

15.6 Cloud-Speicher, Backup und Datenmanagement

Cloud-Speicher ist Speicherplatz, der als Dienst über ein Netzwerk bereitgestellt wird.

Er wird genutzt für:

- Dateien
- Backups
- Datenbanken
- Archive
- Logs
- Medien
- virtuelle Festplatten
- Anwendungsdaten
- Dokumente
- Wiederherstellung nach Ausfällen

Merksatz:

Cloud-Speicher ist Speicher als Dienst,
aber kein automatisches Backup-Konzept.

Warum Cloud-Speicher wichtig ist

Daten sind für Unternehmen oft wichtiger als die Systeme selbst.

Ein Server kann neu installiert werden.

Aber verlorene Daten können kritisch sein.

Cloud-Speicher hilft bei:

zentraler Speicherung
Skalierung
weltweiter Verfügbarkeit
Backup
Archivierung

Zusammenarbeit
Datenanalyse
Notfallwiederherstellung

Merksatz:

Cloud-Speicher muss nach Datenart,
Zugriff,
Schutzbedarf
und Kosten geplant werden.

Arten von Cloud-Speicher

Die wichtigsten Speicherarten sind:

- Objektspeicher
- Blockspeicher
- Dateispeicher
- Archivspeicher
- Datenbankspeicher
- Backup-Speicher

Merksatz:

Nicht jeder Cloud-Speicher ist für denselben Zweck geeignet.

Objektspeicher

Objektspeicher speichert Daten als Objekte.

Ein Objekt besteht typischerweise aus:

Dateiinhalt
Metadaten
eindeutigem Namen oder Schlüssel

Typische Nutzung:

Backups
Bilder
Videos
Dokumente
Logs
Archivdaten
statische Webseiten
große unstrukturierte Datenmengen

Merksatz:

Objektspeicher eignet sich gut für viele unstrukturierte Dateien.

Objektspeicher einfach erklärt

Bei Objektspeicher denkt man nicht zuerst an Ordner und Laufwerke, sondern an Objekte in einem Speicherbereich.

Beispiel:

Objekt:

rechnung-2026-07.pdf

Metadaten:

Dateityp,

Erstellungsdatum,

Besitzer,

Speicherklasse,

Verschlüsselung

Schlüssel:

kunden/2026/rechnung-2026-07.pdf

Merksatz:

Objektspeicher arbeitet mit Objekten,
Schlüsseln
und Metadaten.

Bucket

Ein Bucket ist ein Speicherbehälter im Objektspeicher.

Darin liegen Objekte.

Beispiele:

backup-produktiv

dokumente-intern

logs-archiv

bilder-webseite

Wichtig:

Bucket-Berechtigungen sind sicherheitskritisch.

Merksatz:

Bucket = Speicherbehälter für Objekte.

Bucket-Berechtigungen

Ein häufiger Cloud-Fehler:

Bucket ist öffentlich lesbar.

Mögliche Folgen:

vertrauliche Daten werden öffentlich

personenbezogene Daten werden offengelegt

Backups können heruntergeladen werden

interne Dokumente sind sichtbar

Angreifer finden Zugangsdaten oder Logs

Merksatz:

Öffentliche Buckets sind ein großes Sicherheitsrisiko.

Objektspeicher: Vorteile

Vorteile:

sehr skalierbar
gut für große Datenmengen
Metadaten möglich
oft hohe Haltbarkeit
verschiedene Speicherklassen
gut für Backup und Archiv
Zugriff über APIs
Versionierung möglich

Merksatz:

Objektspeicher ist stark bei Skalierung und unstrukturierten Daten.

Objektspeicher: Nachteile

Nachteile:

nicht wie eine klassische Festplatte
nicht ideal für jede Anwendung
Latenz kann höher sein
Zugriff meist über API
Rechte müssen sauber gesetzt werden
Kosten für Zugriff und Datenübertragung beachten

Merksatz:

Objektspeicher ist kein direkter Ersatz für jedes Dateisystem.

Blockspeicher

Blockspeicher stellt Speicherblöcke bereit, ähnlich wie eine Festplatte.

Typische Nutzung:

- virtuelle Maschinen
- Betriebssystemplatten
- Datenbankserver
- Anwendungen mit Dateisystem
- leistungsabhängige Workloads

Beispiele:

- virtuelle Systemplatte
- virtuelle Datenplatte
- Datenbankvolume

Merksatz:

Blockspeicher verhält sich wie eine virtuelle Festplatte.

Blockspeicher: Vorteile

Vorteile:

- gut für Betriebssysteme
- gut für Datenbanken
- geringe Latenz möglich
- Dateisystem frei wählbar
- an virtuelle Maschinen anbindbar
- Leistung oft wählbar

Merksatz:

Blockspeicher eignet sich für VMs und leistungsabhängige Anwendungen.

Blockspeicher: Nachteile

Nachteile:

meist an einzelne Instanzen gebunden
Verwaltung von Dateisystem bleibt nötig
falsche Größe oder Leistung kann Kosten erzeugen
Backup muss geplant werden
nicht ideal für einfache Dateifreigaben zwischen vielen Systemen

Merksatz:

Blockspeicher braucht Administration wie eine Festplatte.

Dateispeicher

Dateispeicher stellt Speicher als Dateifreigabe bereit.

Typische Nutzung:

gemeinsame Dateien
klassische Ordnerstrukturen
Benutzerdateien
Anwendungen mit gemeinsamem Dateisystem
zentrale Ablagen

Typische Protokolle:

SMB
NFS

Merksatz:

Dateispeicher arbeitet mit Ordnern,
Dateien
und Freigaben.

Dateispeicher: Vorteile

Vorteile:

bekannte Ordnerstruktur
gemeinsame Nutzung möglich
geeignet für klassische Anwendungen
SMB oder NFS möglich
einfache Integration in viele Systeme

Merksatz:

Dateispeicher passt gut zu klassischen Freigaben.

Dateispeicher: Nachteile

Nachteile:

Berechtigungen müssen sauber geplant werden
Performance abhängig von Dienst und Netzwerk
nicht immer so skalierbar wie Objektspeicher
Kosten für Kapazität und Leistung beachten
Backup und Versionierung prüfen

Merksatz:

Cloud-Dateifreigaben brauchen Rechtekonzept und Backup.

Objekt-, Block- und Dateispeicher vergleichen

Speicherart	Typischer Einsatz	Vergleich
Objektspeicher	Backups, Medien, Archive, Logs	Objekt mit Metadaten
Blockspeicher	VM-Festplatten, Datenbanken	virtuelle Festplatte
Dateispeicher	gemeinsame Dateien, klassische Freigaben	Ordner und Dateien

Merksatz:

Objekt für große Datenmengen,
Block für VM und Datenbank,
Datei für Freigaben.

Archivspeicher

Archivspeicher ist für Daten gedacht, die selten benötigt werden.

Beispiele:

- alte Backups
- Langzeitarchive
- gesetzliche Aufbewahrung
- abgeschlossene Projekte
- alte Logs
- historische Dokumente

Vorteil:

- oft günstiger für langfristige Speicherung

Nachteil:

- Wiederherstellung kann länger dauern
- Zugriff kann teurer sein
- Mindestaufbewahrungszeiten möglich

Merksatz:

- Archivspeicher ist günstig für selten genutzte Daten, aber langsamer beim Zugriff.

Hot, Cool und Archive Storage

Viele Cloud-Anbieter unterscheiden Speicherklassen.

Typische Idee:

Speicherklasse	Nutzung
Hot	häufig genutzte Daten
Cool	selten genutzte Daten
Archive	sehr selten genutzte Langzeitdaten

Merksatz:

Je seltener der Zugriff,
desto günstiger oft die Speicherung,
aber desto teurer oder langsamer der Zugriff.

Lifecycle Management

Lifecycle Management bedeutet:

Daten werden automatisch nach Regeln verschoben oder gelöscht.

Beispiele:

Logs nach 30 Tagen in günstigere Speicherklasse verschieben.

Backups nach 1 Jahr archivieren.

temporäre Dateien nach 7 Tagen löschen.

alte Versionen nach 90 Tagen entfernen.

Merksatz:

Lifecycle-Regeln steuern den Lebenszyklus von Daten.

Versionierung

Versionierung bedeutet:

ältere Versionen einer Datei oder eines Objekts werden aufbewahrt.

Vorteile:

Wiederherstellung nach versehentlicher Änderung
Schutz vor Überschreiben
Hilfe bei Ransomware

Nachvollziehbarkeit

Aber:

Versionen verbrauchen Speicher
Kosten können steigen
Löschregeln müssen geplant werden

Merksatz:

Versionierung schützt vor Änderungen,
braucht aber Speicher- und Löschkonzept.

Snapshots

Ein Snapshot ist eine Momentaufnahme eines Systems oder Speichers.

Typische Nutzung:

VM-Zustand sichern
Volume-Zustand sichern
vor Update erstellen
schnelle Wiederherstellung
Testumgebung aus Produktivdaten erzeugen

Wichtig:

Snapshots sind nicht immer vollständiger Backup-Ersatz.

Merksatz:

Snapshot ist Momentaufnahme,
aber nicht automatisch Backup-Strategie.

Backup

Backup bedeutet:

Daten werden zusätzlich gesichert,
damit sie bei Verlust wiederhergestellt werden können.

Backup schützt vor:

versehentlichem Löschen
Hardwareausfall
Fehlkonfiguration
Ransomware
Datenkorruption
Benutzerfehler
fehlerhaften Updates
Ausfall eines Dienstes

Merksatz:

Backup ist nur wertvoll,
wenn Wiederherstellung funktioniert.

Cloud ist kein Backup

Ein häufiger Denkfehler:

Die Daten liegen in der Cloud,
also brauche ich kein Backup.

Das ist falsch.

Auch in der Cloud können Daten verloren gehen durch:

Benutzerfehler
falsche Synchronisation
Ransomware
gelöschte Benutzer
kompromittierte Adminzugänge
Fehlkonfiguration
abgelaufene Aufbewahrung
defekte Anwendung

Anbieterproblem

Merksatz:

Cloud-Speicherung ersetzt kein Backup-Konzept.

Backup-Ziele

Ein Backup-Konzept muss klären:

Was wird gesichert?

Wie oft wird gesichert?

Wie lange wird gesichert?

Wo wird gesichert?

Wer darf wiederherstellen?

Wie wird Wiederherstellung getestet?

Wie wird Backup geschützt?

Wie schnell muss Wiederherstellung sein?

Wie viel Datenverlust ist tolerierbar?

Merksatz:

Backup ohne Wiederherstellungsziel ist unvollständig.

RPO

RPO steht für:

Recovery Point Objective

RPO beschreibt, wie viel Datenverlust maximal akzeptabel ist.

Beispiel:

RPO = 24 Stunden

Bedeutung:

Im schlimmsten Fall dürfen Daten der letzten 24 Stunden verloren gehen.

Merksatz:

RPO fragt:

Wie viel Datenverlust ist erlaubt?

RTO

RTO steht für:

Recovery Time Objective

RTO beschreibt, wie schnell ein System wiederhergestellt sein muss.

Beispiel:

RTO = 4 Stunden

Bedeutung:

Das System soll innerhalb von 4 Stunden wieder verfügbar sein.

Merksatz:

RTO fragt:

Wie lange darf Wiederherstellung dauern?

RPO und RTO vergleichen

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

Merksatz:

RPO betrifft Datenverlust.

RTO betrifft Ausfallzeit.

Backup-Arten

Wichtige Backup-Arten:

Vollbackup

inkrementelles Backup

differentielles Backup

Snapshot

Replikation

Archivierung

Merksatz:

Backup-Art beeinflusst Speicherbedarf,

Dauer

und Wiederherstellung.

Vollbackup

Ein Vollbackup sichert alle ausgewählten Daten vollständig.

Vorteile:

einfache Wiederherstellung

vollständiger Sicherungsstand

unabhängig von vielen Zwischenschritten

Nachteile:

hoher Speicherbedarf

längere Sicherungsdauer

mehr Last

Merksatz:

Vollbackup ist vollständig,
aber aufwendiger.

Inkrementelles Backup

Ein inkrementelles Backup sichert nur Änderungen seit dem letzten Backup.

Vorteile:

weniger Speicherbedarf
schneller als Vollbackup
weniger Datenübertragung

Nachteile:

Wiederherstellung kann mehrere Sicherungen benötigen
Backup-Kette muss intakt sein

Merksatz:

Inkrementell sichert nur neue Änderungen seit dem letzten Backup.

Differentielles Backup

Ein differentielles Backup sichert Änderungen seit dem letzten Vollbackup.

Vorteile:

Wiederherstellung einfacher als bei langen inkrementellen Ketten
weniger aufwendig als tägliches Vollbackup

Nachteile:

wächst bis zum nächsten Vollbackup
braucht mehr Speicher als inkrementell

Merksatz:

Differentiell sichert Änderungen seit dem letzten Vollbackup.

Replikation

Replikation bedeutet:

Daten werden auf ein anderes System oder in eine andere Region kopiert.

Ziel:

höhere Verfügbarkeit
schnellere Umschaltung
Schutz vor Standortausfall

Aber:

Replikation ist nicht automatisch Backup.

Warum?

Fehler,
Löschungen
oder Ransomware können mit repliziert werden.

Merksatz:

Replikation schützt Verfügbarkeit,
Backup schützt Wiederherstellung.

Backup und Replikation vergleichen

Merkmal	Backup	Replikation
Zweck	Wiederherstellung alter Stände	Verfügbarkeit und Kopie
schützt vor Löschen	ja, wenn richtig aufbewahrt	nicht unbedingt
schützt vor Ransomware	ja, wenn isoliert oder unveränderlich	nicht unbedingt
Zugriff	meist Wiederherstellung nötig	oft direkt nutzbar

Merkmal	Backup	Replikation
Risiko	Backup zu alt	Fehler wird mitkopiert

Merksatz:

Replikation ist kein Ersatz für Backup.

3-2-1-Regel

Die 3-2-1-Regel ist eine bekannte Backup-Grundregel.

Sie bedeutet:

3 Kopien der Daten

2 unterschiedliche Speichermedien oder Speicherarten

1 Kopie außer Haus oder getrennt vom Hauptsystem

Für Cloud kann man ergänzen:

eine Kopie unveränderlich oder besonders geschützt

Merksatz:

Mehrere getrennte Kopien schützen besser vor Datenverlust.

Immutable Backup

Immutable bedeutet:

unveränderlich

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

Vorteile:

Schutz vor Ransomware
Schutz vor versehentlicher Löschung
Schutz vor kompromittierten Konten
bessere Wiederherstellungschance

Merksatz:

Immutable Backup schützt vor Manipulation und Löschung.

Air Gap

Air Gap bedeutet:

Eine Sicherung ist vom produktiven System getrennt.

Klassisch:

offline gelagertes Backup

In Cloud-Konzepten:

logisch getrennte Konten
getrennte Berechtigungen
unveränderliche Backups
getrennte Regionen
separate Backup-Tenants

Merksatz:

Air Gap bedeutet Trennung vom normalen Zugriffspfad.

Backup-Verschlüsselung

Backups enthalten oft sehr sensible Daten.

Deshalb sollten Backups verschlüsselt werden.

Wichtig:

- Schlüssel sicher verwalten
- Zugriff begrenzen
- Wiederherstellung testen
- Schlüsselverlust vermeiden
- Schlüsselrotation planen

Merksatz:

Verschlüsseltes Backup ist nur nutzbar,
wenn Schlüssel verfügbar sind.

Backup-Zugriffsrechte

Nicht jeder Administrator sollte Backups löschen dürfen.

Wichtige Regeln:

- getrennte Backup-Adminrolle
- Wiederherstellung nur berechtigte Personen
- Löschung stark begrenzen
- MFA für Backupverwaltung
- Protokollierung
- Genehmigung bei kritischen Aktionen

Merksatz:

Wer Backups löschen kann,
kann Wiederherstellung verhindern.

Restore

Restore bedeutet:

Daten werden aus einem Backup wiederhergestellt.

Mögliche Arten:

- einzelne Datei wiederherstellen
- gesamtes Verzeichnis wiederherstellen
- Datenbank wiederherstellen
- VM wiederherstellen
- Anwendung wiederherstellen
- System in anderer Region wiederherstellen

Merksatz:

Backup ohne getesteten Restore ist unsicher.

Restore-Test

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

Warum wichtig?

- Backup könnte unvollständig sein.
- Rechte könnten fehlen.
- Schlüssel könnten fehlen.
- Wiederherstellung dauert zu lange.
- Anwendung startet nicht.
- Daten sind inkonsistent.

Merksatz:

Erst Restore-Test zeigt,
ob Backup wirklich brauchbar ist.

Datenkonsistenz

Datenkonsistenz bedeutet:

Daten sind logisch korrekt und zusammenpassend.

Problem:

Wenn eine Datenbank während des Backups verändert wird,
kann ein einfaches Dateibackup inkonsistent sein.

Lösung:

anwendungskonsistente Backups
Datenbank-Dumps
Snapshots mit Quiescing
Transaktionslogs
passende Backup-Agenten

Merksatz:

Datenbanken brauchen konsistente Backups.

Datenbank-Backup

Datenbanken brauchen besondere Backup-Verfahren.

Wichtige Punkte:

konsistenter Zustand
Transaktionslogs
Point-in-Time-Recovery
regelmäßige Restore-Tests
Verschlüsselung
Aufbewahrung
Rechtekontrolle

Merksatz:

Datenbankdateien einfach kopieren reicht oft nicht.

Point-in-Time-Recovery

Point-in-Time-Recovery bedeutet:

Wiederherstellung auf einen bestimmten Zeitpunkt.

Beispiel:

Datenbankzustand von gestern 14:35 Uhr wiederherstellen.

Nützlich bei:

versehentlicher Löschung
fehlerhaftem Import
falschem Update
Ransomware
Datenkorruption

Merksatz:

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

Aufbewahrungsfrist

Aufbewahrungsfrist bedeutet:

Wie lange Daten oder Backups gespeichert werden.

Beispiele:

tägliche Backups 30 Tage
monatliche Backups 12 Monate
Jahresarchive 10 Jahre

Wichtig:

technische Anforderungen
rechtliche Vorgaben
Datenschutz
Speicherplatz

Kosten

Merksatz:

Aufbewahrung muss fachlich,
rechtlich
und technisch passen.

Löschkonzept

Ein Löschkonzept beschreibt, wann Daten gelöscht werden.

Wichtig bei:

personenbezogenen Daten
alten Backups
Projektarchiven
Logs
temporären Dateien
Testdaten
Benutzerkonten

Merksatz:

Daten dürfen nicht unbegrenzt ohne Zweck gespeichert werden.

Datenklassifizierung

Datenklassifizierung bedeutet:

Daten werden nach Schutzbedarf eingeteilt.

Beispiele:

öffentlich
intern
vertraulich

streng vertraulich
personenbezogen
geschäftskritisch

Die Klasse bestimmt:

Speicherort
Verschlüsselung
Zugriff
Backup
Aufbewahrung
Logging
Freigaben

Merksatz:

Datenklasse bestimmt Schutzmaßnahmen.

Personenbezogene Daten

Personenbezogene Daten sind Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen.

Beispiele:

Name
Adresse
E-Mail-Adresse
Kundennummer
Personalnummer
IP-Adresse je nach Kontext
Gesundheitsdaten
Bewerbungsdaten

Merksatz:

Personenbezogene Daten brauchen besonderen Schutz.

Datenminimierung

Datenminimierung bedeutet:

Nur Daten speichern,
die wirklich benötigt werden.

Cloud-Bezug:

keine unnötigen Kopien
keine unnötigen Exporte
keine unnötigen Logs mit Personendaten
keine ewigen Testdaten
keine Vollkopien für einfache Tests

Merksatz:

Weniger unnötige Daten bedeuten weniger Risiko.

Datenresidenz

Datenresidenz bedeutet:

Daten müssen in einem bestimmten Land oder einer bestimmten Region gespeichert werden.

Beispiel:

Speicherung innerhalb der EU

Wichtig für:

Datenschutz
Compliance
Verträge
Kundenanforderungen
Branchenvorgaben

Merksatz:

Datenresidenz beschreibt,
wo Daten liegen dürfen.

Datenhoheit

Datenhoheit bedeutet:

Wer Kontrolle über Daten hat.

Fragen:

Wer darf Daten lesen?
Wer darf Daten löschen?
Wer darf Daten exportieren?
Wer verwaltet Schlüssel?
Wer kann Zugriff technisch erzwingen?
Was passiert bei Anbieterwechsel?

Merksatz:

Datenhoheit ist Kontrolle über Zugriff,
Nutzung
und Verbleib von Daten.

Datenportabilität

Datenportabilität bedeutet:

Daten können in ein anderes System übertragen werden.

Wichtig:

Exportfunktion
offenes Format
vollständige Daten
Metadaten

Berechtigungen
Dokumentation
Wiederimport möglich

Merksatz:

Datenportabilität ist wichtig für Anbieterwechsel und Exit-Strategie.

Exit-Strategie für Daten

Eine Exit-Strategie beschreibt, wie Daten aus einem Cloud-Dienst wieder herauskommen.

Fragen:

Wie werden Daten exportiert?
In welchem Format?
Wie lange dauert Export?
Welche Kosten entstehen?
Werden Metadaten mit exportiert?
Werden Berechtigungen mit exportiert?
Wie wird Löschung beim Anbieter bestätigt?

Merksatz:

Cloud-Einstieg braucht auch Daten-Ausstiegsplan.

Cloud-Synchronisation

Cloud-Synchronisation hält Daten zwischen Geräten oder Diensten auf gleichem Stand.

Beispiele:

Datei auf Notebook geändert
Änderung wird in Cloud synchronisiert
andere Geräte erhalten Änderung

Risiko:

versehentliche Löschung wird synchronisiert

Ransomware verschlüsselt Dateien und Änderung wird synchronisiert

falsche Version überschreibt richtige Version

Merksatz:

Synchronisation ist kein Backup.

Cloud-Speicher und Ransomware

Ransomware kann auch Cloud-Speicher betreffen.

Beispiele:

verschlüsselte Dateien werden synchronisiert

Angreifer löscht Backups

kompromittiertes Konto löscht Daten

API-Schlüssel wird missbraucht

Versionen werden entfernt

Schutz:

MFA

Versionierung

Immutable Backup

getrennte Backup-Konten

Least Privilege

Monitoring

Restore-Tests

Merksatz:

Cloud-Speicher braucht Ransomware-Schutz.

Freigaben in Cloud-Speicher

Cloud-Speicher bietet oft einfache Freigaben.

Risiken:

- öffentlicher Link
- Link ohne Ablaufdatum
- Link ohne Passwort
- externe Benutzer nicht geprüft
- Ordner zu breit freigegeben
- alte Freigaben bleiben aktiv
- Download nicht eingeschränkt

Merksatz:

Cloud-Freigaben regelmäßig prüfen.

Externe Freigaben

Externe Freigaben erlauben Zugriff außerhalb der Organisation.

Sicherheitsregeln:

- nur bei Bedarf
- zeitlich begrenzen
- Empfänger prüfen
- Passwort oder MFA nutzen
- Download einschränken
- Protokollierung aktivieren
- Freigaben regelmäßig entfernen

Merksatz:

Externe Freigaben sind kontrollierter Extranet-Zugriff.

Cloud-Speicher und Berechtigungen

Berechtigungen sollten festlegen:

- Wer darf lesen?
- Wer darf schreiben?

Wer darf löschen?
Wer darf freigeben?
Wer darf externe Benutzer einladen?
Wer darf Versionen löschen?
Wer darf Aufbewahrung ändern?

Merksatz:

Speicherrechte müssen genauer sein als nur „Zugriff erlaubt“.

Cloud-Speicher und Logs

Wichtige Logs:

Datei gelesen
Datei geändert
Datei gelöscht
Datei geteilt
externer Zugriff
Download
Adminänderung
Berechtigung geändert
Version gelöscht
Aufbewahrung geändert

Merksatz:

Speicherlogs helfen,
Datenzugriffe nachvollziehbar zu machen.

Cloud-Speicher und Kosten

Kosten entstehen durch:

Speichergröße
Speicherklasse
Anzahl der Zugriffe

Datenübertragung
Wiederherstellung aus Archiv
Versionen
Snapshots
Backups
Replikation
Logs

Merksatz:

Cloud-Speicher ist skalierbar,
aber nicht automatisch billig.

Typische Cloud-Speicherfehler

Häufige Fehler:

Bucket öffentlich lesbar
keine Versionierung
keine Backups
keine Restore-Tests
zu lange Aufbewahrung
keine Löschregeln
falsche Speicherklasse
alte Snapshots vergessen
API-Schlüssel im Speicher
externe Freigaben nicht geprüft
Backups im gleichen Konto wie Produktivdaten ungeschützt
keine Verschlüsselung
keine Logs

Merksatz:

Cloud-Speicherfehler entstehen oft durch Rechte,
Freigaben,
Aufbewahrung
und fehlende Tests.

Checkliste: Cloud-Speicher sicher nutzen

Speicherart passend auswählen.
Daten klassifizieren.
Öffentliche Zugriffe vermeiden.
Berechtigungen minimal vergeben.
MFA für Admins erzwingen.
Versionierung prüfen.
Backup einrichten.
Immutable Backup prüfen.
Wiederherstellung testen.
Verschlüsselung aktivieren.
Schlüsselverwaltung klären.
Aufbewahrungsfristen festlegen.
Löschkonzept erstellen.
Lifecycle-Regeln nutzen.
Logs aktivieren.
Kosten überwachen.
Externe Freigaben regelmäßig prüfen.

Merksatz:

Cloud-Speicher braucht Technik,
Rechte,
Backup
und Kostenkontrolle.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist Objektspeicher?
- Was ist Blockspeicher?
- Was ist Dateispeicher?
- Wofür nutzt man Archivspeicher?
- Was ist ein Bucket?
- Warum sind öffentliche Buckets gefährlich?
- Was bedeutet Versionierung?

- Was ist ein Snapshot?
- Warum ist Cloud-Speicher kein automatisches Backup?
- Was ist der Unterschied zwischen Backup und Replikation?
- Was bedeutet RPO?
- Was bedeutet RTO?
- Was ist die 3-2-1-Regel?
- Was ist ein Immutable Backup?
- Warum sind Restore-Tests wichtig?
- Was ist Point-in-Time-Recovery?
- Was bedeutet Datenklassifizierung?
- Was bedeutet Datenresidenz?
- Warum ist Synchronisation kein Backup?
- Warum müssen externe Freigaben geprüft werden?

Typische Prüfungsfallen

Cloud-Speicher ist nicht automatisch Backup.

Synchronisation ist kein Backup.

Replikation ist kein Backup.

Snapshot ist nicht immer vollständiger Backup-Ersatz.

Backup ohne Restore-Test ist unsicher.

Objektspeicher ist nicht dasselbe wie Blockspeicher.

Blockspeicher ist eher virtuelle Festplatte.

Dateispeicher ist eher klassische Freigabe.

Bucket-Berechtigungen sind sicherheitskritisch.

Öffentliche Buckets vermeiden.

RPO betrifft Datenverlust.

RTO betrifft Wiederherstellungszeit.

Immutable Backup schützt vor Löschung und Manipulation.

Backups müssen verschlüsselt und geschützt sein.

Datenbanken brauchen konsistente Backups.

Datenklassifizierung bestimmt Schutzmaßnahmen.

Datenresidenz beschreibt Speicherort.

Datenportabilität ist wichtig für Anbieterwechsel.

Externe Freigaben regelmäßig prüfen.

Cloud-Speicher verursacht auch Zugriffskosten,
Versionierungskosten
und Wiederherstellungskosten.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Cloud-Speicher	Speicher als Dienst
Objektspeicher	Speicher für Objekte mit Metadaten
Blockspeicher	Speicher wie virtuelle Festplatte
Dateispeicher	Speicher als Ordner- und Dateifreigabe
Archivspeicher	Speicher für selten genutzte Langzeitdaten
Bucket	Speicherbehälter für Objekte
Metadaten	beschreibende Zusatzinformationen
Speicherklasse	Kosten- und Zugriffskategorie
Lifecycle Management	automatische Regeln für Verschieben oder Löschen
Versionierung	Aufbewahrung früherer Dateiversionen
Snapshot	Momentaufnahme eines Systems oder Speichers
Backup	zusätzliche Sicherung zur Wiederherstellung
Restore	Wiederherstellung aus Backup
Restore-Test	Prüfung der Wiederherstellung

Begriff	Kurze Erklärung
RPO	maximal akzeptabler Datenverlust
RTO	maximal akzeptable Wiederherstellungszeit
Vollbackup	vollständige Sicherung
inkrementelles Backup	Änderungen seit letztem Backup
differentielles Backup	Änderungen seit letztem Vollbackup
Replikation	Kopie auf anderes System oder Region
3-2-1-Regel	drei Kopien, zwei Medien, eine getrennte Kopie
Immutable Backup	unveränderliches Backup
Air Gap	getrennte Sicherung
Point-in-Time-Recovery	Wiederherstellung auf bestimmten Zeitpunkt
Aufbewahrungsfrist	Speicherdauer von Daten
Löschkonzept	Regelung zur Datenlöschung
Datenklassifizierung	Einteilung nach Schutzbedarf
Datenresidenz	Ort der Datenspeicherung
Datenhoheit	Kontrolle über Daten
Datenportabilität	Übertragbarkeit von Daten
Exit-Strategie	Plan zum Verlassen eines Dienstes
Synchronisation	Abgleich von Datenständen

IHK-sichere Kurzformulierung

Cloud-Speicher stellt Speicherplatz als Dienst bereit. Man unterscheidet vor allem Objektspeicher, Blockspeicher und Dateispeicher. Objektspeicher eignet sich für unstrukturierte Daten wie Backups, Medien, Logs und Archive. Blockspeicher wird häufig wie eine virtuelle Festplatte für virtuelle Maschinen oder Datenbanken genutzt. Dateispeicher stellt klassische Datei- und Ordnerfreigaben bereit. Cloud-Speicher ersetzt kein Backup-Konzept, da Löschungen, Fehlkonfigurationen, Ransomware oder falsche Synchronisation auch Cloud-Daten betreffen können. Wichtige Backup-Kennzahlen sind RPO für maximal tolerierbaren Datenverlust und RTO für maximal tolerierbare Wiederherstellungszeit. Backups müssen geschützt, verschlüsselt, regelmäßig getestet und passend aufbewahrt werden.

Merksätze

Cloud-Speicher = Speicher als Dienst.

Nicht jeder Speicher passt zu jedem Zweck.

Objektspeicher speichert Objekte mit Metadaten.

Bucket = Speicherbehälter.

Öffentliche Buckets sind gefährlich.

Blockspeicher = virtuelle Festplatte.

Dateispeicher = klassische Freigabe.

Archivspeicher für selten genutzte Daten.

Hot Storage für häufige Zugriffe.

Archive Storage für seltene Zugriffe.

Lifecycle-Regeln steuern Datenlebenszyklus.

Versionierung schützt vor Überschreiben.

Snapshot ist Momentaufnahme.

Snapshot ist nicht automatisch Backup-Strategie.

Cloud ist kein Backup.

Synchronisation ist kein Backup.

Replikation ist kein Backup.

Backup schützt Wiederherstellung.

Replikation schützt eher Verfügbarkeit.

RPO = erlaubter Datenverlust.

RTO = erlaubte Wiederherstellungszeit.

Vollbackup sichert alles.

Inkrementell sichert Änderungen seit letztem Backup.

Differentiell sichert Änderungen seit letztem Vollbackup.

3-2-1-Regel schützt besser vor Datenverlust.

Immutable Backup schützt vor Löschung.

Air Gap trennt Backup vom Hauptsystem.

Backup-Schlüssel sicher verwalten.

Restore-Test ist Pflicht.

Datenbanken brauchen konsistente Backups.

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

Aufbewahrung und Löschung planen.

Datenklassifizierung bestimmt Schutz.

Datenresidenz beschreibt Speicherort.

Datenportabilität für Anbieterwechsel beachten.

Cloud-Freigaben regelmäßig prüfen.

Speicherlogs aktivieren.

Cloud-Speicher-Kosten überwachen.
