

Hier finden sich meine Notizen zur Vorbereitung eines Workshops zum Thema Datensicherung/Datensicherheit. Ergänzungen und Hinweise bitte hier im Wiki oder direkt an mich [RalphGL](#)

---

# Die Gefahr des Datenverlusts und Vorkehrungen zum Schutz

## Ein paar Überlegungen zur Gefahr des Datenverlusts.

### Welche Gefahren und Risiken drohen?

- Hardwarefehler z.B. Ausfall einer Festplatte oder eines Controllers
- Benutzerfehler (versehentliches Löschen von Daten und Sabotage)
- Softwarefehler (bzw. Schadsoftware, Cracker etc.)
- höhere Gewalt (Brand, Wasser, Blitzschlag)
- Diebstahl (Einbruch)

### Welche Maßnahmen taugen gegen welche Gefahren, gegen welche nicht?

Mit unendlichem Aufwand lässt sich JEDES Risiko minimieren. Kein Aufwand bedeutet MAXIMALES Risiko. In jedem Einzelfall gilt es eine Abwägung zu treffen und das **Optimum zwischen Risiko und Sicherheit** unter **Berücksichtigung der entstehenden Kosten (des Aufwandes)** zu beurteilen.

#### manuelle Sicherung durch Benutzer

Ergebnis: leider völlig unbrauchbar, wird erfahrungsgemäß nicht dauerhaft regelmäßig durchgeführt, oft unvollständig und zu zeitaufwändig;

#### automatische Sicherung durch Bandlaufwerk:

Bedingt geeignet, allerdings müssen Prüfverfahren für die Sicherungsmedien implementiert werden. Es besteht die Gefahr dass die Datensicherung im Bedarfsfall nicht brauchbar ist. Schützt nicht vor höherer Gewalt, wenn die Bänder im Gerät verbleiben. Mehrere Versionsstände nur umständlich verwaltbar.

#### Absicherung gegen höhere Gewalt:

Ist eingeschränkt möglich durch Wahl eines guten Standortes - z.B. erhöht um vor Wasserschaden zu schützen, durch technische Vorkehrung, z.B. durch Überspannungsschutz der Stromzufuhr etc.

## Welche Kriterien sollten vor der Wahl der optimalen Maßnahmen geprüft werden?

- Welche Kosten würden sich aus einem Totalverlust aller Daten ergeben?
- Welche Daten müssen gesichert werden, welche sollten gesichert werden, auf welche kann verzichtet werden?
- Wo befinden sich die Daten, auf welchen Computern und Festplatten?
- Welchen Schaden würde ein Verlust der geänderten Daten der letzten 3 Tage, letzten 8 Tage, letzten 14 Tage, letzten 4 Wochen ergeben? Außer der Angabe in € ist auch die Einteilung in folgende Kategorien möglich: (A) existentiell bedrohend, (B) unvereinbar mit einem positiven Betriebsergebnis, (C) Gewinnmindernd, (D) vertretbare Kosten, (E) unerhebliche Kosten;
  - Verlust der Daten der letzten 3 Tage
  - Verlust der Daten der letzten 8 Tage
  - Verlust der Daten der letzten 14 Tage
  - Verlust der Daten der letzten 4 Wochen
- Wie wichtig ist es, dass ein unterbrechungsfreier Betrieb gewährleistet ist?
- Sind mehrere Versionsstände wünschenswert?

## Mögliche Anforderungen an die Datensicherung:

Ein mögliches Anforderungsprofil könnte sein:

- Bei Totalverlust entstehen Kosten die mit einem einem positiven Betriebsergebnis unvereinbar sind, evtl. sogar ein existentiell bedrohliches Ausmaß annehmen.
- Zu sichernde Daten:

MUSS Inhouse-Server „A“ /home /data

MUSS Windows-Arbeitsplatz „A“ Benutzerverzeichnis

MUSS Internet-Server „B“ /var/www /etc

MUSS Inhouse-Server Komplettsystem

SOLL Windows-Arbeitsplatz „C“ komplett,

SOLL Internet-Server „B“ Komplettsystem

NICHT: Windows-Arbeitsplatz „C“

NICHT: Inhouse-Server „A“ /tmp /var/log

NICHT: Internet-Server „B“ /tmp /var/log

- Dimension der Schäden:
  - Verlust der letzten 3 Tage: „unerhebliche Kosten“
  - Verlust der letzten 8 Tage: „vertretbare Kosten“
  - Verlust der letzten 14 Tage: „vertretbare Kosten“
  - Verlust der letzten 4 Wochen: „Gewinnmindernd“

- Auf einen unterbrechungsfreien Betrieb im Störfall kann verzichtet werden.
- Mehrere Versionsstände sind gewünscht.
- Möglichst vollautomatische Sicherung ohne Benutzerinteraktion
- Einfache Verifizierung der Sicherung
- Einfache komplette oder partielle Wiederherstellung
- Nur bedingte Sabotagesicherheit
- Totalverlust der letzten 14 Tage stellt „nur“ eine nichtexistenzielle Bedrohung dar
- kompletter Totalverlust ist existentiell bedrohend
- Mehrere ältere Versionen sollen wiederherstellbar sein.

## Das Konzept von rsnapshot

rsnapshot ist eine Sammlung von perl-Skripts, welche Unix-Standardmechanismen (wie z.B. hardlinks) nutzt um eine frei konfigurierbare automatisierte Sicherung von Daten vorzunehmen.

- 1:1 Kopie aller Dateien genau ein mal
- Automatisches setzen von hardlinks

## Die Installation



## Die Konfiguration



## Ist ein Backup der Datensicherung sinnvoll

Durch eine Sicherung der Daten mittels rsnapshot auf eine dedizierte Festplatte im Server können die meisten Anforderungen gut erfüllt werden.

- Nicht erfüllt sind die Anforderungen die sich stellen, wenn ein Schutz vor höherer Gewalt erfolgen soll.
- Nur bedingt erfüllbar sind die Anforderungen vor einem Schutz vor Sabotage und Softwarefehlern.

Um diese beiden Kriterien besser zu erfüllen wird eine zweite Form der Datensicherung eingeführt, das Backup des Backups auf eine externe Festplatte, welche im Normalbetrieb NICHT am System angeschlossen ist.



## Ausblicke

- Datensicherung von Windows-Arbeitsplätzen mit rsnapshot 
- Datensicherung von Apple OS X-Arbeitsplätzen mit rsnapshot 

From:  
<http://lusc.de/dokuwiki/> - **LUSC - Linux User Schwabach**

Permanent link:  
[http://lusc.de/dokuwiki/users/vorbereitung\\_workshop\\_datensicherheit\\_und\\_datensicherung?rev=1208508977](http://lusc.de/dokuwiki/users/vorbereitung_workshop_datensicherheit_und_datensicherung?rev=1208508977) 

Last update: **2008/08/11 15:11**