Musik, (schriftliche) Kommunikation, etc.
- Wie wichtig sind mir diese Daten?
  Wäre es schlimm, wenn ich plötzlich (ganz oder teilweise) nicht mehr darauf zugreifen könnte?

Photo by Usman Yousaf on Unsplash

RAID ist kein Backup!

- RAID schützt genau gegen eine Bedrohung: Ausfall einer Festplatte / SSD
- Und das im Zweifelsfall auch nur, wenn ich ein sauberes Monitoring meines RAID habe
- Vorteil: Keine zeitliche Lücke

Bedrohungen für meine Daten

- Versehentliches Löschen / versehentliches Überschreiben mit anderen Inhalten
- Das Gerät, auf dem sie gespeichert sind, geht unwiederbringlich kaputt
- Ein Zimmerbrand vernichtet auf einmal alle meine persönlichen Endgeräte
- Der Provider, bei dem ich alle meine Urlaubsfotos gespeichert habe, geht in Konkurs und die Server werden (sehr kurzfristig) abgeschaltet
- Ein Ransomware-Trojaner auf meinem Rechner verschlüsselt alle Daten, auf die er zugreifen kann und verlangt Lösegeld

Welche Daten sollte ich sichern?

- Einfache Antwort:
  Alles, was Dir wichtig ist!

Ja, aber jetzt konkret…

(aka: Worüber sollte ich zumindest mal nachgedacht haben?)

- Auf einem Linux-Rechner
  - /home
  - /root
  - /etc
  - /usr/local
  - /srv
- Wo nicht direkt Dateien im Filesystem abgelegt werden
  - SQL Dump von Datenbanken
  - Export vom Adressbuch (z. B. vCard)
  - Export des Kalenders (z. B. iCalendar)
  - etc.
- Will ich mir eine lokale Kopie von meinen Daten im Internet machen?
  - Fotos / Videos beim Cloud-Provider
  - Homepage / Blog / etc. beim Hosting-Provider
  - etc.
- Und falls ja: Will ich die dann nochmal mit sichern?

Eine sinnvolle Backup-Strategie

- Auch im privaten Umfeld gilt:
  Eine einzige Kopie meiner Daten schützt nicht vor allen o. g. Bedrohungen

Photo by John on commons.wikimedia.org

3-2-1-1: Deine Glückszahlen

- Man sollte mindestens 3 Kopien seiner wichtigen Daten haben (Backup Generationen)
- Diese befinden sich auf mindestens 2 verschiedenen Datenträgern (separate Hardware!!)
- Zu jedem beliebigen Zeitpunkt ist mindestens 1 davon offline (d. h. nicht mit einem Rechner verbunden)
- Mindestens 1 davon an einem anderen Ort

Ein Beispiel für zu Hause

Photo by Raimond Spekking on commons.wikimedia.org

- Man nutzt 2 USB-Festplatten
  (niemals beide gleichzeitig mit einem Rechner verbinden)
- Auf jeder davon mehrere Unterverzeichnisse mit je einer Backup-Generation
- Zusätzlich eine (verschlüsselte) Kopie über’s Internet auf Storage an einem anderen Ort
  - Gemieteter Storage bei einem (Cloud-)Provider
  - RasPi mit USB-Drive bei einem Freund, den Eltern, etc.

Woche 1 – USB-Platte Nr. 1 anschließen:

```
rsync -avP /home /run/media/backup-1/2023-03-13
```

(genauso mit /etc und weiteren Verzeichnissen)

Woche 2 – USB-Platte Nr. 2 anschließen:

```
rsync -avP /home /run/media/backup-2/2023-03-20
```

Woche 3 – USB-Platte Nr. 1 anschließen:

```
rsync --link-dest=/run/media/backup-1/2023-03-13/ \
-avP /home /run/media/backup-1/2023-03-27
```

Woche 4 – USB-Platte Nr. 2 anschließen:

```
rsync --link-dest=/run/media/backup-2/2023-03-20/ \
-avP /home /run/media/backup-2/2023-04-03
```

Spezielle Herausforderungen bei Cloud-Storage

- Will ich meinem Provider Zugriff auf alle meine privaten Daten ermöglichen?
  → Falls nein, muss ich dafür sorgen, dass sie nur verschlüsselt dort hin gelangen und nur ich den Schlüssel zur Entschlüsselung besitze
- Begrenzte Bandbreite des privaten Internet-Anschlusses:
  - 100 GB oder auch 1 TB Daten zu haben, ist auch für Privatpersonen heute nicht außergewöhnlich
  - Die Upstream-Bandbreite von Internet-Anschlüssen in Privathaushalten ist meist recht begrenzt (oft 10 Mbit/s oder weniger)
  - Jedes Mal alle Daten zum Provider zu übertragen würde jeweils mehrere Tage dauern

Überlegungen zur Umsetzung

- Vorteil im privaten Umfeld: Meist geringe Änderungrate
- Rsync hilft Internet-Bandbreite sparen, da nur die geänderten Daten übertragen werden
- Bei der Verschlüsselung: Wir müssen ein Filesystem wählen, das diesen Vorteil nicht zunichte macht
- Auch Dateinamen enthalten oft sensible Informationen und müssen daher verschlüsselt werden
- Keine besonderen Anforderungen an den Provider: Ich will möglichst überall Storage beziehen können

Beispiel-Script

https://github.com/booboo-at-gluga-de/offsite_backup

- Vorbereitung: Mit gocrpytfs wird lokal (auf dem zu sichernden System) ein verschlüsseltes Filesystem erzeugt
- Ablauf bei jedem Backup:
  - Lokal: mount des gocryptfs Filesystems
  - rsync synchronisiert die Daten in das Filesystem
  - umount des gocryptfs Filesystems
  - rsync synchronisiert die verschlüsselten Daten über das Internet zum Zielsystem

Demo

Recovery testen!

- Separat testen für lokale Backup-Medien und Cloud-Backup
- Recovery-Zeiten beachten
- Was nicht getestet ist, wird im Zweifelsfall nicht funktionieren!
- Backup ohne Recovery-Test ist nicht nennenswert besser als gar kein Backup

Kein Backup? Kein Mitleid!

(Alter Informatiker-Spruch)

Backup Reminder

Bei den o. g. Backup-Verfahren sind manuelle Schritte erforderlich und
Teil des Konzepts:

- USB-Disk anstecken
- Passwort-Eingabe beim Mount des verschlüsselten Filesystems

Lasst Euch regelmäßig erinnern!

- Serientermin im Kalender
- Reminder am Handy
- Cronjob der eine Mail schickt
- Alert in Eurem Monitoring-System
- etc.

Fragen / Diskussion

Icon from freesvg.org / Public Domain

Schaut gerne mal bei uns vorbei...

Live vor Ort in Nürnberg oder Remote

Linux-Cafe

(1x pro Monat an einem Mittwoch, immer hybrid,
wechselnde Vortrags- bzw. Workshop-Themen)

https://termine.gluga.de/

Linux-Treff Nord

(donnerstags, 2x im Monat vor Ort,
2x im Monat als Videokonferenz)

https://lug-noris.de/