Warum dein Backup nicht vor Ransomware schützt

Ein paar Dinge, die man vielleicht im Hinblick auf Ransomware berücksichtigen möchte.

Wer bin ich?

Andreas Rogge

- Hauptberuflich Bareos-Entwickler
- Viel Linux- und Netzwerk-Consulting
- Linux seit 1995, aber man lernt stets noch etwas Neues dazu

Rücksicherung nach Ransomware

- Jede aktuelle Systemsicherung ist wahrscheinlich bereits kompromittiert
- Systeme neu aufbauen, Datenbestand wiederherstellen
- Erfordert hinreichend aktuelle und wiederherstellbare Datensicherung

Problem-Szenarien

- Sicherungen
  - wurden gelöscht
  - wurden gar nicht erst gemacht
  - sind nicht (mehr) wiederherstellbar
  - enthalten nur Unsinn
  - lagen auf einem „geransomten“ Server

Hausaufgaben

- MFA für Admin-Zugang am Backup-Server
  - und niemand sonst kann ein Backup löschen
- Backupmedien unveränderbar machen
- Restore-Tests auf „saubere“ Systeme machen
- Intervall Restore-Test << Backup-Vorhaltezeit