17.7 Backup, Restore und Notfallmaßnahmen in der Praxis

Backups, Wiederherstellung und Notfallmaßnahmen gehören zu den wichtigsten Aufgaben in der Systemadministration.

Sie sorgen dafür, dass Systeme und Daten nach Fehlern, Ausfällen oder Angriffen wiederhergestellt werden können.

Typische Situationen:

```
- Datei versehentlich gelöscht
- Datenbank beschädigt
- Server ausgefallen
- Ransomware-Angriff
- Hardware defekt
- falsche Konfiguration eingespielt
- Update fehlgeschlagen
- Benutzerkonto kompromittiert
- Cloud-Ressource gelöscht
- Standort nicht erreichbar
```

Merksatz:

```
Backup ist nicht nur Datensicherung,
sondern Teil der Wiederherstellungsstrategie.
```

Warum Backup wichtig ist

Daten können auf viele Arten verloren gehen.

Ursachen:

```
Bedienfehler
Hardwaredefekt
Softwarefehler
Malware
Ransomware
```

Sabotage
Diebstahl
Feuer
Wasserschaden
Stromausfall
fehlerhafte Updates
falsche Synchronisation
Cloud-Fehlkonfiguration

Merksatz:

Backup schützt nicht vor jedem Vorfall,
aber es ermöglicht Wiederherstellung.

Backup und Restore unterscheiden

Backup:

Sicherung von Daten,
Systemen
oder Konfigurationen

Restore:

Wiederherstellung aus einer Sicherung

Wichtig:

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

Merksatz:

Backup ist die Sicherung.
Restore ist die Wiederherstellung.

Backup allein reicht nicht

Ein Backup-Konzept ist unvollständig, wenn nicht geklärt ist:

```
was gesichert wird
wie oft gesichert wird
wohin gesichert wird
wie lange gesichert wird
wer Zugriff hat
wie wiederhergestellt wird
wie Restore getestet wird
wie Backups geschützt werden
wie schnell Systeme wieder laufen müssen
```

Merksatz:

```
Backup ohne Restore-Plan ist nur halbe Sicherheit.
```

Restore-Test

Ein Restore-Test prüft, ob eine Wiederherstellung wirklich funktioniert.

Zu prüfen:

```
Daten vollständig?
Datei lesbar?
Datenbank konsistent?
Anwendung startet?
Rechte korrekt?
Konfiguration passend?
Schlüssel vorhanden?
Wiederherstellungszeit akzeptabel?
Dokumentation korrekt?
```

Merksatz:

```
Nur getestete Backups sind verlässliche Backups.
```

Typische Backup-Ziele

Backups können gespeichert werden auf:

```
lokaler Festplatte
NAS
Backup-Server
Bandlaufwerk
externer Festplatte
Cloud-Speicher
Objektspeicher
zweitem Standort
Offline-Medium
Immutable Storage
```

Merksatz:

```
Backup-Ziel muss zum Schutzbedarf passen.
```

Lokales Backup

Ein lokales Backup liegt in derselben Umgebung wie das Hauptsystem.

Vorteile:

```
schnelle Wiederherstellung
einfache Verwaltung
gute Kontrolle
geringe Latenz
```

Nachteile:

```
anfällig bei Feuer,
Diebstahl,
Ransomware
oder Standortausfall
```

Merksatz:

```
Lokales Backup ist schnell,
aber nicht ausreichend gegen Standortausfall.
```

Externes Backup

Ein externes Backup liegt getrennt vom Hauptsystem.

Beispiele:

```
zweiter Standort
Cloud-Speicher
ausgelagerte Festplatte
Bandsicherung außerhalb des Gebäudes
```

Vorteil:

```
Schutz bei Standortschaden
```

Merksatz:

```
Externes Backup schützt besser gegen lokale Katastrophen.
```

Offline-Backup

Ein Offline-Backup ist nicht dauerhaft mit dem produktiven System verbunden.

Vorteile:

```
besserer Schutz gegen Ransomware
besserer Schutz gegen versehentliches Löschen
besserer Schutz gegen kompromittierte Adminzugänge
```

Beispiele:

```
getrennte Festplatte
Band
abgeschottetes Backup-System
```

zeitweise getrenntes Speichermedium

Merksatz:

Offline-Backup ist nicht dauerhaft erreichbar und dadurch besser geschützt.

Immutable Backup

Immutable bedeutet:

unveränderlich

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

Schützt gegen:

Ransomware
versehentliche Löschung
kompromittierte Adminzugänge
Manipulation von Sicherungen

Merksatz:

Immutable Backup schützt die Wiederherstellungsmöglichkeit.

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 in Cloud oder auf Offline-Medium
```

Merksatz:

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

3-2-1-1-0-Regel

Eine erweiterte Variante ist:

```
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.
```

Vollbackup

Ein Vollbackup sichert alle ausgewählten Daten vollständig.

Vorteile:

```
einfache Wiederherstellung
vollständige Sicherung
```

weniger Abhängigkeit von anderen Sicherungen

Nachteile:

benötigt viel Speicherplatz
dauert länger
erzeugt mehr Last

Merksatz:

Vollbackup sichert alles,
braucht aber mehr Zeit und Speicher.

Inkrementelles Backup

Ein inkrementelles Backup sichert nur Änderungen seit dem letzten Backup.

Das letzte Backup kann sein:

Vollbackup

oder

anderes inkrementelles Backup

Vorteile:

schnell
spart Speicherplatz

Nachteile:

Wiederherstellung benötigt mehrere Sicherungen
Kette darf nicht beschädigt sein

Merksatz:

Inkrementell sichert Änderungen seit dem letzten Backup.

Differenzielles Backup

Ein differenzielles Backup sichert Änderungen seit dem letzten Vollbackup.

Vorteile:

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

Nachteile:

wächst bis zum nächsten Vollbackup

Merksatz:

Differenziell sichert Änderungen seit dem letzten Vollbackup.

Vollbackup, inkrementell und differenziell vergleichen

Backup-Art	Sichert	Vorteil	Nachteil
Vollbackup	alles	einfache Wiederherstellung	viel Speicher und Zeit
inkrementell	Änderungen seit letztem Backup	schnell und platzsparend	Restore braucht Backup-Kette
differenziell	Änderungen seit letztem Vollbackup	Restore einfacher als inkrementell	wächst mit der Zeit

Merksatz:

Vollbackup ist vollständig.
Inkrementell bezieht sich auf letztes Backup.
Differenziell bezieht sich auf letztes Vollbackup.

Snapshot

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

Snapshots sind nützlich vor:

```
Updates
Konfigurationsänderungen
Tests
Softwareinstallationen
Migrationen
```

Wichtig:

```
Snapshot ist nicht automatisch ein vollständiges Backup.
```

Merksatz:

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

Warum Snapshot kein vollständiges Backup ist

Snapshots liegen oft auf demselben System oder Speicher.

Risiken:

```
Speicher defekt
Ransomware erreicht Snapshot
Snapshot-Kette beschädigt
Speicherplatz läuft voll
Snapshot wird versehentlich gelöscht
Standortausfall betrifft Snapshot ebenfalls
```

Merksatz:

```
Snapshot ist praktisch,
aber kein Ersatz für getrennte Sicherung.
```

Image-Backup

Ein Image-Backup sichert ein komplettes Systemabbild.

Typische Inhalte:

```
Betriebssystem
Anwendungen
Konfiguration
Dateien
Bootinformationen
```

Vorteil:

```
gesamtes System kann wiederhergestellt werden
```

Merksatz:

```
Image-Backup sichert ein komplettes Systemabbild.
```

Dateibasiertes Backup

Ein dateibasiertes Backup sichert ausgewählte Dateien und Ordner.

Geeignet für:

```
Benutzerdateien
Projektdaten
Dokumente
Konfigurationsdateien
Exportdateien
```

Merksatz:

```
Dateibasiertes Backup sichert ausgewählte Dateien und Ordner.
```

Datenbank-Backup

Datenbanken brauchen besondere Sicherungsverfahren.

Wichtig:

Konsistenz
Transaktionen
Schreibzugriffe
Zeitpunkt der Sicherung
Wiederherstellungstest
Point-in-Time-Recovery je nach System

Merksatz:

Datenbankdateien nicht blind kopieren,
sondern datenbankgerechte Backups nutzen.

Konsistentes Backup

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

Beispiel:

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

Mittel:

Datenbankdump
Anwendungsstopp
Snapshot mit Anwendungskonsistenz
Backup-Agent
Transaktionslogs

Merksatz:

Konsistenz ist bei Datenbanken und Anwendungen besonders wichtig.

Point-in-Time-Recovery

Point-in-Time-Recovery bedeutet:

Wiederherstellung auf einen bestimmten Zeitpunkt.

Beispiel:

Datenbank wird auf den Zustand von 10:15 Uhr zurückgesetzt.

Nützlich bei:

versehentlichem Löschen
Datenbankfehler
fehlerhafter Import
beschädigten Daten

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 bedeutet:
Es dürfen höchstens Daten von einer Stunde verloren gehen.

Merksatz:

RPO beschreibt maximal akzeptablen Datenverlust.

RTO

RTO steht für:

Recovery Time Objective

Frage:

Wie lange darf die Wiederherstellung dauern?

Beispiel:

RTO 4 Stunden bedeutet:
Der Dienst soll spätestens nach 4 Stunden wieder laufen.

Merksatz:

RTO beschreibt maximal akzeptable Wiederherstellungszeit.

RPO und RTO unterscheiden

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

Merksatz:

RPO = Datenverlust.
RTO = Zeit bis Wiederherstellung.

Backup-Frequenz

Die Backup-Frequenz beschreibt, wie oft gesichert wird.

Sie hängt ab von:

Änderungsrate der Daten
Schutzbedarf
RPO
Speicherplatz

Systemlast
Wiederherstellungsanforderung
Kosten

Merksatz:

Je kleiner das erlaubte RPO,
desto häufiger muss gesichert werden.

Aufbewahrungszeit

Die Aufbewahrungszeit beschreibt, wie lange Backups behalten werden.

Zu beachten:

gesetzliche Vorgaben
interne Regeln
Speicherplatz
Datenschutz
Wiederherstellungsbedarf
Schutz vor später entdeckten Fehlern

Merksatz:

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

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,
wann alte Backups gelöscht 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.

Backup-Verschlüsselung

Backups sollten verschlüsselt werden, besonders wenn sie sensible Daten enthalten oder extern gespeichert werden.

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.

Zu vermeiden:

```
Jeder kann Backups lesen.
normales Benutzerkonto kann Backups löschen.
Backup-Admin nutzt Alltagskonto.
Ransomware kann Backup-Speicher erreichen.
Dienstkonto hat zu viele Rechte.
```

Merksatz:

```
Backups brauchen stärkeren Schutz als viele Produktivdaten.
```

Backup und Ransomware

Ransomware versucht häufig, Backups zu löschen oder zu verschlüsseln.

Schutzmaßnahmen:

```
Immutable Backup
Offline-Backup
getrennte Zugangsdaten
getrenntes Backupnetz
```

keine normalen Schreibrechte
MFA für Backup-Konsole
Backup-Logs überwachen
Restore regelmäßig testen

Merksatz:

Backups müssen vor dem Angreifer geschützt werden,
nicht nur vor Datenverlust.

Backup-Netz

Ein Backup-Netz ist ein getrenntes Netzwerk für Backup-Verkehr oder Backup-Systeme.

Vorteile:

weniger Angriffsfläche
weniger Störung des Produktivnetzes
bessere Kontrolle
Schutz vor lateraler Bewegung
gezieltere Firewall-Regeln

Merksatz:

Backup-Systeme sollten nicht frei aus jedem Netz erreichbar sein.

Backup-Monitoring

Backup-Monitoring prüft, ob Sicherungen erfolgreich laufen.

Zu überwachen:

letzter erfolgreicher Lauf
Fehlermeldungen
Datenmenge
Laufzeit
Speicherziel
Kapazität

```
Verschlüsselung
Aufbewahrung
Restore-Tests
```

Merksatz:

```
Ein fehlgeschlagenes Backup muss auffallen,
bevor ein Restore gebraucht 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 auswerten.
```

Restore-Reihenfolge

Bei Wiederherstellung ist die Reihenfolge wichtig.

Beispiele:

```
Netzwerk zuerst

dann
```

```
Verzeichnisdienst

dann

Speicher

dann

Datenbank

dann

Anwendung

dann

Benutzerzugriff
```

Merksatz:

```
Systeme hängen voneinander ab;
Restore braucht Reihenfolge.
```

Abhängigkeiten beim Restore

Vor einem Restore prüfen:

```
Welche Systeme hängen voneinander ab?
Welche Datenbanken werden benötigt?
Welche Zugangsdaten werden gebraucht?
Welche Zertifikate werden gebraucht?
Welche DNS-Namen müssen stimmen?
Welche Firewall-Regeln sind nötig?
Welche Speicherziele sind erreichbar?
Welche Versionen passen zusammen?
```

Merksatz:

Restore scheitert oft an vergessenen Abhängigkeiten.

Notfallhandbuch

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

Inhalte:

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

Merksatz:

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

Notfallkontaktliste

Eine Notfallkontaktliste enthält wichtige Kontakte.

Beispiele:

interne IT
Geschäftsleitung
Datenschutzbeauftragte
Sicherheitsverantwortliche
Internetprovider
Cloud-Anbieter
Hardware-Support

Softwaredienstleister
Versicherer
Behörden je nach Vorfall

Merksatz:

Notfallkontakte müssen aktuell und erreichbar sein.

Priorisierung im Notfall

Nicht jedes System ist gleich wichtig.

Zu priorisieren nach:

Geschäftsprozesse
kritische Dienste
Benutzeranzahl
Datenklassifizierung
Abhängigkeiten
RTO
RPO
Sicherheitslage
rechtliche Anforderungen

Merksatz:

Im Notfall zuerst die wichtigsten Dienste wiederherstellen.

Business Continuity

Business Continuity bedeutet:

Geschäftsprozesse sollen trotz Störung weiterlaufen oder schnell wieder anlaufen.

Dazu gehören:

Notfallplanung
Ersatzprozesse
Backup
Wiederanlauf
Kommunikation
Verantwortlichkeiten
Tests

Merksatz:

Business Continuity betrachtet nicht nur IT,
sondern den Betrieb insgesamt.

Disaster Recovery

Disaster Recovery beschreibt die Wiederherstellung von IT nach schweren Störungen.

Beispiele:

Rechenzentrumsausfall
Brand
Ransomware
massiver Hardwaredefekt
Cloud-Ausfall
Datenverlust

Merksatz:

Disaster Recovery ist IT-Wiederherstellung nach schwerem Vorfall.

Failover

Failover bedeutet:

Ein Dienst wird bei Ausfall automatisch oder manuell auf ein Ersatzsystem umgeschaltet.

Beispiele:

zweiter Server übernimmt
zweite Firewall übernimmt
anderer Standort übernimmt
Datenbank-Replikat wird aktiv

Merksatz:

Failover reduziert Ausfallzeit,
ersetzt aber kein Backup.

Redundanz

Redundanz bedeutet:

wichtige Komponenten sind mehrfach vorhanden.

Beispiele:

zwei Netzteile
zwei Firewalls
mehrere Server
mehrere Internetleitungen
RAID
Cluster
mehrere Standorte

Merksatz:

Redundanz erhöht Verfügbarkeit,
ersetzt aber kein Backup.

Replikation

Replikation bedeutet:

Daten werden auf ein anderes System kopiert,
oft nahezu in Echtzeit.

Vorteile:

schnelle Umschaltung
höhere Verfügbarkeit

Risiko:

Fehler,
Löschung
oder Verschlüsselung können mitrepliziert werden.

Merksatz:

Replikation ist kein Backup.

Backup, Redundanz und Replikation unterscheiden

Begriff	Ziel	Grenze
Backup	Wiederherstellung alter Zustände	Restore dauert
Redundanz	Ausfall vermeiden oder abfedern	schützt nicht vor Datenfehlern
Replikation	Daten auf zweitem System aktuell halten	Fehler werden oft mitkopiert

Merksatz:

Backup schützt Wiederherstellung.
Redundanz schützt Verfügbarkeit.
Replikation hält Daten aktuell.

Notfallübung

Eine Notfallübung testet, ob Notfallpläne funktionieren.

Zu prüfen:

Erreichen wir Kontakte?
Finden wir Dokumentation?
Funktionieren Zugänge?
Können wir Backups wiederherstellen?
Stimmen RTO und RPO?
Funktioniert Kommunikation?
Wer entscheidet was?
Wo fehlen Informationen?

Merksatz:

Notfallpläne müssen geübt werden.

Kommunikation im Notfall

Im Notfall muss klar sein:

Wer informiert wen?
Wer entscheidet?
Welche Kanäle werden genutzt?
Was wird Benutzern gesagt?
Was wird Kunden gesagt?
Was wird dokumentiert?
Wer spricht mit Dienstleistern?
Wer spricht mit Behörden,
falls nötig?

Merksatz:

Schlechte Kommunikation verschlimmert technische Notfälle.

Dokumentation beim Restore

Beim Restore dokumentieren:

Grund der Wiederherstellung
Zeitpunkt

betroffene Systeme
verwendetes Backup
Restore-Schritte
Probleme
Dauer
Ergebnis
Datenverlust
beteiligte Personen
Nacharbeiten

Merksatz:

Restore-Dokumentation hilft bei Nachvollziehbarkeit und Verbesserung.

Nacharbeiten nach Restore

Nach einem Restore prüfen:

Funktioniert der Dienst?
Sind Daten vollständig?
Stimmen Benutzerrechte?
Sind Logs aktiv?
Funktionieren Backups wieder?
Ist Monitoring aktiv?
Sind Zertifikate gültig?
Sind Schnittstellen erreichbar?
Gibt es Sicherheitslücken?
Muss Ursache behoben werden?

Merksatz:

Nach Restore ist die Arbeit nicht automatisch beendet.

Typische Fehler bei Backup und Restore

Häufige Fehler:

Backups nie getestet
Backupziel voll
Backup läuft mit Fehlern
Backups nicht verschlüsselt
Schlüssel nicht auffindbar
Backups im selben Netz wie Ransomware
keine Offline- oder Immutable-Kopie
nur Synchronisation statt Backup
Datenbank unsauber gesichert
Restore-Reihenfolge unbekannt
Dokumentation veraltet
alte Systeme nicht mehr kompatibel

Merksatz:

Der häufigste Backup-Fehler ist:
Man merkt das Problem erst beim Restore.

Checkliste: Backup-Konzept prüfen

Welche Daten sind kritisch?
Welche Systeme sind kritisch?
RPO festlegen.
RTO festlegen.
Backup-Art wählen.
Backup-Frequenz festlegen.
Aufbewahrung festlegen.
Backup-Ziel festlegen.
Verschlüsselung prüfen.
Zugriffsschutz prüfen.
Offline- oder Immutable-Kopie planen.
Backup-Logs überwachen.
Restore regelmäßig testen.
Notfallhandbuch erstellen.
Verantwortlichkeiten festlegen.
Dokumentation aktuell halten.

Merksatz:

```
Backup-Konzept muss geplant,
geschützt,
überwacht
und getestet werden.
```

Checkliste: Restore durchführen

```
Vorfall bewerten.
Ursache eingrenzen.
Passendes Backup auswählen.
Integrität des Backups prüfen.
Abhängigkeiten prüfen.
Zielsystem vorbereiten.
Restore durchführen.
Funktion testen.
Rechte prüfen.
Logs prüfen.
Monitoring prüfen.
Backupbetrieb wieder aktivieren.
Benutzer informieren.
Ergebnis dokumentieren.
Ursache dauerhaft beheben.
```

Merksatz:

```
Restore ist ein kontrollierter Prozess,
nicht nur Zurückkopieren von Dateien.
```

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 bedeutet die 3-2-1-Regel?
- 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 ist ein Image-Backup?
- Warum brauchen Datenbanken besondere Backups?
- Was bedeutet RPO?
- Was bedeutet RTO?
- Was ist Retention?
- Was ist das Großvater-Vater-Sohn-Prinzip?
- Warum sollten Backups verschlüsselt werden?
- Was ist ein Immutable Backup?
- Warum ist Replikation kein Backup?
- Was ist Disaster Recovery?
- Was ist Business Continuity?
- Was ist ein Notfallhandbuch?

Typische Prüfungsfallen

Backup und Restore unterscheiden.

Backup verhindert keinen Angriff.

Backup ermöglicht Wiederherstellung.

Backup ohne Restore-Test ist unsicher.

Synchronisation ist kein Backup.

Replikation ist kein Backup.

Redundanz ist kein Backup.

Snapshot ist nicht automatisch Backup.

Vollbackup sichert alles.

Inkrementell sichert seit letztem Backup.

Differenziell sichert seit letztem Vollbackup.

RPO ist Datenverlust.

RTO ist Wiederherstellungszeit.

Backups müssen geschützt werden.

Backups können Ziel von Ransomware sein.

Verschlüsselung braucht Schlüsselverwaltung.

Datenbank-Backups müssen konsistent sein.

Restore braucht Reihenfolge.

Notfallhandbuch aktuell halten.

Notfallpläne müssen getestet werden.

Nach Restore Funktion und Sicherheit prüfen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Backup	Sicherung von Daten oder Systemen
Restore	Wiederherstellung aus Sicherung
Restore-Test	Prüfung der Wiederherstellung
lokales Backup	Sicherung in gleicher Umgebung
externes Backup	Sicherung an getrenntem Ort
Offline-Backup	nicht dauerhaft verbundenes Backup
Immutable Backup	unveränderliches Backup
3-2-1-Regel	drei Kopien, zwei Medien, eine externe Kopie
Vollbackup	vollständige Sicherung
inkrementelles Backup	Änderungen seit letztem Backup
differenzielles Backup	Änderungen seit letztem Vollbackup
Snapshot	Momentaufnahme

Begriff	Kurze Erklärung
Image-Backup	vollständiges Systemabbild
dateibasiertes Backup	Sicherung ausgewählter Dateien
Datenbank-Backup	konsistente Sicherung einer Datenbank
Point-in-Time-Recovery	Wiederherstellung zu bestimmtem Zeitpunkt
RPO	maximal akzeptabler Datenverlust
RTO	maximal akzeptable Wiederherstellungszeit
Backup-Frequenz	Häufigkeit der Sicherung
Retention	Aufbewahrungsregel
Großvater-Vater-Sohn	Backup-Rotationsschema
Backup-Verschlüsselung	Schutz gesicherter Daten
Backup-Netz	getrenntes Netz für Backup
Backup-Monitoring	Überwachung von Sicherungen
Notfallhandbuch	Anleitung für schwere Störungen
Business Continuity	Aufrechterhaltung von Geschäftsprozessen
Disaster Recovery	IT-Wiederherstellung nach schwerem Vorfall
Failover	Umschaltung auf Ersatzsystem
Redundanz	mehrfach vorhandene Komponenten
Replikation	Kopie aktueller Daten auf anderes System
Notfallübung	Test des Notfallplans

IHK-sichere Kurzformulierung

Ein Backup ist eine Sicherung von Daten, Systemen oder Konfigurationen, während Restore die Wiederherstellung aus dieser Sicherung bezeichnet. Backups schützen nicht direkt vor Angriffen oder Ausfällen, ermöglichen aber die Wiederherstellung nach Datenverlust, Ransomware, Fehlkonfiguration oder Hardwaredefekt. Wichtige Konzepte sind Vollbackup, inkrementelles Backup, differenzielles Backup, Snapshot, Image-Backup, RPO, RTO, Retention, 3-2-1-Regel, Offline-Backup und Immutable Backup. Backups müssen geschützt, verschlüsselt, überwacht und regelmäßig durch Restore-Tests geprüft werden. Replikation, Redundanz und Synchronisation ersetzen kein Backup. Ein gutes Notfallkonzept umfasst Wiederherstellungsreihenfolge, Verantwortlichkeiten, Notfallhandbuch, Kommunikation und regelmäßige Übungen.

Merksätze

Backup = Sicherung.

Restore = Wiederherstellung.

Backup ohne Restore-Test ist unsicher.

Backup schützt nicht vor jedem Vorfall,
aber ermöglicht Wiederherstellung.

Synchronisation ist kein Backup.

Replikation ist kein Backup.

Redundanz ist kein Backup.

Snapshot ist nicht automatisch Backup.

Lokales Backup ist schnell,
aber nicht genug gegen Standortausfall.

Externes Backup schützt gegen Standortschaden.

Offline-Backup schützt gegen dauerhaften Zugriff durch Angreifer.

Immutable Backup schützt vor Veränderung und Löschung.

3-2-1 reduziert Gesamtrisiko.

Vollbackup sichert alles.

Inkrementell sichert Änderungen seit letztem Backup.

Differenziell sichert Änderungen seit letztem Vollbackup.

Datenbank-Backups müssen konsistent sein.

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

RPO = erlaubter Datenverlust.

RTO = erlaubte Wiederherstellungszeit.

Backup-Frequenz hängt vom RPO ab.

Retention regelt Aufbewahrung.

Verschlüsseltes Backup braucht verfügbaren Schlüssel.

Backups brauchen strenge Zugriffsrechte.

Ransomware greift oft Backups an.

Backup-Monitoring ist Pflicht.

Backup-Logs regelmäßig prüfen.

Restore braucht Reihenfolge.

Abhängigkeiten vor Restore prüfen.

Notfallhandbuch aktuell halten.

Business Continuity betrachtet Geschäftsprozesse.

Disaster Recovery betrachtet IT-Wiederherstellung.

Failover reduziert Ausfallzeit.

Notfallpläne üben.

Kommunikation im Notfall vorbereiten.

Restore dokumentieren.

Nach Restore Funktion,
Sicherheit
und Backupbetrieb prüfen.