Backup: Verschlüsselung des Backups

19.04.2024 03:34:19

FAQ-Artikel-Ausdruck

Kategorie:	Datenspeicher & Datenablage::Backup	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	10:49:37 - 23.04.2021

Schlüsselwörter

Backup Verschlüsselung Konfiguration

Lösung (öffentlich)

Dafür gibt es verschiedene Möglichkeiten:

-

Verschlüsseln der Daten mit "herkömmlichen Mitteln" wie "zip -e .. " und anschließendes Abspeichern in einem bestimmten Verzeichnis. Nur dieses bestimmte Verzeichnis wird ins Backup eingebunden.

-

Vor dem TSM-Backup können die Daten (nur Datei-Inhalte, nicht Dateinamen) mit TSM-Mitteln auf Ihrem Rechner verschlüsselt werden. (Achtung: CPU-und Memory-intensiv) .

-

Das sind die relevanten Zeilen für die dsm.sys-Datei unter Linux/Unix:
include.encrypt /home/geheim/.../*
ENCryptkey save
EncryptionType AES128

-

Das sind die relevanten Zeilen für die dsm.opt-Datei unter Windows:
include.encrypt c:\home\geheim\...*
ENCryptkey save
EncryptionType AES128

-

Nach Änderung der Konfigurationsdatei muss zunächst das Crypt-Password gespeichert werden. Sichern Sie dazu eine einzelne Datei aus dem zu verschlüsselnden Datenbereich.

-

Nach der Beantwortung der Passwortanfrage ist dieses lokal bei Ihnen auf der Platte verschlüsselt abgelegt und auch automatische Backups funktionieren danach.

-

Die sichere Verwahrung des Verschlüsselung-Passwortes (getrennt von Ihrer Maschine) ist Voraussetzung für die Wiederherstellung der Daten. Mit dem Verlust des Passwords sind die Daten verloren.