

ANLEITUNG

BR-DMS.



Sicherung und Wiederherstellung

Das Konzept für das Gremium, das Einrichten der Sicherung und die Wiederherstellung im Ernstfall

Version	1.3.1
Stand	Oktober 2026
Autor	Tim van der Hoven
Kontakt	support@vanderhoven.eu

Inhalt

TEIL I – DAS KONZEPT

1 Auf einen Blick	4
1.1 Was gesichert wird	4
1.2 Wogegen was schützt	4
2 Wer kann was lesen?	6
2.1 Die zwei Schlüssel	6
3 Regeln für den Betrieb	7

TEIL II – SICHERUNG EINRICHTEN

4 Schritt für Schritt	9
4.1 Backup-Schlüssel anlegen	9
4.2 Schlüssel auf Papier sichern	9
4.3 Nächtliche Sicherung planen	9
4.4 Snapshots einschalten (QNAP)	10
4.5 Kopie zur IT	10

TEIL III – WIEDERHERSTELLEN

5 Welcher Fall liegt vor?	12
5.1 Einzelnes zurückholen	12
6 Auf demselben NAS wiederherstellen	13
7 Auf einem neuen Gerät wiederherstellen	14
8 Nach der Wiederherstellung prüfen	15

TEIL IV – VORDRUCKE

9 Schlüsselblatt	17
10 Protokoll der Wiederherstellungstests	18

TEIL I



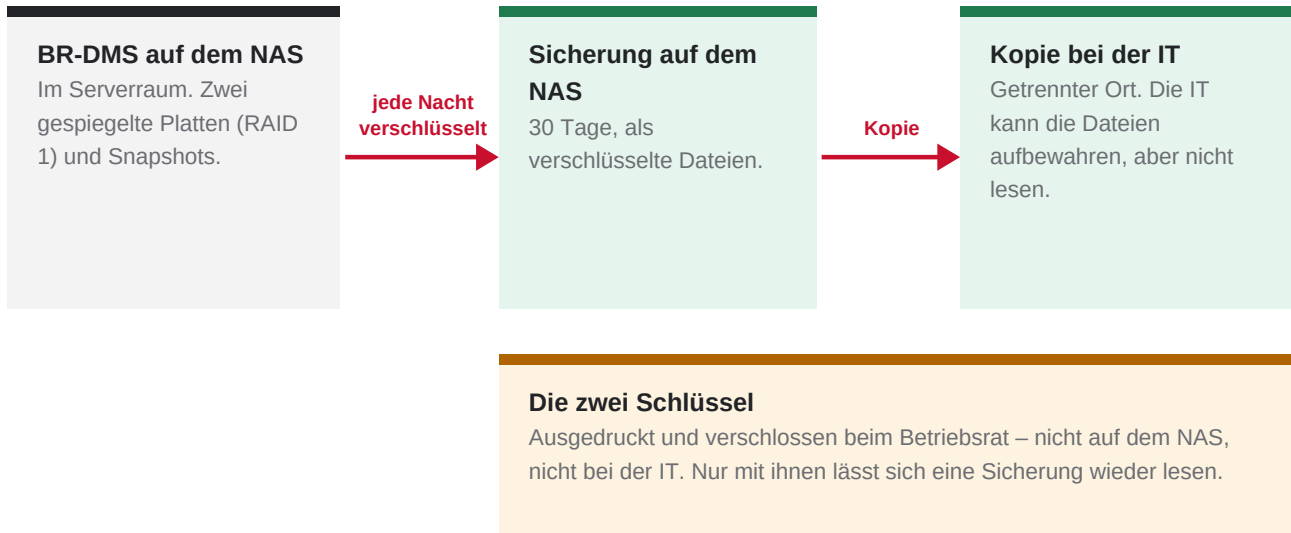
Das Konzept

Für das Gremium: was gesichert wird, wogegen die Sicherung schützt, wer was lesen kann und warum die Schlüssel so wichtig sind. Ohne Technik.

KAPITEL 1

Auf einen Blick

BR-DMS enthält alles, was der Betriebsrat schriftlich festhält: Sitzungen, Protokolle, Beschlüsse, Anhörungen, Personal- und Gehaltsdaten. Geht das verloren, ist die Arbeit von Jahren weg – und mit ihr der Nachweis, dass Fristen eingehalten und Beschlüsse ordnungsgemäß gefasst wurden. Die Sicherung ist deshalb in drei Stufen aufgebaut, und sie ist so verschlüsselt, dass eine Kopie außer Haus liegen kann, ohne dass jemand anderes sie lesen kann.



1.1 Was gesichert wird

Teil	Inhalt	Gesichert
Datenbank	Sitzungen, Protokolle, Beschlüsse, Fristen, Aufgaben, Benutzer, Personal- und Gehaltsdaten, Audit-Log, Suchtext der Dokumente	jede Nacht
Dokumente	Alle hochgeladenen Dateien, Scans und Fremdprotokolle (schon einzeln verschlüsselt)	jede Nacht
Schlüssel	ENCRYPTION_KEY (Dokumente) und BACKUP_KEY (Sicherung)	einmal, auf Papier
Zertifikat, Einstellungen des Servers	Lassen sich bei einer Neuinstallation neu erzeugen	nicht nötig

1.2 Wogegen was schützt

Keine Maßnahme allein reicht. Erst zusammen decken sie die üblichen Schadensfälle ab:

Schadensfall	RAID 1	Snapshots	Kopie bei der IT
Eine Festplatte fällt aus	ja	–	ja

Schadensfall	RAID 1	Snapshots	Kopie bei der IT
Versehentlich gelöscht oder überschrieben	–	ja	ja
Verschlüsselungstrojaner auf dem NAS	–	ja ¹	ja
NAS defekt, gestohlen, Brand, Wasser	–	–	ja
Fehler nach einem Update	–	ja	ja

¹ Snapshots sind schreibgeschützt; ein Trojaner, der nur die Dateien verschlüsselt, kann sie nicht verändern. Wer aber die Verwaltung des NAS übernimmt, kann auch Snapshots löschen – deshalb zusätzlich die Kopie außer Haus.

RAID ist kein Backup

RAID 1 spiegelt jede Änderung sofort auf die zweite Platte – auch ein versehentliches Löschen oder eine Verschlüsselung durch einen Trojaner. RAID schützt nur gegen den Ausfall einer Platte und ersetzt keine Sicherung.

Wie stark ist die Verschlüsselung?

Die Sicherung wird mit AES-256 verschlüsselt (AES-256-CBC, OpenSSL) – dem Standard, den auch Behörden und Banken einsetzen. Der BACKUP_KEY ist ein 256-Bit-Zufallswert; der eigentliche Schlüssel wird per PBKDF2 (HMAC-SHA256, 600.000 Durchläufe, eigener Zufalls-Salt je Datei) daraus abgeleitet. Ohne den Schlüssel lassen sich die Dateien nach heutigem Stand der Technik nicht lesen. Die Schwachstelle ist nicht die Mathematik, sondern der Ort, an dem der Ausdruck des Schlüssels liegt (Kapitel 2.1).

KAPITEL 2

Wer kann was lesen?

Die häufigste Sorge im Gremium: Liegt eine Kopie bei der IT, kann dann die IT – oder der Arbeitgeber – unsere Daten lesen? Die Antwort hängt an den Schlüsseln.

Wer	Hat	Kann lesen?
IT mit der Sicherungskopie	verschlüsselte Dateien, keinen Schlüssel	Nein – ohne BACKUP_KEY sind die Dateien wertlos
Jemand mit einer Platte aus dem NAS	Dokumente verschlüsselt, Datenbank offen	Dokumente nein; Datenbank ja, falls das NAS-Volume nicht verschlüsselt ist
Wer das NAS verwaltet (Admin)	Zugriff auf alles auf dem NAS, auch die Schlüssel in der .env	Technisch ja – deshalb muss geregelt sein, wer das ist
Mitglieder in BR-DMS	Anmeldung mit eigener Rolle	Nur, was ihre Rolle erlaubt (Handbuch Kapitel 10)

Der Administrator des NAS

Die Verschlüsselung schützt Kopien, die das NAS verlassen. Gegen jemanden, der das NAS selbst verwaltet, hilft keine Technik – nur eine klare Regelung: wer Administrator ist, dass Zugriffe nur mit Wissen des Betriebsrats erfolgen, und am besten ein Vier-Augen-Prinzip. Das gehört schriftlich in eine Vereinbarung mit der IT. Empfehlung: Admins des NAS sind nur Vorsitz und Stellvertretung; die Checkliste zum Absichern des NAS steht im Handbuch, Kapitel 11.3.

2.1 Die zwei Schlüssel

Schlüssel	Wofür	Wenn er verloren geht
ENCRYPTION_KEY	Ver- und entschlüsselt jedes Dokument in BR-DMS	Alle Dokumente sind dauerhaft unlesbar – auch mit Sicherung
BACKUP_KEY	Ver- und entschlüsselt die nächtliche Sicherung	Die Sicherungen lassen sich nicht mehr einspielen

Dazu kommen die Notfallzugänge: Verwaltungskonto des NAS und Admin von BR-DMS samt 2FA-Notfallcodes – sonst ist das Gremium ausgesperrt, wenn beide Admins ausfallen. Die übrigen Geheimnisse der .env erzeugt der Installationsassistent bei einer Wiederherstellung neu.

- **Aufbewahrung** – Beide Schlüssel und die Notfallzugänge ausdrucken (Vordruck in Teil IV), in einen Umschlag, versiegeln, in den Tresor bzw. einen verschlossenen Schrank des Betriebsrats
- **Nicht dort** – Nicht auf dem NAS (dort liegen sie schon), nicht bei der IT, nicht als Foto auf dem Handy, nicht per E-Mail
- **Zugang** – Vorsitz und Stellvertretung wissen, wo der Umschlag liegt; eine Zweitschrift an einem zweiten Ort (z. B. beim Rechtsanwalt des Betriebsrats) ist sinnvoll
- **Wechsel** – Bei jedem Passwort- oder Amtswechsel die Notfallzugänge neu eintragen

KAPITEL 3

Regeln für den Betrieb

Was	Wie oft	Wer
Sicherung läuft automatisch	jede Nacht, 02:00 Uhr	NAS (Aufgabenplaner)
Sicherung prüfen (Einstellungen → System)	monatlich	Vorsitz oder Stellvertretung
Kopie zur IT	täglich bzw. wöchentlich, wie mit der IT vereinbart	IT
Wiederherstellung testen	halbjährlich und nach größeren Updates	Vorsitz mit IT
Schlüssel-Umschlag prüfen	jährlich (noch da, versiegelt?)	Vorsitz

Auf dem NAS bleiben die Sicherungen 30 Tage, danach werden sie automatisch gelöscht. Wie lange die IT ihre Kopien aufbewahrt, wird mit ihr vereinbart – mindestens ebenso lange ist sinnvoll.

Wiederherstellung üben

Eine Sicherung ist erst dann eine Sicherung, wenn sie einmal auf einem anderen Gerät wiederhergestellt wurde. Das Ergebnis jedes Tests wird im Vordruck in Teil IV festgehalten.

TEIL II



Sicherung einrichten

Einmalig auf dem NAS: Backup-Schlüssel anlegen, Schlüssel sichern, nächtliche Sicherung planen, Snapshots einschalten und die Kopie zur IT einrichten.

KAPITEL 4

Schritt für Schritt

Alle Befehle werden per SSH auf dem NAS ausgeführt, im Installationsordner von BR-DMS – dem Ordner mit docker-compose.yml und .env. Er heißt im Folgenden <DATA_PATH>, z. B. /share/Container/br-dms (QNAP) oder /volume1/docker/br-dms (Synology).

4.1 Backup-Schlüssel anlegen

Neue Installationen bekommen den BACKUP_KEY vom Installationsassistenten. Bei einer bestehenden Installation einmal einen erzeugen und in die .env schreiben:

```
cd <DATA_PATH>
grep -q '^BACKUP_KEY=.' .env || echo "BACKUP_KEY=$(openssl rand -hex 32)" >> .env
grep -E '^(ENCRYPTION_KEY|BACKUP_KEY)=.' .env      # beide Schlüssel anzeigen
```

Die erste Zeile legt den Schlüssel nur an, wenn noch keiner da ist – ein vorhandener wird nie überschrieben. Ein Neustart von BR-DMS ist nicht nötig: Nur das Sicherungsskript liest den Schlüssel.

4.2 Schlüssel auf Papier sichern

1 Anzeigen

Mit dem letzten Befehl aus 4.1 beide Schlüssel anzeigen lassen.

2 Übertragen

In den Vordruck „Schlüsselblatt“ (Teil IV) eintragen oder die beiden Zeilen direkt ausdrucken. Jeder Schlüssel hat genau 64 Zeichen aus 0–9 und a–f.

3 Gegenlesen

Eine zweite Person liest die Abschrift Zeichen für Zeichen gegen die Anzeige. Dann die Notfallzugänge eintragen (Kapitel 2.1).

4 Verschließen

Umschlag versiegeln, mit Datum und Unterschrift versehen, wegschließen.

4.3 Nächtliche Sicherung planen

QNAP

QNAP plant Aufgaben über die Datei /etc/config/crontab. Per SSH als admin eine Zeile anhängen und den Zeitplan neu laden:

```
echo '0 2 * * * bash <DATA_PATH>/backup.sh > /tmp/brdms-backup.log 2>&1' \
>> /etc/config/crontab
crontab /etc/config/crontab && /etc/init.d/crond.sh restart
```

Synology

Systemsteuerung → Aufgabenplaner → Erstellen → Geplante Aufgabe → Benutzerdefiniertes Skript.
Benutzer: root, Zeitplan: täglich 02:00, Befehl:

```
bash /volume1/docker/br-dms/backup.sh
```

Erste Sicherung von Hand

```
sudo bash <DATA_PATH>/backup.sh  
ls -lh <DATA_PATH>/backups/  
# db_<Zeit>.sql.gz.enc, storage_<Zeit>.tar.gz.enc, info_<Zeit>.txt
```

Enden die beiden neuen Dateien auf .enc, ist die Sicherung verschlüsselt. Meldet das Skript „Kein BACKUP_KEY in der .env“, fehlt Schritt 4.1. In BR-DMS zeigt Einstellungen → System das letzte Backup mit dem Zusatz „verschlüsselt“ – sonst erscheint dort eine Warnung. Die kleine Datei info_<Zeit>.txt hält fest, mit welcher BR-DMS-Version die Sicherung entstand (siehe Kapitel 6).

4.4 Snapshots einschalten (QNAP)

Speicher & Snapshots → das Volume mit dem BR-DMS-Ordner → Snapshot → Snapshot-Zeitplan: täglich, Aufbewahrung z. B. 14 Tage. Snapshots brauchen ein Thick- oder Thin-Volume; auf einem statischen Volume steht die Funktion nicht zur Verfügung. Ein Snapshot belegt nur den Platz der seitdem geänderten Daten.

4.5 Kopie zur IT

Die IT holt bzw. bekommt regelmäßig den Inhalt von <DATA_PATH>/backups – etwa per Hybrid Backup Sync (QNAP), Hyper Backup (Synology) oder über ihre eigene Sicherungssoftware mit Lesezugriff nur auf diesen Ordner. Dabei gilt:

- **Nur .enc-Dateien** – In den Ordner gehören nur verschlüsselte Sicherungen; vorher prüfen (4.3)
- **Nie die .env** – Sie enthält die Schlüssel. Die IT bekommt sie nicht, auch nicht „zur Sicherheit“
- **Nur lesend** – Die IT braucht keinen Schreibzugriff auf das NAS
- **Aufbewahrung** – Wie lange die IT Kopien hält, schriftlich vereinbaren

TEIL III



Wiederherstellen

Was im Ernstfall zu tun ist – vom versehentlich gelöschten Eintrag bis zum kompletten Verlust des NAS – und wie man prüft, ob alles wieder da ist.

KAPITEL 5

Welcher Fall liegt vor?

Fall	Weg	Kapitel
Einzelnes versehentlich gelöscht oder geändert	Snapshot von gestern oder Sicherung in einer Testinstanz öffnen und das Benötigte heraussuchen	5.1
BR-DMS kaputt, z. B. nach einem Update	Letzte Sicherung auf demselben NAS einspielen	6
NAS defekt, gestohlen, verbrannt	Neues Gerät einrichten, Kopie der IT einspielen	7

Zurücksetzen betrifft alles

Eine Wiederherstellung setzt das ganze System auf den Stand der Sicherung zurück. Alles, was danach eingegeben wurde, ist weg. Deshalb bei einzelnen Verlusten nicht das laufende System zurücksetzen, sondern wie in 5.1 vorgehen.

5.1 Einzelnes zurückholen

Auf einem zweiten Gerät oder in einer Testinstanz (z. B. wie die Demo-Instanz aus Handbuch Kapitel 13.3, aber mit den echten Schlüsseln) die Sicherung von vor dem Verlust einspielen, das Benötigte dort heraussuchen – Dokument herunterladen, Text kopieren – und im laufenden System neu anlegen. Danach die Testinstanz wieder löschen.

KAPITEL 6

Auf demselben NAS wiederherstellen

1 Anmelden

Per SSH auf das NAS, in den Installationsordner wechseln.

2 Starten

restore.sh starten. Es listet alle Sicherungen auf, verschlüsselte erkennt es an .enc.

```
cd <DATA_PATH>
sudo bash restore.sh
```

3 Auswählen

Nummer der Sicherung eingeben und „j“ für die zugehörigen Dokumente.

4 Bestätigen

Mit „ja“ bestätigen. Das Skript prüft zuerst den BACKUP_KEY – passt er nicht, bricht es ab, bevor etwas überschrieben wird.

5 Warten

Das Skript hält BR-DMS an, spielt Datenbank und Dokumente ein und startet neu.

Passt die Version?

restore.sh zeigt vor dem Einspielen die Version der Sicherung und die des Systems. Stammt die Sicherung von einer neueren Version, bricht es ab: zuerst BR-DMS auf diese Version aktualisieren, dann erneut starten. Ältere Sicherungen werden eingespielt; BR-DMS ergänzt beim Start, was seither neu hinzugekommen ist. Sicherungen von vor Version 1.3.1 haben keine Versionsangabe – dann meldet das Skript „nicht vergleichbar“ und versucht es trotzdem.

6 Prüfen

Wie in Kapitel 8 beschrieben.

KAPITEL 7

Auf einem neuen Gerät wiederherstellen

Für den Totalverlust: Das neue Gerät kann ein anderes NAS sein, auch eines anderen Herstellers – ein Umzug von QNAP auf Synology wurde bereits erfolgreich getestet. Benötigt werden: das neue Gerät mit Docker, die Kopie der Sicherung von der IT und der Schlüssel-Umschlag.

1 BR-DMS installieren

Wie im Handbuch Kapitel 12 beschrieben. Im Installationsassistenten bei ENCRYPTION_KEY und BACKUP_KEY jeweils „Eigenen ... eingeben“ wählen und die Schlüssel vom Ausdruck eintragen – nicht neu erzeugen lassen.

2 Starten

BR-DMS einmal starten, damit Datenbank und Ordner angelegt werden.

3 Sicherung ablegen

Die beiden .enc-Dateien einer Nacht (gleiche Zeit im Namen) und die zugehörige info_<Zeit>.txt von der IT nach <DATA_PATH>/backups kopieren. Die neue Installation muss mindestens die Version der Sicherung haben (steht in der info-Datei).

4 Einspielen

restore.sh wie in Kapitel 6 ausführen.

5 Anmelden

Es gelten wieder die Benutzer und Passwörter des alten Systems – nicht das Admin-Konto aus dem Installationsassistenten.

6 Nacharbeiten

Zertifikat einrichten bzw. importieren (Handbuch 12.4), nächtliche Sicherung und Snapshots wieder einplanen (Kapitel 4), Kopie zur IT wieder einrichten.

Notfall ohne restore.sh

Ist das Skript nicht greifbar, lässt sich eine Sicherung auch von Hand mit openssl entschlüsseln. Das Ergebnis ist der Datenbank-Dump bzw. das Dokumenten-Archiv – dafür braucht es danach fachkundige Hilfe.

```
openssl enc -d -aes-256-cbc -pbkdf2 -iter 600000 -pass pass:<BACKUP_KEY> \
-in db_<Zeit>.sql.gz.enc | gunzip > db.sql
openssl enc -d -aes-256-cbc -pbkdf2 -iter 600000 -pass pass:<BACKUP_KEY> \
-in storage_<Zeit>.tar.gz.enc | tar -xzf -
```

KAPITEL 8

Nach der Wiederherstellung prüfen

Prüfung	Zeigt, dass ...
Anmeldung mit einem eigenen Konto	die Datenbank (Benutzer) zurück ist
Letzte Sitzung öffnen, Protokoll ansehen	Sitzungen und Protokolle vollständig sind
Ein beliebiges Dokument öffnen (Vorschau)	Dokumente zurück sind und der ENCRYPTION_KEY stimmt
Ein vertrauliches Dokument öffnen	auch die Rechte stimmen
Einstellungen → System	die Sicherungen wieder sichtbar sind
Audit-Log: letzter Eintrag	bis zu welchem Zeitpunkt die Daten reichen

Lässt sich kein Dokument öffnen, obwohl die Anmeldung klappt, stimmt der ENCRYPTION_KEY nicht mit dem des alten Systems überein: Schlüssel in der .env mit dem Ausdruck vergleichen, korrigieren und BR-DMS neu starten – eine erneute Wiederherstellung ist dafür nicht nötig.

TEIL IV



Vordrucke

Schlüsselblatt für den versiegelten Umschlag und Protokoll für die Wiederherstellungstests.

KAPITEL 9

Schlüsselblatt

Streng vertraulich

Dieses Blatt nach dem Ausfüllen nicht kopieren, scannen oder fotografieren. Es gehört versiegelt in den Tresor des Betriebsrats.

Installation / Gerät

Adresse von BR-DMS

ENCRYPTION_KEY – entschlüsselt die Dokumente

[illegible][illegible]

Zeichen 1–32

[illegible][illegible]

Zeichen 33–64

BACKUP_KEY – entschlüsselt die Sicherungen

[illegible][illegible]

Zeichen 1–32

[illegible][illegible]

Zeichen 33–64

Notfallzugänge – falls beide Admins ausfallen

NAS-Verwaltungskonto

Passphrase

2FA-Notfallcodes (NAS)

BR-DMS-Admin (E-Mail)

Passwort

Wiederherstellungscodes

Erstellt am / von

Gegengelesen von

Aufbewahrungsort

Zweitschrift bei

KAPITEL 10

Protokoll der Wiederherstellungstests

Ein Eintrag je Test. Ziel: einmal im Halbjahr und nach größeren Updates.

Datum	Sicherung vom	Zielgerät	Anmeldung	Dokument	Durchgeführt von