Chaos Seminar: Mein Backup Konzept

Nobody cares about backup - all just care about restore

Marcus
h+chaosseminarbackup@crystaldown.de

Chaos Computer Club Ulm

2017-07-10

Technikerzusammenfassung

Backup

- raid1 (mirror) mit 5 HDDs (mdadm)
- scp/rsync/rdiff-backup

```
rsync -vaHux --include inc.list --exclude exc.list
```

- 3 offsites
- Debian, Devuan, OSX, SailfishOS
- OS kein Backup, Exclude-List und Include-List

Sicherheit

- cryptsetup

Welche Geräte?

- Laptop Linux
- Händi Linux
- Laptop OSx
- TowerPC Linux
- nicht Android-Händi (Simons Cloud)

Welche Daten?

- /home
- keine Filme
- ausgewählte große Binärdateien (Leaks)
- kein OS (Reinstall automatisiert, Restore Ubuntu 3h)

Luxusprobleme

Wenn wir uns darüber streiten, können wir ein Bier trinken und den Abend hinter uns lassen

- rdiff vs rsnapshot vs duplicity vs borg
- Seagate vs Western Digital vs Toshiba vs HGST (`https://github.com/tdotu/smart`)
- aes-xts vs aes-cbc vs gpg

Einleitung

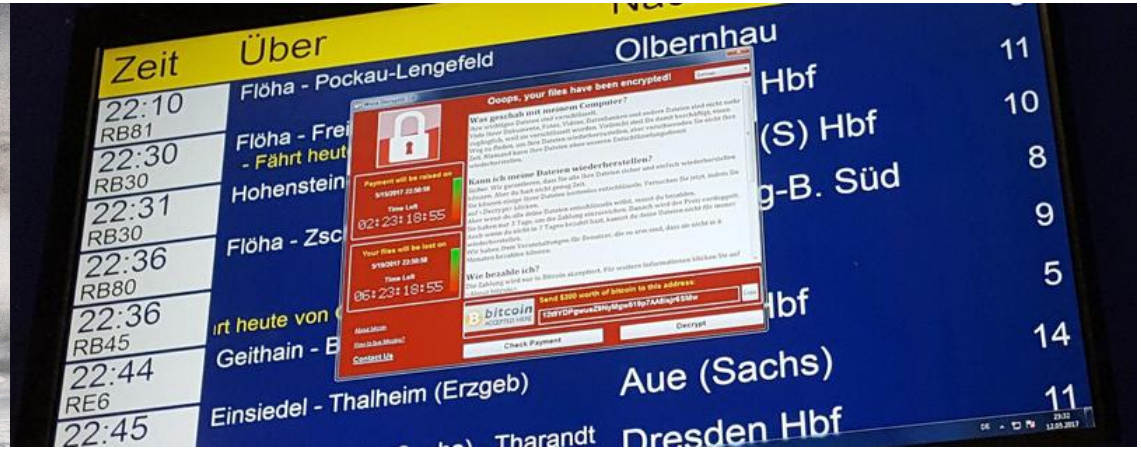
- **Publikumsaufgabe: Prototyp v1. Denkfehler suchen, kritische Fragen stellen**
- mein erster Restore: Tcom Spielelaptop Bild r1e
- lernen mit Schmerzen
- ausgewählte Leute

Backupgeschichten

- Kannst du mal meine Urlaubsbilder ...?
- LUGU Backup wegautomatisiert
- Restore dauert zu lange Kraft
- Wannacry (GB NHS, DB Bild DB)
- Ich hatte deine Händinummer nicht mehr.

Anforderungen - Bedrohungsszenarien

Bilder groß



Iteration 1: Backup Anfangen

- Festplattenverschlüsselung
- kopieren
- Dokumentensicherung: Fotografieren

Iteration 2: Schutzmaßnahmen

- Feuer
- Diebstahl (Laptop, Händi, Flughafenkontrolle)
- Polizeieinbruch
- Grundremmingen
- Cryptotrojaner

Hypotetisch

- verzögernder Cryptotrojaner
- Hardwaremanipulationserkennung (tripwire)

`00_do_not_touch_or_device_will_emergency_shutdown.docx`

(inotify)

Backupmedien

- HDD
- Magnetband
- Cloud
- optischer Datenträger
- Papierdruck

Iteration 3: Kosten

- Marketingbullshit Cloud - minimaler Preis undrückbar
- backblaze.com (2/15 StoragePod, 3/20 Pods/Vault) Bild
  - 5 $/Mon all-you-can-upload
  - 5 $/Mon/TByte rsync
- HDD
  - 60 Euro/2 TByte HDD, HDD 3 Jahre
  - $\frac{60 Euro}{2 TByte \cdot 3 Jahre \cdot 12 \frac{Monate}{Jahr}}$
  - $0,85 \frac{Euro}{Monat \cdot TByte}$
- Magnetband Generation 4 (Laufwerk 180 Euro/Stück)
- Magnetband Generation 5 (Laufwerk 450 Euro/Stück)
- Magnetband Generation 6 (Laufwerk 1800 Euro/Stück)
- Blue Ray
  - $\frac{16 Euro}{25 Stueck \cdot 25 \frac{GByte}{Stueck}} = \frac{16 Euro}{625 GByte} = 26 \frac{Euro}{TByte}$
  - Lebensdauer
  - Lagerverwaltung
  - inkrementelle Backups

Zusammenfassung

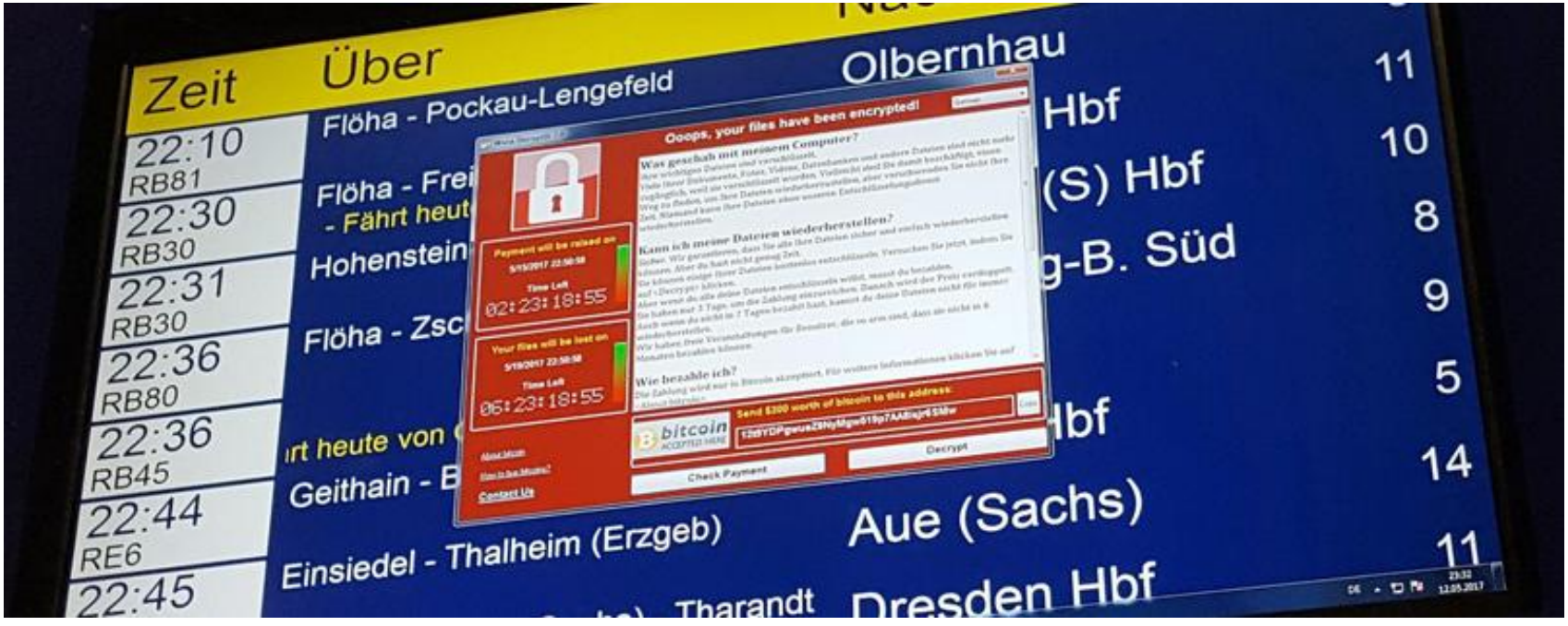
- Offsite
- offline Medien (verzögertes Backup)
- Restore testen
- Backup pullen (Cryptotrojaner)
- Backup verifizieren

Diskussion

- SSD durchschreiben: Firefox, gparted, cbc, Nagios Tcom
- Backblaze: Seagate 50% Preis, 150% Ausfall
- wear levelling vs cbc vs xts
- Bankschließfach
- hdparm vs raid vs Lautstärke
- rdbmfs
- Redundanz: mdadm vs lvm vs snap-raid vs git vs rsync
- SATA 50 Steckvorgänge
- Versionierung: nicht Cryptotrojaner, versehendliches Löschen, versehentliches Ändern

Asus R1e

Erpressungstrojaner Wannacry Deutsche Bahn



Mondelez - Milka - Kraft - Jacobs

CC-SA-AT Alex Arkink, derivative work: Rôtkæppchen68

Anforderung Diebstahl

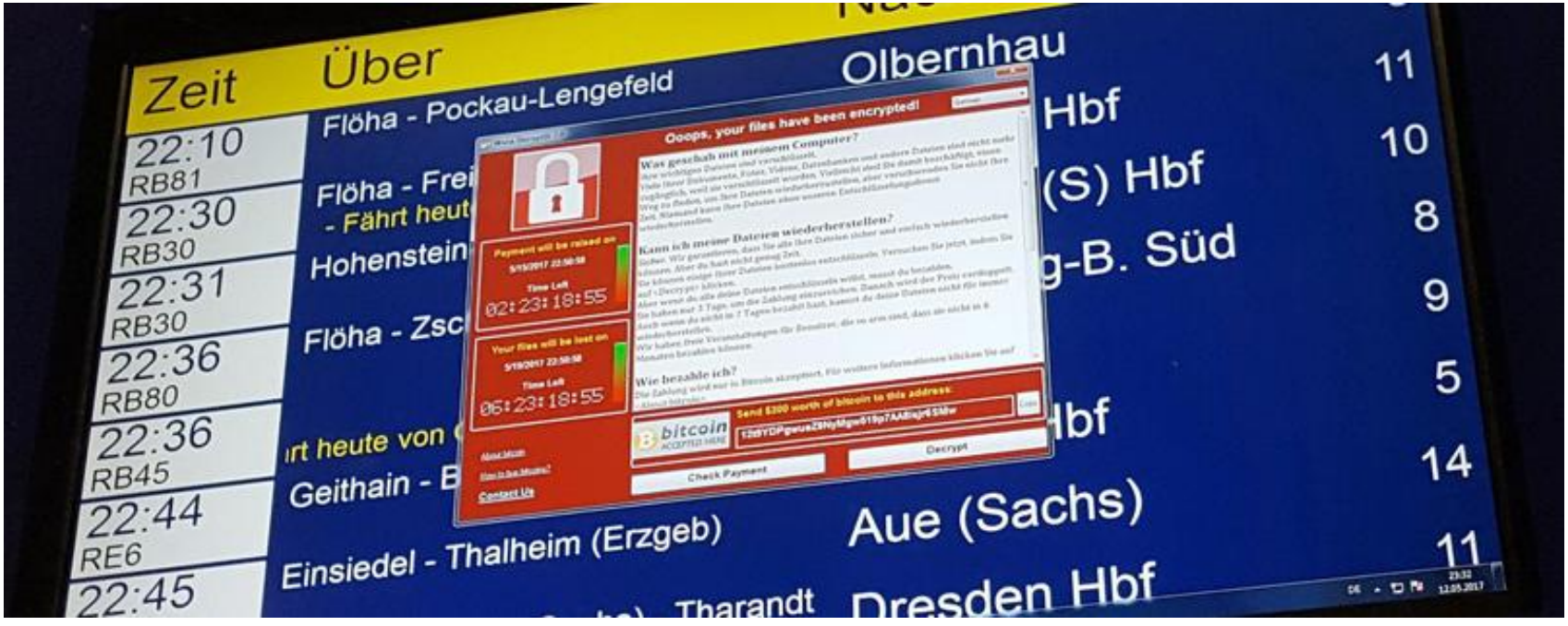
zurück

Anforderung Assetvernichtung

zurück

Anforderung Crpytotrojaner

zurück



backblaze storage pod

zurück