

19.9 Backup, Restore, RPO und RTO Spickzettel

Dieser Spickzettel fasst die wichtigsten Begriffe rund um Datensicherung, Wiederherstellung und Notfallplanung kompakt zusammen.

Er ist besonders wichtig für:

- Backup-Konzepte
- Restore-Aufgaben
- Ransomware-Schutz
- Notfallplanung
- Verfügbarkeitsanforderungen
- Prüfungsfragen zu RPO und RTO

Merksatz:

Backup ist die Sicherung.
Restore ist die Wiederherstellung.

Grundübersicht

Begriff	Bedeutung
Backup	Sicherung von Daten, Systemen oder Konfigurationen
Restore	Wiederherstellung aus einer Sicherung
RPO	maximal akzeptabler Datenverlust
RTO	maximal akzeptable Wiederherstellungszeit
Retention	Aufbewahrungsregel für Backups
Restore-Test	Prüfung, ob Wiederherstellung funktioniert
3-2-1-Regel	Grundregel für mehrere Backup-Kopien
Immutable Backup	unveränderliches Backup
Offline-Backup	nicht dauerhaft verbundenes Backup

Merksatz:

Ein Backup ist nur dann wertvoll,
wenn der Restore funktioniert.

Backup kurz erklärt

Backup bedeutet:

Daten,
Systeme,
Anwendungen
oder Konfigurationen werden gesichert,
damit sie später wiederhergestellt werden können.

Typische Sicherungsobjekte:

Dateien
Datenbanken
virtuelle Maschinen
Server
Konfigurationen
Benutzerprofile
Cloud-Daten
Anwendungen
Systemeinstellungen

Merksatz:

Backup schützt nicht direkt vor Fehlern,
aber ermöglicht Wiederherstellung.

Restore kurz erklärt

Restore bedeutet:

Wiederherstellung von Daten,
Systemen
oder Konfigurationen aus einem Backup.

Beispiele:

gelöschte Datei wiederherstellen

Datenbank auf früheren Zustand zurücksetzen

Server nach Defekt wiederherstellen

Konfiguration nach Fehler zurückspielen

Merksatz:

Restore ist der eigentliche Beweis,
dass ein Backup brauchbar ist.

Backup und Restore unterscheiden

Begriff	Frage	Ziel
Backup	Was wird gesichert?	Datenverlust vorbeugen
Restore	Wie wird wiederhergestellt?	Betrieb wiederherstellen

Merksatz:

Backup ist Vorbereitung.
Restore ist Wiederherstellung im Ernstfall.

Warum Restore-Tests wichtig sind

Ein Restore-Test prüft, ob ein Backup wirklich nutzbar ist.

Zu prüfen:

Daten vollständig?
Dateien lesbar?
Datenbank konsistent?
Anwendung startet?
Rechte korrekt?
Schlüssel vorhanden?
Wiederherstellungszeit akzeptabel?

Dokumentation korrekt?

Merksatz:

Backup ohne Restore-Test ist unsicher.

Typische Backup-Arten

Backup-Art	Bedeutung	Vorteil	Nachteil
Vollbackup	sichert alle ausgewählten Daten	einfache Wiederherstellung	viel Speicher und Zeit
inkrementelles Backup	sichert Änderungen seit letztem Backup	schnell, wenig Speicher	Restore braucht Backup-Kette
differenzielles Backup	sichert Änderungen seit letztem Vollbackup	Restore einfacher als inkrementell	wächst bis zum nächsten Vollbackup
Snapshot	Momentaufnahme	schnelle Rückkehr möglich	ersetzt kein vollständiges Backup
Image-Backup	vollständiges Systemabbild	komplettes System wiederherstellbar	größerer Speicherbedarf
dateibasiertes Backup	ausgewählte Dateien und Ordner	gezielt und flexibel	kein komplettes Systemabbild

Merksatz:

Backup-Art nach Wiederherstellungsziel auswählen.

Vollbackup

Ein Vollbackup sichert alle ausgewählten Daten vollständig.

Vorteile:

einfache Wiederherstellung
weniger Abhängigkeiten
vollständiger Sicherheitsstand

Nachteile:

benötigt viel Speicherplatz
dauert länger
erzeugt mehr Last

Merksatz:

Vollbackup sichert alles,
braucht aber mehr Speicher und Zeit.

Inkrementelles Backup

Ein inkrementelles Backup sichert nur Änderungen seit dem letzten Backup.

Das letzte Backup kann sein:

Vollbackup

oder

inkrementelles Backup

Vorteile:

schnell
spart Speicherplatz

Nachteile:

Wiederherstellung braucht mehrere Sicherungen
Backup-Kette darf nicht beschädigt sein

Merksatz:

Inkrementell = Änderungen seit letztem Backup.

Differenzielles Backup

Ein differenzielles Backup sichert Änderungen seit dem letzten Vollbackup.

Vorteile:

Restore einfacher als bei langer inkrementeller Kette
weniger Speicher als tägliches Vollbackup

Nachteile:

wird bis zum nächsten Vollbackup immer größer

Merksatz:

Differenziell = Änderungen seit letztem Vollbackup.

Snapshot

Ein Snapshot ist eine Momentaufnahme eines Systems, Datenträgers, Dateisystems oder einer virtuellen Maschine.

Typische Nutzung:

vor Updates
vor Konfigurationsänderungen
vor Tests
vor Softwareinstallationen

Wichtig:

Snapshot ist nicht automatisch ein vollwertiges Backup.

Merksatz:

Snapshot hilft bei schneller Rückkehr,
ersetzt aber kein Backup-Konzept.

Warum Snapshot kein Backup ersetzt

Snapshots liegen oft auf demselben System oder Speicher wie die Produktivdaten.

Risiken:

- Speicherdefekt betrifft Snapshot ebenfalls
- Ransomware kann Snapshot erreichen
- Snapshot kann gelöscht werden
- Snapshot-Kette kann beschädigt werden
- Speicherplatz kann volllaufen
- Standortausfall betrifft alles gemeinsam

Merksatz:

Backup muss getrennt,
geschützt
und wiederherstellbar sein.

Image-Backup

Ein Image-Backup sichert ein komplettes Systemabbild.

Enthalten sein können:

- Betriebssystem
- Anwendungen
- Konfiguration
- Dateien
- Bootinformationen

Vorteil:

gesamtes System kann wiederhergestellt werden

Merksatz:

Image-Backup = komplettes Systemabbild.

Dateibasiertes Backup

Ein dateibasiertes Backup sichert ausgewählte Dateien oder Ordner.

Geeignet für:

- Dokumente
- Benutzerdateien
- Projektdaten
- Konfigurationsdateien
- Exporte
- einzelne Verzeichnisse

Merksatz:

Dateibasiertes Backup sichert gezielt ausgewählte Inhalte.

Datenbank-Backup

Datenbanken brauchen besondere Sicherungsverfahren.

Wichtig:

- Konsistenz
- laufende Transaktionen
- Schreibzugriffe
- Transaktionslogs
- Zeitpunkt der Sicherung
- Wiederherstellbarkeit

Merksatz:

Datenbanken nicht einfach blind als Datei kopieren.

Konsistentes Backup

Ein konsistentes Backup stellt sicher, dass Daten in einem gültigen Zustand gesichert werden.

Beispiel:

Eine Datenbank darf nicht mitten in einer unvollständigen Transaktion unsauber kopiert werden.

Mögliche Verfahren:

Datenbankdump
Backup-Agent
Anwendungskonsistenter Snapshot
Transaktionslogs
Wartungsfenster

Merksatz:

Konsistenz ist besonders bei Datenbanken wichtig.

Point-in-Time-Recovery

Point-in-Time-Recovery bedeutet:

Wiederherstellung auf einen bestimmten Zeitpunkt.

Beispiel:

Datenbank auf Zustand von 10:15 Uhr zurücksetzen.

Nützlich bei:

versehentlichem Löschen
fehlerhaftem Import
beschädigten Daten
falscher Änderung

Merksatz:

Point-in-Time-Recovery stellt gezielt einen früheren Zeitpunkt wieder her.

RPO

RPO steht für:

Recovery Point Objective

Frage:

Wie viel Datenverlust ist maximal akzeptabel?

Beispiel:

RPO 1 Stunde

Bedeutung:

Es dürfen höchstens Daten von einer Stunde verloren gehen.

Merksatz:

RPO = maximal akzeptabler Datenverlust.

RTO

RTO steht für:

Recovery Time Objective

Frage:

Wie lange darf die Wiederherstellung dauern?

Beispiel:

RTO 4 Stunden

Bedeutung:

Der Dienst soll spätestens nach 4 Stunden wieder laufen.

Merksatz:

RTO = maximal akzeptable Wiederherstellungszeit.

RPO und RTO vergleichen

Begriff	Frage	Beispiel
RPO	Wie viel Datenverlust ist erlaubt?	maximal 1 Stunde Datenverlust
RTO	Wie lange darf Wiederherstellung dauern?	System läuft nach spätestens 4 Stunden

Merksatz:

RPO betrifft Datenverlust.

RTO betrifft Zeit bis Wiederherstellung.

RPO und Backup-Frequenz

Je kleiner das RPO, desto häufiger muss gesichert werden.

Beispiel:

RPO	mögliche Backup-Frequenz
24 Stunden	tägliches Backup
1 Stunde	stündliches Backup oder kontinuierliche Sicherung
wenige Minuten	Replikation plus Backup-Konzept oder spezielle Lösung

Merksatz:

Backup-Frequenz muss zum RPO passen.

RTO und Wiederherstellung

Das RTO hängt ab von:

Backup-Größe
Restore-Geschwindigkeit
Netzwerkgeschwindigkeit
Speicherleistung
Systemkomplexität
Abhängigkeiten
Personal
Dokumentation
Tests

Merksatz:

RTO wird nicht nur durch Backup bestimmt,
sondern durch den gesamten Wiederherstellungsprozess.

Retention

Retention bedeutet:

Aufbewahrungsregel für Backups.

Beispiele:

tägliche Backups 14 Tage behalten

wöchentliche Backups 8 Wochen behalten

monatliche Backups 12 Monate behalten

Merksatz:

Retention regelt,
wie lange Backups behalten werden.

Aufbewahrungszeit

Die Aufbewahrungszeit hängt ab von:

gesetzlichen Vorgaben
internen Regeln
Speicherplatz
Datenschutz
Wiederstellungsbedarf
Kosten
Risiko später entdeckter Fehler

Merksatz:

Backups müssen lange genug,
aber nicht unbegrenzt ohne Grund aufbewahrt werden.

Großvater-Vater-Sohn-Prinzip

Das Großvater-Vater-Sohn-Prinzip ist ein Rotationsschema.

Typisch:

Sohn:
tägliche Sicherung

Vater:
wöchentliche Sicherung

Großvater:
monatliche Sicherung

Merksatz:

Großvater-Vater-Sohn kombiniert tägliche,
wöchentliche
und monatliche Backups.

3-2-1-Regel

Die 3-2-1-Regel lautet:

3 Kopien der Daten

2 unterschiedliche Speicherarten

1 Kopie extern oder getrennt

Beispiel:

Produktivdaten

Backup auf NAS

zusätzliches Backup extern oder in Cloud

Merksatz:

3-2-1 reduziert das Risiko,
dass alle Kopien gleichzeitig verloren gehen.

3-2-1-1-0-Regel

Erweiterte Variante:

3 Kopien

2 unterschiedliche Medien

1 Kopie extern

1 Kopie offline oder immutable

0 Fehler bei Restore-Tests

Merksatz:

Die 0 steht für fehlerfrei getestete Wiederherstellung.

Offline-Backup

Ein Offline-Backup ist nicht dauerhaft mit dem Produktivsystem verbunden.

Beispiele:

getrennte Festplatte
Band
ausgelagertes Medium
abgeschottetes Backup-System

Vorteil:

besserer Schutz gegen Ransomware und versehentliche Löschung

Merksatz:

Offline-Backup ist nicht dauerhaft erreichbar.

Immutable Backup

Immutable bedeutet:

unveränderlich

Ein Immutable Backup kann für eine festgelegte Zeit nicht verändert oder gelöscht werden.

Schützt gegen:

Ransomware
Manipulation
versehentliche Löschung
kompromittierte Adminzugänge

Merksatz:

Immutable Backup schützt die Wiederherstellungsmöglichkeit.

Backup-Verschlüsselung

Backups sollten verschlüsselt werden, besonders bei sensiblen Daten oder externer Speicherung.

Wichtig:

- Schlüssel sicher aufbewahren
- Zugriff begrenzen
- Wiederherstellung mit Schlüssel testen
- Schlüsselverlust vermeiden

Merksatz:

Verschlüsseltes Backup ist nur nutzbar,
wenn der Schlüssel verfügbar ist.

Backup-Zugriffsrechte

Backups enthalten oft besonders viele Daten.

Deshalb müssen Zugriffe streng begrenzt werden.

Wichtig:

- keine normalen Benutzerrechte auf Backup-Speicher
- getrennte Adminrechte
- MFA für Backup-Konsole
- keine unnötigen Löschrechte
- Dienstkonto rechtearm halten
- Zugriff protokollieren

Merksatz:

Backups brauchen starken Zugriffsschutz.

Backup und Ransomware

Ransomware versucht häufig, Backups zu löschen oder zu verschlüsseln.

Schutzmaßnahmen:

Offline-Backup
Immutable Backup
getrennte Zugangsdaten
getrenntes Backupnetz
MFA
Monitoring
Restore-Test
Rechtebegrenzung

Merksatz:

Backups müssen auch vor Angreifern geschützt werden.

Backup-Monitoring

Backup-Monitoring prüft, ob Sicherungen erfolgreich laufen.

Zu überwachen:

letzter erfolgreicher Backup-Lauf
Fehlermeldungen
Datenmenge
Laufzeit
Speicherplatz
Aufbewahrung
Verschlüsselung
Restore-Test
ungewöhnliche Löschungen

Merksatz:

Ein fehlgeschlagenes Backup muss auffallen,
bevor ein Restore benötigt wird.

Backup-Logs

Backup-Logs zeigen, was bei einer Sicherung passiert ist.

Zu prüfen:

Startzeit
Endzeit
Erfolg oder Fehler
gesicherte Datenmenge
übersprungene Dateien
Warnungen
Zielsystem
Speicherplatz
Berechtigungsfehler

Merksatz:

Backup-Logs regelmäßig prüfen.

Redundanz

Redundanz bedeutet:

wichtige Komponenten sind mehrfach vorhanden.

Beispiele:

zwei Netzteile
RAID
mehrere Server
mehrere Internetleitungen
Cluster
zweite Firewall

Ziel:

Ausfall vermeiden oder abfedern

Merksatz:

Redundanz erhöht Verfügbarkeit,
ersetzt aber kein Backup.

Replikation

Replikation bedeutet:

Daten werden auf ein anderes System kopiert,
oft nahezu aktuell.

Vorteile:

schnelle Umschaltung
aktuelle Kopie
höhere Verfügbarkeit

Risiko:

Fehler,
Löschung
oder Ransomware können mitrepliziert werden.

Merksatz:

Replikation ist kein Backup.

Synchronisation

Synchronisation bedeutet:

Daten werden zwischen Speicherorten abgeglichen.

Problem:

Löschung,
Fehler

oder Verschlüsselung können mitsynchronisiert werden.

Merksatz:

Synchronisation hält Daten gleich,
stellt aber nicht automatisch alte Stände wieder her.

Backup, Redundanz, Replikation und Synchronisation vergleichen

Begriff	Ziel	Ersetzt Backup?
Backup	alte Zustände wiederherstellen	ja, ist Backup
Redundanz	Ausfall abfedern	nein
Replikation	aktuelle Kopie bereitstellen	nein
Synchronisation	Datenstände abgleichen	nein

Merksatz:

Redundanz,
Replikation
und Synchronisation ersetzen kein Backup.

Notfallhandbuch

Ein Notfallhandbuch beschreibt, was bei schweren Störungen zu tun ist.

Inhalte:

Ansprechpartner
Systeme
Prioritäten
Wiederherstellungsreihenfolge
Backup-Orte
Restore-Anleitungen
Zugangsdatenablage
Kommunikationswege
Eskalationswege

Merksatz:

Im Notfall darf nicht erst gesucht werden,
wer was weiß.

Restore-Reihenfolge

Bei Wiederherstellung ist die Reihenfolge wichtig.

Beispiel:

Netzwerk

Verzeichnisdienst

Speicher

Datenbank

Anwendung

Benutzerzugriff

Merksatz:

Restore braucht Reihenfolge,
weil Systeme voneinander abhängen.

Business Continuity

Business Continuity bedeutet:

Geschäftsprozesse sollen trotz Störung weiterlaufen
oder schnell wieder anlaufen.

Dazu gehören:

Notfallplanung

Ersatzprozesse

Kommunikation
Verantwortlichkeiten
Wiederanlauf
Tests

Merksatz:

Business Continuity betrachtet den Betrieb insgesamt.

Disaster Recovery

Disaster Recovery beschreibt:

Wiederherstellung der IT nach schweren Störungen.

Beispiele:

Ransomware
Brand
Rechenzentrumsausfall
Hardwaredefekt
Cloud-Ausfall
massiver Datenverlust

Merksatz:

Disaster Recovery ist IT-Wiederherstellung nach schwerem Vorfall.

Failover

Failover bedeutet:

Ein Dienst wird bei Ausfall auf ein Ersatzsystem umgeschaltet.

Möglich:

automatisch

oder

manuell

Beispiele:

zweite Firewall übernimmt

Datenbank-Replikat wird aktiv

anderer Server übernimmt Dienst

Merksatz:

Failover reduziert Ausfallzeit,

ersetzt aber kein Backup.

Typische Fehlerbilder

Fehlerbild	Wahrscheinliche Ursache
Backup angeblich erfolgreich, Restore geht nicht	Restore nie getestet
Backupziel voll	Speicherplatz oder Retention falsch
Datenbank nach Restore beschädigt	kein konsistentes Datenbank-Backup
Ransomware verschlüsselt Backups mit	Backup online und beschreibbar
Backup nicht lesbar	Medium defekt oder Datei beschädigt
verschlüsseltes Backup nicht nutzbar	Schlüssel fehlt
Restore dauert zu lange	RTO nicht realistisch geprüft
zu viel Datenverlust	RPO nicht eingehalten
alte Datei fehlt	Retention zu kurz
Dienst startet nach Restore nicht	Abhängigkeiten vergessen

Merksatz:

Backup-Probleme fallen oft erst beim Restore auf.

Typische Prüfungsfallen

Backup und Restore verwechseln.

Backup ohne Restore-Test als sicher ansehen.

Snapshot als vollständiges Backup bezeichnen.

Replikation als Backup bezeichnen.

Synchronisation als Backup bezeichnen.

Redundanz als Backup bezeichnen.

RPO und RTO verwechseln.

Retention mit RPO verwechseln.

Datenbankdateien ohne Konsistenz sichern.

Backup-Verschlüsselung ohne Schlüsselverwaltung planen.

Ransomware-Schutz für Backups vergessen.

Notfallhandbuch nicht berücksichtigen.

Merksatz:

In Prüfungen wird oft gefragt,
was kein Backup ersetzt.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist ein Backup?
- Was ist ein Restore?
- Warum ist ein Restore-Test wichtig?

- Was ist ein Vollbackup?
- Was ist ein inkrementelles Backup?
- Was ist ein differenzielles Backup?
- Was ist ein Snapshot?
- Warum ersetzt ein Snapshot kein Backup?
- Was bedeutet RPO?
- Was bedeutet RTO?
- Was ist Retention?
- Was bedeutet die 3-2-1-Regel?
- Was ist ein Immutable Backup?
- Warum ist ein Offline-Backup sinnvoll?
- Warum ist Replikation kein Backup?
- Warum ist Synchronisation kein Backup?
- Warum ersetzt Redundanz kein Backup?
- Was ist Disaster Recovery?
- Was ist Business Continuity?
- Warum müssen Backups gegen Ransomware geschützt werden?

IHK-sichere Kurzformulierung

Ein Backup ist eine Sicherung von Daten, Systemen oder Konfigurationen. Restore bezeichnet die Wiederherstellung aus dieser Sicherung. Ein Backup ist nur zuverlässig, wenn die Wiederherstellung regelmäßig getestet wird. Vollbackups sichern alle ausgewählten Daten, inkrementelle Backups sichern Änderungen seit dem letzten Backup und differenzielle Backups sichern Änderungen seit dem letzten Vollbackup. RPO beschreibt den maximal akzeptablen Datenverlust, RTO die maximal akzeptable Wiederherstellungszeit. Backups sollten nach geeigneten Regeln aufbewahrt, überwacht, geschützt, verschlüsselt und durch Offline- oder Immutable-Kopien gegen Ransomware abgesichert werden. Replikation, Synchronisation, Redundanz und Snapshots ersetzen kein vollständiges Backup-Konzept.

Merksätze

Backup = Sicherung.

Restore = Wiederherstellung.

Backup ohne Restore-Test ist unsicher.

Vollbackup sichert alles.

Inkrementell sichert seit letztem Backup.

Differenziell sichert seit letztem Vollbackup.

Snapshot ist Momentaufnahme.

Snapshot ersetzt kein vollständiges Backup.

Image-Backup sichert ein Systemabbild.

Datenbank-Backups müssen konsistent sein.

Point-in-Time-Recovery stellt einen Zeitpunkt wieder her.

RPO = Datenverlust.

RTO = Wiederherstellungszeit.

Retention = Aufbewahrungsregel.

Backup-Frequenz muss zum RPO passen.

Restore-Prozess muss zum RTO passen.

3-2-1 reduziert Gesamtrisiko.

3-2-1-1-0 ergänzt Offline oder Immutable und fehlerfreie Restore-Tests.

Offline-Backup ist nicht dauerhaft verbunden.

Immutable Backup ist unveränderlich.

Verschlüsseltes Backup braucht Schlüssel.

Backups brauchen starke Rechtebegrenzung.

Backups müssen vor Ransomware geschützt werden.

Backup-Monitoring ist Pflicht.

Backup-Logs regelmäßig prüfen.

Redundanz ist kein Backup.

Replikation ist kein Backup.

Synchronisation ist kein Backup.

Failover ist kein Backup.

Notfallhandbuch hilft im Ernstfall.

Restore braucht Reihenfolge.

Business Continuity betrachtet Geschäftsprozesse.

Disaster Recovery betrachtet IT-Wiederherstellung.

Im Notfall zählt nicht nur,
ob ein Backup existiert,
sondern ob es schnell und korrekt wiederhergestellt werden kann.
