

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



Zeit	Über	Olbernhau	
22:10	Flöha - Pockau-Lengefeld	Hbf	11
RB81			
22:30	Flöha - Fre...	(S) Hbf	10
RB30	- Fahrt heut		
22:31	Hohenstein	g-B. Süd	8
RB30			
22:36	Flöha - Zsc		9
RB80			
22:36	irt heute von	Hbf	5
RB45	Geithain - B		
22:44		Aue (Sachs)	14
REG	Einsiedel - Thalheim (Erzgeb)		
22:45		Dresden Hbf	11

Oberrhein

Check your link here before connecting

Bitte beachten Sie, dass die Verbindung zu den Servern nicht hergestellt werden konnte. Bitte überprüfen Sie Ihre Internetverbindung.

Bitte beachten Sie, dass die Verbindung zu den Servern nicht hergestellt werden konnte. Bitte überprüfen Sie Ihre Internetverbindung.

Bitte beachten Sie, dass die Verbindung zu den Servern nicht hergestellt werden konnte. Bitte überprüfen Sie Ihre Internetverbindung.

Iteration 1: Backup Anfängen

- ▶ Festplattenverschlüsselung
- ▶ kopieren
- ▶ Dokumentensicherung: Fotografieren

Iteration 2: Schutzmaßnahmen

- ▶ Feuer
- ▶ Diebstahl (Laptop, Händi, Flughafenkontrolle)
- ▶ Polizeieinbruch
- ▶ Grundremmungen
- ▶ 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
 - ▶ $\frac{60 \text{ Euro}}{2 \text{ TByte} \cdot 3 \text{ Jahre} \cdot 12 \frac{\text{Monate}}{\text{Jahr}}}$
 - ▶ $0,85 \frac{\text{Euro}}{\text{Monat} \cdot \text{TByte}}$
- ▶ Magnetband Generation 4 (Laufwerk 180 Euro/Stück)
- ▶ Magnetband Generation 5 (Laufwerk 450 Euro/Stück)
- ▶ Magnetband Generation 6 (Laufwerk 1800 Euro/Stück)
- ▶ Blue Ray
 - ▶ $\frac{16 \text{ Euro}}{25 \text{ Stueck} \cdot 25 \frac{\text{GByte}}{\text{Stueck}}} = \frac{16 \text{ Euro}}{625 \text{ GByte}} = 26 \frac{\text{Euro}}{\text{TByte}}$
 - ▶ 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, versehentliches Löschen, versehentliches Ändern

Asus R1e



Erpressungstrojaner Wannacry Deutsche Bahn

The image shows a train departure board with a ransomware notification overlaid. The board lists train times and destinations. The ransomware window is titled "Oops, your files have been encrypted!" and contains the following text:

Oops, your files have been encrypted!

Was geschieht mit meinem Computer?
Alle Ihre Dateien sind verschlüsselt. Die Dateien sind nicht mehr nutzbar. Sie können sie wiederherstellen, aber Sie müssen zuerst Bitcoin bezahlen. Wenn Sie nicht bezahlen, werden Ihre Dateien zerstört. Sie werden sie nie wieder sehen können. Sie können Ihre Dateien wiederherstellen, aber Sie müssen zuerst Bitcoin bezahlen. Wenn Sie nicht bezahlen, werden Ihre Dateien zerstört. Sie werden sie nie wieder sehen können.

Kann ich meine Dateien wiederherstellen?
Ja, aber Sie müssen zuerst Bitcoin bezahlen. Wenn Sie nicht bezahlen, werden Ihre Dateien zerstört. Sie werden sie nie wieder sehen können.

Wie bezahle ich?
Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf den Bitcoin-Link.

Send 0.5 BTC worth of bitcoin to this address: [13870P...](https://www.bitcoin.com/address/13870P...)

Bitcoin

Check Payment Decrypt

The board lists the following train times and destinations:

Zeit	Über	Olbernhau
22:10 RB81	Flöha - Pockau-Lengefeld	Hbf
22:30 RB30	Flöha - Freital - Fahrt heute	(S) Hbf
22:31 RB30	Hohenstein	g-B. Süd
22:36 RB80	Flöha - Zsch...	
22:36 RB45	irt heute von	Hbf
22:44 RE6	Geithain - B...	14
22:45	Einsiedel - Thalheim (Erzgeb)	Aue (Sachs)
	Tharandt	Dresden Hbf

Mondelez - Milka - Kraft - Jacobs

CC-SA-AT Alex Arkink, derivative work: Røtkæppchen68



Anforderung Diebstahl [zurück](#)



Anforderung Assetvernichtung

[zurück](#)



Anforderung Crpytotrojaner zurück

Zeit Über

Zeit	Über
22:10 RB81	Floha - Pockau-Lengefeld
22:30 RB30	Floha - Fre... - Fahrt heut...
22:31 RB30	Hohenstein
22:36 RB80	Floha - Zsc...
22:36 RB45	irt heute von
22:44 RE6	Geithain - B...
22:45	Einsiedel - Thalheim (Erzgeb)

Olbernhau

Destination	Time
Hbf	11
(S) Hbf	10
g-B. Süd	8
	9
	5
Hbf	14
Aue (Sachs)	11
Tharandt	
Dresden Hbf	

Coop, your files have been encrypted!

Was geschieht mit meinem Computer?
Ihre Dateien sind verschlüsselt. Die Dateien sind verschlüsselt und können nicht mehr geöffnet werden. Um Ihre Dateien wiederherzustellen, müssen Sie eine Zahlung von 0,01 Bitcoin leisten. Wenn Sie die Zahlung nicht leisten, werden Ihre Dateien dauerhaft gelöscht.

Kann ich meine Dateien wiederherstellen?
Ja, wenn Sie die Zahlung leisten. Die Dateien werden innerhalb von 24 Stunden wiederhergestellt. Wenn Sie die Zahlung nicht leisten, werden Ihre Dateien dauerhaft gelöscht.

Wie bezahle ich?
Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf den Bitcoin-Link.

Send 0,01 worth of bitcoin to this address:
13870P...
[Bitcoin QR code]

Check Payment Decrypt

11.05.2017

Backblaze Storage Pod 6.0

60 Drive 480TB Storage Server

[Shop Now](#)

