

# Sicherheit in der IT-Infrastruktur

Beispiele aus der Praxis, Ausfallsicherheit, Backups,  
Verschlüsselung

---

Timo Schindler

14.03.2019

OTH Regensburg

1. Einführung: Backup
2. Backupinfrastruktur in der Praxis
3. Grundlagen: Verschlüsselung und Signierung
4. Verschlüsselung und Signierung in der Praxis
5. Zusammenfassung

# Einführung: Backup

---

**Timo Schindler**  
OTH Regensburg

- Promotion: IT Security & Machine Learning
- Server- und Storage-Systeme
- Virtualisierungs-Infrastruktur
- Sysadmin mit Leidenschaft

# Zentralisierung als Lösung?

- In Zeiten von Cloud: Services wandern in die Rechenzentren
- Zentraler Zugriff für alle Benutzer
- Zentraler Schwachpunkt
- Vertrauen in Administratoren
- Sicherheit an Zentraler Stelle wichtiger den je!



---

Bild: <https://fsfe.org/activities/nocloud>

# Warum Backup?

Gründe für Backups sehr divers. Datenverlust durch:

- Versehentliches Löschen
- Unberechtigte Veränderung durch Dritte
- Technischer Systemausfall
- Diebstahl, Sabotage, Betrug
- Katastrophen (Brand, Wasserschaden)
- Angriffe (z.B. Ransomware)

Backupmechanismen und -maßnahmen unterscheiden sich dadurch erheblich.

# Schutzziele der Informationssicherheit

## Allgemeine Schutzziele

### Vertraulichkeit

Lesen nur durch autorisierte Benutzer

### Integrität

Keine unbemerkte Veränderung

### Verfügbarkeit

Verhinderung von Systemausfällen

## Weiter Schutzziele

### Authentizität

Echtheit bzw. Überprüfbarkeit eines Objektes

### Verbindlichkeit

Kein unzulässiges Abstreiten von Aktionen

### Zurechenbarkeit

Zuordnung einer Aktion auf Benutzer

Schutzziele können nur durch Zusammenspiel aus Hard- und Software erreicht werden.

## Tier 1 - Die Holzklasse

- Keine Redundanz
- Jährliche Ausfallzeit 28,8 Stunden
- 99,67 % Verfügbarkeit
- Wartung im Betrieb nicht möglich
- Nur ein Versorgungsweg für Kälte- und Energieverteilung

Tier 1



V = 99,67 %  
DTPA 28,8 h



## Tier 2 - Einfache Redundanz im Rechenzentrum

- Redundanz nur in Versorgungsweg
- Jährliche Ausfallzeit 22 Stunden
- 99,75 % Verfügbarkeit
- Wartung im Betrieb bedingt möglich
- Redundanter Versorgungsweg für Kälte- und Energieverteilung

Tier 2



V = 99,75 %  
DTPA 22 h

## Tier 3 - Fehlertoleranz möglich

- Redundanz in Versorgung
- Server mehrfach vorhanden
- Jährliche Ausfallzeit 1,6 Stunden
- 99,98 % Verfügbarkeit
- Wartung im Betrieb möglich
- Redundanter Versorgungsweg für Kälte- und Energieverteilung

### Tier 3



V = 99,98 %  
DTPA 1,6 h

## Tier 4 - Die Masterclass

- Komplette doppelte Redundanz
- Server mehrfach vorhanden
- Jährliche Ausfallzeit 0,8 Stunden
- 99,991 % Verfügbarkeit
- Wartung im Betrieb möglich
- Mehrfach redundanter Versorgungsweg für Kälte- und Energieverteilung

### Tier 4



V = 99,991 %  
DTPA 0,8 h

# RAID ist kein Backup!

- Daten werden auf mehrere Festplatten verteilt
- Relative Ausfallsicherheit von Festplatten
- Problem bei Systematischen Fehlern
- Problem bei bestimmten RAID-Leveln
- RAID ist unverzichtbar, aber kein Backup!

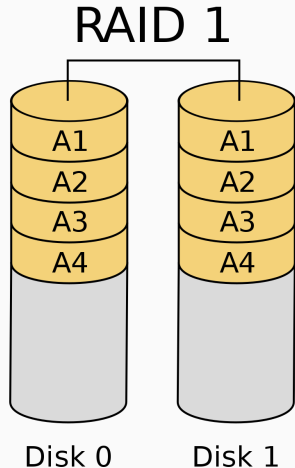


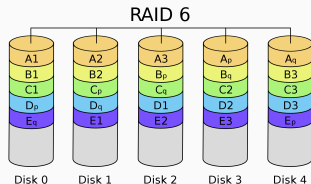
Bild: <https://de.wikipedia.org/wiki/RAID>

# RAID ja, aber welche Konfiguration?

## RAID 6 oder 60

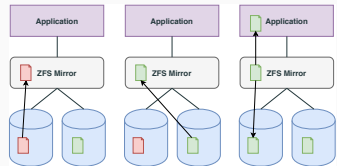
- Bis zu zwei Festplatten können ausfallen
- Bei der Wiederherstellung von Festplatten oft Ausfall weiterer Platte
- Gutes Preis/Leistungs-Verhältnis

<https://de.wikipedia.org/wiki/RAID>

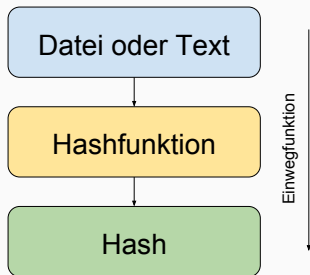


## Zettabyte File System

- Spezielles Filesystem
- Als Software-RAID umgesetzt
- Ausfallsicherheit wie RAID 6
- Reparatur von Files durch Hashes
- Möglich: Deduplizierung & Kompression
- Möglich: Verschlüsselung & Caching



- Einwegfunktion
- Hash immer gleiche Größe
- Gleiche Datei erzeugt gleichen Hash
- Minimale Änderungen erzeugen völlig unterschiedlichen Hash
- Kryptographische Sicherheit



- Schutz vor Manipulation
- Schutz vor nachträglicher Änderung
- Wird oft durch kryptografische Signaturen sichergestellt
- Zertifizierte Systeme sehr teuer
- Nötig für Compliance, Finanz- und Gesundheitsdaten



- Backups: Beliebtes Ziel für Datenmanipulation und -diebstahl
- Backups: Oft nachlässige Sicherheit
- Verschlüsselung macht Backup unbequem
- Eigener Infrastruktur sollte nicht vertraut werden
- Transportverschlüsselung nicht vergessen

# Vertraue keinem Backup!

Niemals!

- Backups prüfen
- Ernstfall simulieren
- Mehrstufige Backups
- Nochmal Backups prüfen!

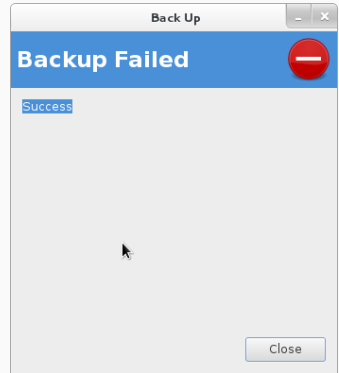


Bild: <https://mail.gnome.org/archives/deja-dup-list/2012-November>

- Ausfälle passieren...
- ...zu unmöglichsten Zeiten
- Notfallplan aufstellen
- Infrastruktur funktioniert nicht
- Dauer?
- Ist diese Zeit vertretbar?



# Backupinfrastruktur in der Praxis

---

# Struktur der OTH Regensburg

- 12000 Studierende
- 850 Mitarbeiter
- 1 Petabyte an Speicher
- 3 Serverräume
- Datenspeicherung >50 Jahre
- Voll redundante Systeme (Tier 2-3)
- Sehr gut aufgestellte Backup-Infrastruktur und Notfallpläne



Bild: [https://de.wikipedia.org/wiki/Ostbayerische\\_Technische\\_Hochschule](https://de.wikipedia.org/wiki/Ostbayerische_Technische_Hochschule)

## Redundanz $\neq$ Redundanz

- Zentrale Kälteanlage an der Hochschule
- Redundant ausgelegte Kälteanlage
- Redundanter Wärmetauscher
- Beide an Kälteanlage angeschlossen
- Pumpenausfall führte zu Ausfall aller Wärmetauscher
- Notabschaltung eines Serverraums nötig

# Problem: Stromausfälle

- Ausfall durch USV gepuffert
- Reale Pufferzeit  $\neq$  Angegebene Pufferzeit
- Längerfristige Pufferung durch Diesel
- Regelmäßige Wartung
- Immer echte Tests! Regelmäßig

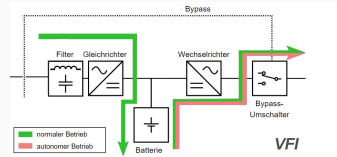


Bild: [https://de.wikipedia.org/wiki/Unterbrechungsfreie\\_Stromversorgung](https://de.wikipedia.org/wiki/Unterbrechungsfreie_Stromversorgung)

# Unbeabsichtigte Änderung/Löschung

- Unbeabsichtigte Änderungen passieren
- Fallen oft Jahre nicht auf
- Funktion zur Wiederherstellung an User
- Gibt auch Sicherheit
- Die Backupfunktion kann ausfallen

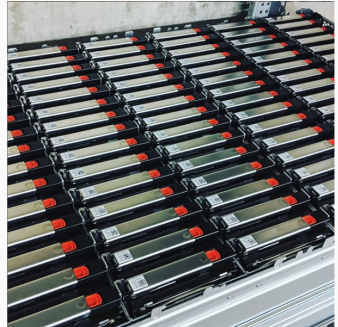


# Problem: Mehrstufige Backups

- Wiederherstellung von Windows war nicht möglich
- Fehler ist erst Monate später aufgefallen
- Keine Datensicherung vorhanden
- zweite Stufe (LUN-Snapshot)
- Wiederherstellung aufwändig aber möglich

# Problem: Festplattenausfall

- Konfiguration: RAID 60 mit zwei Hot-Spare Platten
- Festplattenausfall
- Hot-Spare Sicherung: Zweite HDD defekt
- Festplattentausch innerhalb von 4 h
- Hot-Spare Konfiguration überprüft



# Deduplizierung und Kompression sind deine Freunde

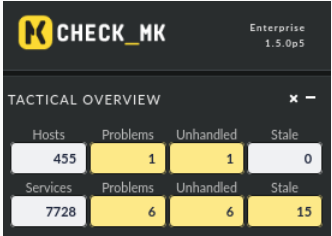
- Deduplizierung: Doppelte Dateien einmal ablegen
- Kompression: Dateien komprimieren
- Besonders effizient bei Snapshots
- Extreme Einsparung möglich
- Brutto-Speicherplatz steigt
- Beispiel OTH: 45,95 %

## Problem: Speicherung über 50 Jahre

- Kein Hersteller garantiert >10 Jahre
- Migration über Jahre hinweg auf jeweils neues System
- Standortunabhängigkeit
- Disasterrecovery schwer
- Retention Lock muss fortgeführt werden

# Problem: Fehler entdecken

- Fehler passieren immer
- Nur bei Erkennung Reaktion möglich
- Schon bei wenig System schnell unübersichtlich
- Empfehlung: check\_mk



The screenshot shows the Check\_MK Enterprise 1.5.0p5 interface. The 'TACTICAL OVERVIEW' section displays two tables. The first table for 'Hosts' shows 455 total hosts, 1 problem, 1 unhandled problem, and 0 stale problems. The second table for 'Services' shows 7728 total services, 6 problems, 6 unhandled problems, and 15 stale problems. Problems and unhandled counts are highlighted in yellow.

| Hosts |   | Problems |   | Unhandled |  | Stale |  |
|-------|---|----------|---|-----------|--|-------|--|
| 455   | 1 | 1        | 0 |           |  |       |  |

| Services |   | Problems |    | Unhandled |  | Stale |  |
|----------|---|----------|----|-----------|--|-------|--|
| 7728     | 6 | 6        | 15 |           |  |       |  |

## Problem: Single Point of Failure

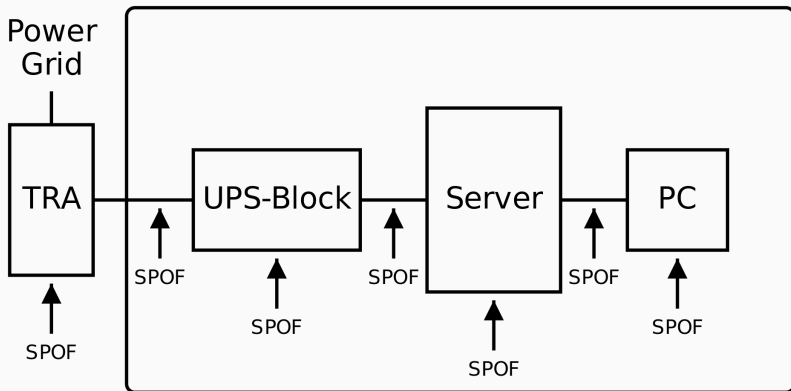


Bild: [https://de.wikipedia.org/wiki/Single\\_Point\\_of\\_Failure](https://de.wikipedia.org/wiki/Single_Point_of_Failure)

## Problem: Single Point of Failure

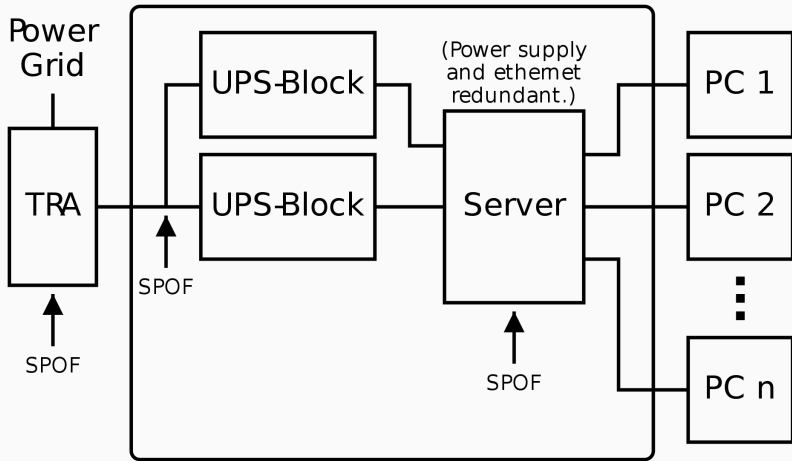


Bild: [https://de.wikipedia.org/wiki/Single\\_Point\\_of\\_Failure](https://de.wikipedia.org/wiki/Single_Point_of_Failure)

# Problem: Single Point of Failure

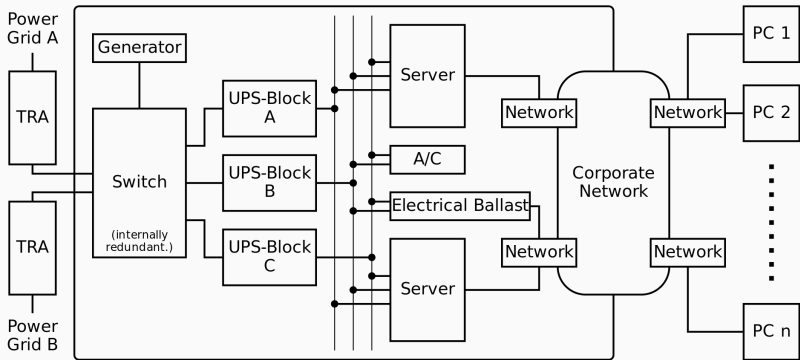


Bild: [https://de.wikipedia.org/wiki/Single\\_Point\\_of\\_Failure](https://de.wikipedia.org/wiki/Single_Point_of_Failure)



# Problem: Netzwerkverteilung

- Klimatechnik auch bei Netzwerkknotenpunkten
- Ringkonfiguration wegen Bauarbeiten
- SPOF zwischen Rechenzentren minimieren

- Abhärtung der Systeme
- Schulung der Mitarbeiter
- Anderen Servern sollte nicht vertraut werden
- Beispiel: OpenVAS
- Beispiel: Logmanagement
- Allgemein: Extrem schwer, alle Angriffe abzuhalten

- Ausfälle passieren!
- Wie ist die Reaktionszeit?
- Bei kritischen Systemen: Externer Service
- Wie schnell kann Ersatz bestellt werden?
- Eventuell: Vorhalten bestimmter Komponenten

# Grundlagen: Verschlüsselung und Signierung

---

# Warum Verschlüsselung?

- Firmenumfeld und Privat: Immer schützenswerte Daten!
- Verschlüsselung schafft vertrauen
- Vertrauen unabhängig von einzelnen
- Verschlüsselung teilweise gesetzlich gefordert
- Am besten: Allgegenwärtig und immer!
- Aber: Verschlüsselung auch unbequem

# Symmetrische Verschlüsselung

- Ein gemeinsames Geheimnis
- Effiziente Implementierung
- Problem des Schlüsselaustausches
- Beispiele: AES oder Blowfish

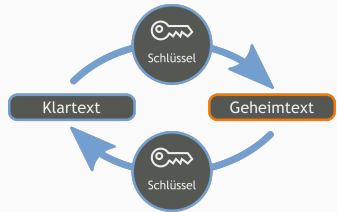


Bild: [https://de.wikipedia.org/wiki/Symmetrisches\\_Kryptosystem](https://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem)

# Asymmetrische Verschlüsselung

- Ein Schlüsselpaar
- Erster Teil: Nur Verschlüsseln
- Zweiter Teil: Nur Entschlüsseln
- Key zum Verschlüsseln öffentlich
- Key zum Entschlüsseln geheim
- Rechenintensiv
- Beispiele: RSA, Elliptic Curve Cryptography (ECC)

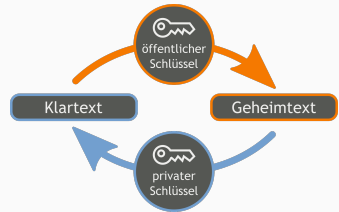
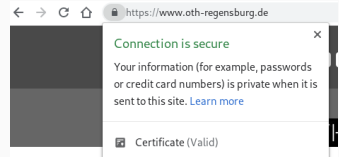


Bild: [https://de.wikipedia.org/wiki/Asymmetrisches\\_Kryptosystem](https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem)

- 1. Verschlüsselte Verbindung
- 2. Authentizität
- Kombination aus Symmetrischer und Asymmetrischer-Verschlüsselung
- Zertifikatsketten sorgen für Authentizität
- TLS ist nicht gleich TLS





- Extrem wichtig bei mobilen Geräten
- Auch wichtig für Cloud-Speicher
- Meist AES = Schnelle Implementation
- Komplex bei Aufsetzen und starten
- Wichtig für Datenschutz bei Diebstahl

- Basiert meist auf Asymmetrischen Kryptographiesystemen
- Integrität elektronischer Information gesichert
- Zeitstempel kryptographisch gesichert
- Wichtig für Compliance
- Unverzichtbar bei Revisionssicherheit

# Email-Verschlüsselung: PGP und S/MIME

- Email nur Transportverschlüsselt
- Ansonsten: Postkarte
- Absender kann ohne weiteres gefälscht werden
- Mögliche Methoden: PGP und S/MIME

[http://de.wikipedia.org/wiki/Pretty\\_Good\\_Privacy](http://de.wikipedia.org/wiki/Pretty_Good_Privacy)

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2.0.16 (GNU/Linux)

hQENAIPUVhZb8UnsAQF+KS9PNvkWYF0NnoStveMc4KwvGT7WlRFv/ZACvdyFsKD0
icurhLS7uh56KCoF1n5drfftwjDQWgMyly0cixqV/2HzeQgjZILE9Z1F0g7cgAbs
UZvy2hmaJf8dhHEUziALotfUMhoSeHeObxmonzb7vovJv5tWdtQ9W+p2tbQ4tiin
LAsJtwQhEVPNLtootBteC0dTg0dISe6kfQUSoN3A22SisUihmjxHPiio6iZB8gBS
hhfiSPa4khNw0DncRe2BjqW+YQHf7L6CFLjx2S1BCSr+KwLmUnVdWUonhHPF9mI
E/q7t2uo8Wg0iQgCjQubgYeqSUYN/xWpqaUX9071zdKUAbVjjLVTqTjNLLvms2H
s4BDzHEqKeuGuMAWFzyfuM+VNofTtXtChzrdjPuYiTsRL3YNUvqUpcGeKGyTAph2
k/fd7U32av7Pq63NoKK2g3RFcyBUiSdNLNhw8TYS1NdMSMXNw1R9dwVgFmsLj2vs
Rv89uFRiPbNLDXcx7CkRrTf13q0mty1850d6kSnt8qUFRnh4xQ==
=z6Xk
-----END PGP MESSAGE-----
```

# **Verschlüsselung und Signierung in der Praxis**

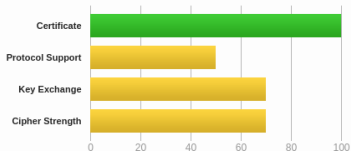
---

## Summary

### Overall Rating



No support for TLS 1.2, which is the only secure protocol version. [MORE »](#)



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. [MORE INFO »](#)

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. [MORE INFO »](#)

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. [MORE INFO »](#)

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. [MORE INFO »](#)

Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. [MORE INFO »](#)

DNS Certification Authority Authorization (CAA) Policy found for this domain. [MORE INFO »](#)

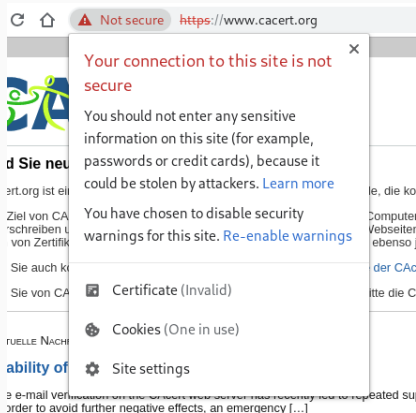


Bild: Screenshot Chrome

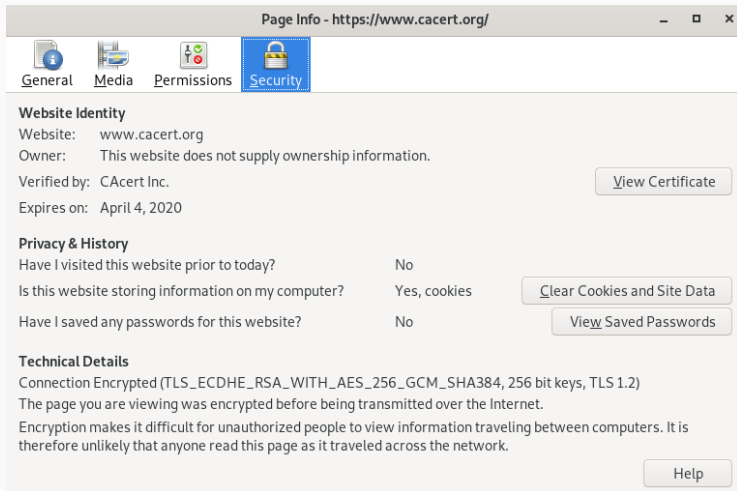


Bild: Screenshot Firefox

## Tipps

- Nogo: Website ohne TLS
- TLS ist kein Hexenwerk mehr
- Kostenlose Zertifikate: [letsencrypt.org](https://letsencrypt.org)
- Gute Verschlüsselung: [cipherli.st](https://cipherli.st)
- Stichwort: TLS 1.3 vs. eTLS



- pEp: Pretty Easy Privacy
- Standard Verschlüsselungsverfahren
- Einfach umgesetzt
- Outlook, Thunderbird, Android, iOS
- [www.pep.security](http://www.pep.security)



---

Bild: [https://de.wikipedia.org/wiki/Pretty\\_Easy\\_privacy](https://de.wikipedia.org/wiki/Pretty_Easy_privacy)

- Messenger praktisch für schnelle Kommunikation
- WhatsApp Ende-zu-Ende verschlüsselt
- Verwendet Signal-Protokoll
- Metadaten unverschlüsselt
- Backups unverschlüsselt
- Bessere Alternativen möglich
- Beispiel: Signal

# Zusammenfassung

---

- Backups sind kein einfaches Thema
- Verschlüsselung noch weniger
- Viel zu beachten
- Aber: Einfache Backups besser als Keine
- Gute Vorbereitung Hilft im Fehlerfall

**Timo Schindler**

timo.schindler@oth-regensburg.de