

15.1 Cloud und moderne Bereitstellungsmodelle

Cloud beschreibt die Bereitstellung von IT-Ressourcen über ein Netzwerk.

Statt alle Systeme selbst lokal zu betreiben, können Unternehmen Rechenleistung, Speicher, Datenbanken, Anwendungen oder Plattformen bei einem Anbieter nutzen.

Typische Cloud-Ressourcen:

- virtuelle Server
- Speicherplatz
- Datenbanken
- Container
- Anwendungen
- Entwicklungsplattformen
- Backup-Dienste
- Identitätsdienste
- Netzwerkdienste
- Sicherheitsdienste

Merksatz:

Cloud bedeutet:
IT-Ressourcen werden als Dienst bereitgestellt.

Warum ist Cloud wichtig?

Cloud-Dienste sind in modernen IT-Umgebungen sehr verbreitet.

Gründe:

- schnelle Bereitstellung
- flexible Skalierung
- weniger eigene Hardware
- weltweite Erreichbarkeit
- nutzungsabhängige Kosten
- viele fertige Dienste
- hohe Automatisierbarkeit
- gute Integration mit modernen Anwendungen

Aber:

Cloud bedeutet nicht automatisch weniger Verantwortung.

Merksatz:

Cloud vereinfacht Bereitstellung,
ersetzt aber kein Sicherheits- und Betriebskonzept.

Cloud einfach erklärt

Klassisch:

Unternehmen kauft Server.
Server steht im eigenen Gebäude.
IT installiert Betriebssystem.
IT betreibt Anwendung.
IT kümmert sich um Hardware,
Strom,
Kühlung,
Backup
und Ausfallsicherheit.

Cloud:

Anbieter stellt Ressourcen bereit.
Unternehmen nutzt diese Ressourcen über Netzwerk oder Portal.
Abrechnung erfolgt häufig nach Nutzung.
Verantwortung wird je nach Modell zwischen Anbieter und Kunde geteilt.

Merksatz:

Cloud verlagert Teile der IT-Bereitstellung zu einem Anbieter.

On-Premises

On-Premises bedeutet:

IT wird lokal im eigenen Unternehmen oder eigenen Rechenzentrum betrieben.

Beispiele:

eigener Serverraum
eigenes Rechenzentrum
eigene Hardware
eigene Storage-Systeme
eigene Netzwerkgeräte
eigene Virtualisierung

Vorteile:

hohe Kontrolle
direkte Verwaltung
Daten bleiben im eigenen Betrieb
individuelle Anpassung möglich

Nachteile:

Hardwarekosten
Wartungsaufwand
Skalierung langsamer
eigene Verantwortung für Ausfallsicherheit

Merksatz:

On-Premises = lokal selbst betrieben.

Cloud

Cloud bedeutet:

IT-Ressourcen werden über ein Netzwerk als Dienst genutzt.

Beispiele:

virtueller Server beim Cloud-Anbieter
Cloud-Speicher
gehostete Datenbank
E-Mail aus der Cloud
Backup in der Cloud
Cloud-Identitätsdienst
Containerplattform

Merksatz:

Cloud = IT-Ressourcen als Dienst.

Hybrid Cloud

Hybrid Cloud kombiniert lokale IT und Cloud.

Beispiel:

interne Server im eigenen Rechenzentrum
plus
Cloud-Dienste für Backup,
Webanwendungen
oder Skalierung

Typische Einsatzfälle:

schrittweise Migration
sensible Systeme lokal
skalierbare Dienste in Cloud
Backup in Cloud
Cloud-Anbindung per VPN

Merksatz:

Hybrid Cloud kombiniert On-Premises und Cloud.

Multi Cloud

Multi Cloud bedeutet:

Ein Unternehmen nutzt mehrere Cloud-Anbieter.

Beispiel:

Anbieter A für virtuelle Server

Anbieter B für E-Mail

Anbieter C für Backup

Anbieter D für KI-Dienste

Vorteile:

weniger Abhängigkeit von einem Anbieter

passende Dienste pro Anbieter

Ausfallsicherheit durch Verteilung

Nachteile:

höhere Komplexität

unterschiedliche Portale

unterschiedliche Sicherheitsmodelle

schwierigeres Monitoring

mehr Know-how nötig

Merksatz:

Multi Cloud = mehrere Cloud-Anbieter gleichzeitig.

Public Cloud

Public Cloud bedeutet:

Cloud-Ressourcen werden von einem Anbieter für viele Kunden bereitgestellt.

Beispiele:

virtuelle Server
Datenbanken
Speicher
Webdienste
Cloud-Anwendungen

Wichtig:

Kunden teilen sich die Anbieterplattform,
sind aber logisch voneinander getrennt.

Merksatz:

Public Cloud = gemeinsam genutzte Anbieterplattform mit logischer Trennung.

Private Cloud

Private Cloud bedeutet:

Cloud-ähnliche Bereitstellung nur für eine Organisation.

Sie kann laufen:

im eigenen Rechenzentrum
bei einem Dienstleister
in einer dedizierten Umgebung

Typische Merkmale:

Selbstbedienung
Automatisierung
Virtualisierung
Ressourcenpools
interne Abrechnung oder Zuordnung
zentrale Verwaltung

Merksatz:

Private Cloud = Cloud-Prinzipien für eine Organisation.

Community Cloud

Community Cloud bedeutet:

Eine Cloud wird von mehreren Organisationen mit ähnlichen Anforderungen genutzt.

Beispiele:

Behörden
Forschungseinrichtungen
Gesundheitswesen
Bildungseinrichtungen

Ziel:

gemeinsame Anforderungen
gemeinsame Sicherheitsvorgaben
gemeinsame Compliance

Merksatz:

Community Cloud wird von einer bestimmten Gemeinschaft genutzt.

Cloud-Bereitstellungsmodelle

Modell	Kurze Erklärung
On-Premises	lokal selbst betrieben
Public Cloud	Cloud beim öffentlichen Anbieter
Private Cloud	Cloud für eine Organisation
Hybrid Cloud	Mischung aus lokal und Cloud
Multi Cloud	Nutzung mehrerer Cloud-Anbieter
Community Cloud	Cloud für bestimmte Organisationengruppe

Merksatz:

Bereitstellungsmodell beschreibt,
wo und für wen Cloud-Ressourcen betrieben werden.

Cloud-Service-Modelle

Die wichtigsten Service-Modelle sind:

- IaaS
- PaaS
- SaaS

Diese Modelle beschreiben, wie viel Verantwortung der Anbieter übernimmt und wie viel der Kunde selbst verwaltet.

Merksatz:

Service-Modell beschreibt,
welche Schichten als Dienst bereitgestellt werden.

IaaS

IaaS steht für:

Infrastructure as a Service

Dabei stellt der Anbieter grundlegende Infrastruktur bereit.

Beispiele:

virtuelle Maschinen
virtuelle Netzwerke
Block Storage
Load Balancer
Firewalls
IP-Adressen

Der Kunde verwaltet meist:

Betriebssystem
Updates im Betriebssystem
Anwendungen
Daten
Benutzer
Konfigurationen

Merksatz:

IaaS = virtuelle Infrastruktur statt eigener Hardware.

PaaS

PaaS steht für:

Platform as a Service

Dabei stellt der Anbieter eine Plattform bereit, auf der Anwendungen betrieben werden können.

Beispiele:

verwaltete Datenbank
App-Plattform
Web-App-Plattform
Containerplattform
Laufzeitumgebung
Entwicklungsplattform

Der Kunde verwaltet meist:

Anwendung
Daten
Konfiguration
Zugriff

Der Anbieter verwaltet mehr vom Betriebssystem, Runtime und Infrastruktur.

Merksatz:

PaaS = Plattform für Anwendungen,
ohne alles darunter selbst zu betreiben.

SaaS

SaaS steht für:

Software as a Service

Dabei nutzt der Kunde eine fertige Anwendung.

Beispiele:

E-Mail-Dienst
Online-Office
CRM-System
Ticketsystem
Cloud-Speicher
Videokonferenzdienst
Projektmanagement-Tool

Der Anbieter betreibt:

Anwendung
Plattform
Infrastruktur
Updates
Verfügbarkeit

Der Kunde kümmert sich vor allem um:

Benutzer
Berechtigungen
Daten
Einstellungen
Sicherheitsrichtlinien

Merksatz:

SaaS = fertige Software aus der Cloud.

IaaS, PaaS und SaaS vergleichen

Modell	Anbieter stellt bereit	Kunde verwaltet vor allem
IaaS	virtuelle Infrastruktur	Betriebssystem, Anwendung, Daten
PaaS	Plattform und Laufzeitumgebung	Anwendung, Daten, Konfiguration
SaaS	fertige Anwendung	Benutzer, Daten, Einstellungen

Merksatz:

IaaS gibt viel Kontrolle.
SaaS nimmt viel Betrieb ab.
PaaS liegt dazwischen.

Verantwortung bei Cloud

In der Cloud wird Verantwortung geteilt.

Der Anbieter ist nicht für alles verantwortlich.

Der Kunde bleibt verantwortlich für viele Dinge, zum Beispiel:

- Benutzerkonten
- Berechtigungen
- Daten
- sichere Konfiguration
- Passwörter und MFA
- Netzfregaben
- Zugriffskonzepte
- Compliance
- Backup-Strategie je nach Dienst

Merksatz:

Cloud bedeutet geteilte Verantwortung.

Shared Responsibility Model

Shared Responsibility Model bedeutet:

Anbieter und Kunde teilen sich Sicherheits- und Betriebsverantwortung.

Je nach Service-Modell verändert sich die Aufteilung.

Bei IaaS hat der Kunde mehr Verantwortung.

Bei SaaS übernimmt der Anbieter mehr Betrieb, aber der Kunde bleibt für Benutzer, Daten und Berechtigungen verantwortlich.

Merksatz:

Je fertiger der Dienst,
desto mehr Betrieb übernimmt der Anbieter,
aber Kundendaten und Zugriffe bleiben Kundenthema.

Beispiel Shared Responsibility bei IaaS

Bei einer virtuellen Maschine in der Cloud:

Anbieter verantwortet typischerweise:

physische Hardware
Rechenzentrum
Strom
Kühlung
Virtualisierungsplattform
Grundinfrastruktur

Kunde verantwortet typischerweise:

Betriebssystem
Patches
Firewall-Regeln
Benutzerkonten
Anwendung
Daten

Backup
Sicherheitskonfiguration

Merksatz:

Cloud-VM ist nicht automatisch sicher gepatcht.

Beispiel Shared Responsibility bei SaaS

Bei einer SaaS-Anwendung:

Anbieter verantwortet typischerweise:

Betrieb der Anwendung
Infrastruktur
Plattform
Updates
technische Verfügbarkeit

Kunde verantwortet typischerweise:

Benutzerverwaltung
Rollen
MFA
Datenklassifizierung
Freigaben
Aufbewahrung
Konfiguration
Schulung

Merksatz:

SaaS nimmt Betrieb ab,
aber nicht die Verantwortung für Zugriffe und Daten.

Virtualisierung in der Cloud

Cloud basiert häufig auf Virtualisierung.

Virtualisierung bedeutet:

physische Hardware wird in mehrere virtuelle Ressourcen aufgeteilt.

Beispiele:

virtuelle Maschinen
virtuelle Netzwerke
virtuelle Festplatten
virtuelle Firewalls
virtuelle Load Balancer

Merksatz:

Virtualisierung ist eine technische Grundlage vieler Cloud-Dienste.

Container in der Cloud

Container sind eine moderne Form der Anwendungsbereitstellung.

Container enthalten:

Anwendung
Abhängigkeiten
Laufzeitumgebung

Sie teilen sich aber den Kernel des Hosts.

Cloud-Dienste können Container bereitstellen, orchestrieren und skalieren.

Merksatz:

Container verpacken Anwendungen portabel und leichtgewichtig.

Orchestrierung

Orchestrierung bedeutet:

automatisierte Verwaltung mehrerer Container oder Dienste.

Aufgaben:

- Container starten
- Container stoppen
- Container verteilen
- Skalierung
- Updates
- Health Checks
- Netzwerke
- Secrets
- Rollbacks

Merksatz:

Orchestrierung verwaltet viele Container automatisch.

Kubernetes

Kubernetes ist eine verbreitete Plattform zur Container-Orchestrierung.

Es verwaltet:

- Pods
- Services
- Deployments
- Skalierung
- Rollouts
- Netzwerke
- Konfigurationen
- Secrets

Für Prüfungen reicht oft:

Kubernetes orchestriert Container.

Merksatz:

Kubernetes verwaltet Container-Anwendungen in Clustern.

Serverless

Serverless bedeutet nicht, dass keine Server existieren.

Es bedeutet:

Der Kunde verwaltet keine einzelnen Server.

Der Anbieter betreibt die Infrastruktur.

Der Kunde stellt Funktionen oder Code bereit.

Beispiele:

Funktionen bei Ereignissen ausführen
automatische Skalierung
Abrechnung nach Ausführung oder Nutzung

Merksatz:

Serverless heißt:
keine Serververwaltung durch den Kunden.

Function as a Service

Function as a Service wird abgekürzt:

FaaS

Dabei wird eine Funktion ausgeführt, wenn ein Ereignis eintritt.

Beispiele:

Datei wird hochgeladen.
Funktion verarbeitet Datei.
API-Aufruf startet Funktion.

Zeitplan löst Funktion aus.

Merksatz:

FaaS führt einzelne Funktionen ereignisgesteuert aus.

Cloud Storage

Cloud Storage ist Speicherplatz aus der Cloud.

Arten:

Objektspeicher
Blockspeicher
Dateispeicher

Typische Nutzung:

Backups
Dateien
Archivierung
Medien
Logs
Daten für Anwendungen
statische Webseiten

Merksatz:

Cloud Storage stellt Speicher als Dienst bereit.

Objektspeicher

Objektspeicher speichert Daten als Objekte.

Ein Objekt besteht typischerweise aus:

Dateiinhalt
Metadaten

eindeutiger Name oder Schlüssel

Typische Nutzung:

Backups
Bilder
Videos
Dokumente
Archivdaten
Logs

Merksatz:

Objektspeicher ist gut für große Mengen unstrukturierter Daten.

Blockspeicher

Blockspeicher stellt Speicherblöcke bereit, ähnlich wie eine Festplatte für einen Server.

Typische Nutzung:

virtuelle Maschinen
Datenbanken
Betriebssystemplatten
Anwendungen mit Dateisystem

Merksatz:

Blockspeicher verhält sich eher wie eine virtuelle Festplatte.

Dateispeicher

Dateispeicher stellt Dateifreigaben bereit.

Typische Nutzung:

gemeinsame Dateisysteme
Anwendungen mit gemeinsamen Dateien

klassische Freigaben

Benutzerdateien

Merksatz:

Dateispeicher arbeitet mit Ordnern und Dateien.

Cloud-Netzwerke

Cloud-Umgebungen haben eigene Netzwerkstrukturen.

Typische Bestandteile:

virtuelle Netzwerke

Subnetze

Routingtabellen

Security Groups

Network Security Groups

Firewalls

Load Balancer

öffentliche IP-Adressen

private IP-Adressen

NAT-Gateways

VPN-Gateways

Merksatz:

Cloud-Netzwerke müssen genauso geplant werden wie lokale Netzwerke.

Virtuelles Netzwerk

Ein virtuelles Netzwerk ist ein logisch getrenntes Netz in der Cloud.

Es enthält:

Subnetze

virtuelle Maschinen

Dienste

Routing
Sicherheitsregeln

Je nach Anbieter heißt es unterschiedlich, zum Beispiel VPC oder VNet.

Merksatz:

Virtuelles Netzwerk ist das Cloud-Gegenstück zum eigenen Netzsegment.

Subnetze in der Cloud

Cloud-Netze werden in Subnetze aufgeteilt.

Beispiele:

Web-Subnetz
App-Subnetz
Datenbank-Subnetz
Management-Subnetz
Public Subnet
Private Subnet

Merksatz:

Subnetze trennen Cloud-Ressourcen logisch.

Public Subnet

Ein Public Subnet enthält Ressourcen, die direkt oder indirekt mit dem Internet verbunden sein können.

Beispiele:

Load Balancer
Bastion Host
öffentlich erreichbarer Webserver

Wichtig:

Nicht jede Ressource sollte öffentlich erreichbar sein.

Merksatz:

Public Subnet nur für wirklich öffentliche Komponenten nutzen.

Private Subnet

Ein Private Subnet enthält interne Ressourcen.

Beispiele:

Datenbankserver
interne Anwendung
Backend
interne APIs
Verarbeitungssysteme

Diese Ressourcen sind normalerweise nicht direkt aus dem Internet erreichbar.

Merksatz:

Private Subnet schützt interne Cloud-Ressourcen vor direktem Internetzugriff.

Security Group

Eine Security Group ist eine virtuelle Firewall-Regelgruppe für Cloud-Ressourcen.

Sie steuert häufig:

eingehenden Verkehr
ausgehenden Verkehr
Ports
Protokolle
Quellen
Ziele

Merksatz:

Security Group ist eine Firewall-Regelgruppe in der Cloud.

Network Security Group

Network Security Group wird oft abgekürzt:

NSG

Sie steuert Netzwerkverkehr auf Subnetz- oder Ressourcenebene, je nach Cloud-Plattform.

Merksatz:

NSG regelt Netzwerkzugriffe in Cloud-Netzen.

Cloud-Firewall

Eine Cloud-Firewall schützt Cloud-Netze oder Cloud-Dienste.

Sie kann filtern nach:

IP-Adresse
Port
Protokoll
Richtung
Anwendung
Bedrohungssignatur
Zone

Merksatz:

Auch in der Cloud braucht man Firewall-Regeln.

Load Balancer

Ein Load Balancer verteilt Anfragen auf mehrere Ziele.

Ziele können sein:

virtuelle Maschinen

Container

Anwendungen

Backends

Vorteile:

höhere Verfügbarkeit

Lastverteilung

Wartung einzelner Systeme möglich

Skalierung

Merksatz:

Load Balancer verteilt Last auf mehrere Systeme.

Auto Scaling

Auto Scaling bedeutet:

Ressourcen werden automatisch erhöht oder reduziert.

Beispiel:

Bei hoher Last werden mehr Instanzen gestartet.

Bei geringer Last werden Instanzen beendet.

Vorteile:

bessere Anpassung an Last

Kostenkontrolle

höhere Verfügbarkeit

Merksatz:

Auto Scaling passt Ressourcen automatisch an Bedarf an.

Cloud und Hochverfügbarkeit

Cloud kann Hochverfügbarkeit unterstützen.

Möglichkeiten:

- mehrere Verfügbarkeitszonen
- mehrere Regionen
- Load Balancer
- Auto Scaling
- replizierte Daten
- Backup
- Monitoring
- automatische Wiederherstellung

Aber:

Hochverfügbarkeit muss geplant und konfiguriert werden.

Merksatz:

Cloud ist nicht automatisch hochverfügbar.

Verfügbarkeitszone

Eine Verfügbarkeitszone ist ein getrenntes Rechenzentrumssegment innerhalb einer Region.

Ziel:

Ausfall einer Zone soll nicht automatisch alle Dienste betreffen.

Beispiele:

- Zone A
- Zone B
- Zone C

Merksatz:

Verfügbarkeitszonen helfen,
Ausfälle innerhalb einer Region abzufangen.

Region

Eine Region ist ein geografischer Standort eines Cloud-Anbieters.

Beispiele:

Deutschland
Europa
USA
Asien

Regionen sind wichtig für:

Latenz
Datenschutz
Ausfallsicherheit
Kosten
Compliance
Datenstandort

Merksatz:

Region bestimmt,
wo Cloud-Ressourcen geografisch betrieben werden.

Datenstandort

Datenstandort bedeutet:

In welchem Land oder welcher Region Daten gespeichert und verarbeitet werden.

Wichtig wegen:

Datenschutz
rechtlichen Anforderungen
Compliance
Latenz
Kundenanforderungen
Unternehmensrichtlinien

Merksatz:

Datenstandort ist bei Cloud-Diensten sicherheits- und rechtsrelevant.

Cloud-Kosten

Cloud-Kosten entstehen häufig durch:

Rechenleistung
Speicher
Datenübertragung
Datenbanknutzung
Lizenzen
Load Balancer
Backups
Logs
Monitoring
öffentliche IP-Adressen
Support

Wichtig:

Cloud ist flexibel,
aber nicht automatisch günstiger.

Merksatz:

Cloud-Kosten müssen überwacht und geplant werden.

OPEX und CAPEX

CAPEX bedeutet:

Investitionsausgaben

Beispiel:

Server kaufen
Storage kaufen
Netzwerkhardware kaufen

OPEX bedeutet:

Betriebsausgaben

Beispiel:

monatliche Cloud-Nutzung
Mietmodell
nutzungsabhängige Abrechnung

Cloud verschiebt Kosten häufig von CAPEX zu OPEX.

Merksatz:

Cloud macht aus Kaufkosten häufig laufende Nutzungskosten.

Pay as you go

Pay as you go bedeutet:

Man bezahlt nach Nutzung.

Beispiele:

pro Stunde
pro GB
pro Anfrage

pro Benutzer
pro Ausführung
pro übertragenem Datenvolumen

Vorteil:

flexible Abrechnung

Risiko:

unerwartete Kosten bei Fehlkonfiguration oder hoher Nutzung

Merksatz:

Pay as you go ist flexibel,
braucht aber Kostenkontrolle.

Cloud-Sicherheit

Cloud-Sicherheit umfasst:

Identitätsmanagement
MFA
Rollen und Rechte
Netzwerksicherheit
Verschlüsselung
Logging
Monitoring
Backup
Patchmanagement
sichere Konfiguration
Datenklassifizierung
Compliance

Merksatz:

Cloud-Sicherheit ist mehr als Anbieter auswählen.

Identity and Access Management

Identity and Access Management wird oft abgekürzt:

IAM

IAM regelt:

Benutzer
Gruppen
Rollen
Berechtigungen
Servicekonten
API-Schlüssel
MFA
Zugriff auf Ressourcen

Merksatz:

IAM entscheidet,
wer was in der Cloud darf.

Cloud-Rollen

Cloud-Zugriffe sollten über Rollen gesteuert werden.

Beispiele:

Leser
Administrator
Netzwerkadministrator
Sicherheitsadministrator
Datenbankadministrator
Entwickler
Abrechnungszugriff

Merksatz:

Rollen helfen,
Cloud-Rechte nach Aufgabe zu vergeben.

Least Privilege in der Cloud

Auch in der Cloud gilt:

so wenig Rechte wie möglich,
so viele wie nötig.

Nicht gut:

alle Benutzer sind Administratoren
API-Schlüssel mit Vollzugriff
öffentliche Speichercontainer
Datenbank öffentlich erreichbar
Managementport offen im Internet

Merksatz:

Least Privilege ist in der Cloud besonders wichtig.

Cloud-Fehlkonfigurationen

Viele Cloud-Sicherheitsvorfälle entstehen durch Fehlkonfigurationen.

Beispiele:

Speicher öffentlich lesbar
Datenbank öffentlich erreichbar
zu breite Security Group
Adminrechte für zu viele Benutzer
fehlende MFA
offene Managementports
unverschlüsselte Daten
keine Logs
keine Kostenlimits

Merksatz:

Cloud-Fehler entstehen häufig durch falsche Konfiguration,
nicht durch defekte Technik.

Cloud-Logging

Cloud-Logs zeigen:

Anmeldungen
API-Aufrufe
Änderungen an Ressourcen
Netzwerkzugriffe
Firewall-Entscheidungen
Fehlermeldungen
Sicherheitsereignisse
Abrechnungsereignisse

Wichtig:

Logs aktivieren
Logs schützen
Logs zentral auswerten
Aufbewahrung regeln

Merksatz:

Cloud-Logs zeigen,
wer was wann geändert hat.

Cloud-Monitoring

Cloud-Monitoring überwacht:

Verfügbarkeit
CPU
RAM

Speicher
Datenbanklast
Netzwerkverkehr
Fehlerquoten
Antwortzeiten
Kosten
Zertifikate
Sicherheitsereignisse

Merksatz:

Cloud-Monitoring ist für Betrieb,
Sicherheit
und Kostenkontrolle wichtig.

Backup in der Cloud

Cloud-Dienste brauchen Backup-Konzepte.

Wichtig:

Was wird gesichert?
Wie oft?
Wie lange?
Wo wird gespeichert?
Wer darf wiederherstellen?
Wurde Wiederherstellung getestet?
Ist Backup vor Löschung oder Ransomware geschützt?

Merksatz:

Cloud ersetzt nicht automatisch Backup.

Cloud und Datenschutz

Bei Cloud-Diensten müssen Datenschutzanforderungen beachtet werden.

Wichtige Fragen:

Welche Daten werden verarbeitet?
Wo werden Daten gespeichert?
Wer hat Zugriff?
Gibt es Auftragsverarbeitung?
Sind Daten verschlüsselt?
Gibt es Löschkonzepte?
Werden Logs personenbezogen?
Welche Anbieterbedingungen gelten?

Merksatz:

Cloud-Nutzung braucht Datenschutzprüfung.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was bedeutet Cloud Computing?
- Was ist der Unterschied zwischen On-Premises und Cloud?
- Was ist Public Cloud?
- Was ist Private Cloud?
- Was ist Hybrid Cloud?
- Was ist Multi Cloud?
- Was bedeutet IaaS?
- Was bedeutet PaaS?
- Was bedeutet SaaS?
- Was ist das Shared Responsibility Model?
- Wer ist bei einer Cloud-VM für Betriebssystemupdates verantwortlich?
- Was ist Serverless?
- Was ist Auto Scaling?
- Was ist ein Load Balancer?
- Warum ist IAM in der Cloud wichtig?
- Warum ist Cloud nicht automatisch sicher?
- Warum ist Cloud nicht automatisch günstiger?
- Warum braucht Cloud Backup und Monitoring?

Typische Prüfungsfallen

Cloud bedeutet nicht automatisch Internetseite.

Cloud bedeutet nicht automatisch weniger Verantwortung.

On-Premises ist lokal selbst betrieben.

Public Cloud ist Anbieterplattform für viele Kunden.

Private Cloud ist Cloud-Prinzip für eine Organisation.

Hybrid Cloud kombiniert lokal und Cloud.

Multi Cloud nutzt mehrere Anbieter.

IaaS ist virtuelle Infrastruktur.

PaaS ist Plattform für Anwendungen.

SaaS ist fertige Software.

Shared Responsibility bedeutet geteilte Verantwortung.

Cloud-VM muss der Kunde oft selbst patchen.

SaaS-Benutzerrechte bleiben Kundenthema.

Serverless heißt nicht serverfrei.

Cloud ist nicht automatisch hochverfügbar.

Cloud ist nicht automatisch günstiger.

Pay as you go braucht Kostenkontrolle.

IAM ist zentral für Cloud-Sicherheit.

Öffentliche Speicherfreigaben sind gefährlich.

Cloud braucht Backup,

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Cloud	IT-Ressourcen als Dienst
On-Premises	lokal selbst betrieben
Public Cloud	öffentliche Anbieterplattform
Private Cloud	Cloud für eine Organisation
Hybrid Cloud	Mischung aus lokal und Cloud
Multi Cloud	mehrere Cloud-Anbieter
Community Cloud	Cloud für bestimmte Gruppe
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
Shared Responsibility	geteilte Verantwortung
Virtualisierung	Aufteilen physischer Ressourcen
Container	portable Anwendungseinheit
Orchestrierung	automatische Verwaltung vieler Dienste
Kubernetes	Container-Orchestrierung
Serverless	keine Serververwaltung durch Kunden
FaaS	Function as a Service
Cloud Storage	Speicher aus der Cloud
Objektspeicher	Speicher für Objekte mit Metadaten
Blockspeicher	virtuelle Festplatte
Dateispeicher	Dateifreigabe als Dienst
VPC / VNet	virtuelles Cloud-Netz
Public Subnet	öffentlich angebundenes Subnetz
Private Subnet	internes Cloud-Subnetz
Security Group	virtuelle Firewall-Regelgruppe
Load Balancer	verteilt Anfragen
Auto Scaling	automatische Skalierung

Begriff	Kurze Erklärung
Region	geografischer Cloud-Standort
Verfügbarkeitszone	getrennte Zone innerhalb Region
IAM	Identitäts- und Rechteverwaltung
CAPEX	Investitionsausgaben
OPEX	Betriebsausgaben

IHK-sichere Kurzformulierung

Cloud Computing bedeutet, dass IT-Ressourcen wie Rechenleistung, Speicher, Datenbanken, Plattformen oder Anwendungen über ein Netzwerk als Dienst bereitgestellt werden. Bei On-Premises betreibt ein Unternehmen seine IT lokal selbst, während Public Cloud von einem Anbieter für viele Kunden bereitgestellt wird. Private Cloud nutzt Cloud-Prinzipien für eine Organisation, Hybrid Cloud kombiniert lokale IT und Cloud, und Multi Cloud nutzt mehrere Anbieter. Die wichtigsten Service-Modelle sind IaaS, PaaS und SaaS. Beim Shared Responsibility Model teilen sich Anbieter und Kunde die Verantwortung. Der Anbieter betreibt je nach Modell Teile der Infrastruktur, der Kunde bleibt aber für Benutzer, Daten, Berechtigungen, sichere Konfiguration, Backup, Monitoring und Compliance verantwortlich.

Merksätze

Cloud = IT-Ressourcen als Dienst.

On-Premises = lokal selbst betrieben.

Public Cloud = Anbieterplattform für viele Kunden.

Private Cloud = Cloud für eine Organisation.

Hybrid Cloud = lokal plus Cloud.

Multi Cloud = mehrere Anbieter.

IaaS = virtuelle Infrastruktur.

PaaS = Plattform für Anwendungen.

SaaS = fertige Software.

Shared Responsibility = geteilte Verantwortung.

Je fertiger der Dienst,
desto mehr Betrieb übernimmt der Anbieter.

Kundendaten und Zugriffe bleiben Kundenthema.

Cloud-VM ist nicht automatisch gepatcht.

SaaS braucht Benutzer- und Rechteverwaltung.

Virtualisierung ist Grundlage vieler Cloud-Dienste.

Container verpacken Anwendungen.

Kubernetes orchestriert Container.

Serverless heißt nicht serverfrei.

FaaS führt Funktionen ereignisgesteuert aus.

Cloud Storage kann Objekt,
Block
oder Datei sein.

Cloud-Netze müssen geplant werden.

Security Groups sind virtuelle Firewall-Regeln.

Load Balancer verteilt Last.

Auto Scaling passt Ressourcen automatisch an.

Cloud ist nicht automatisch hochverfügbar.

Region bestimmt Datenstandort.

Cloud ist nicht automatisch günstiger.

Pay as you go braucht Kostenkontrolle.

IAM ist zentral für Cloud-Sicherheit.

Least Privilege gilt auch in der Cloud.

Cloud-Fehlkonfigurationen sind häufige Risiken.

Cloud braucht Logs,
Monitoring,
Backup
und Datenschutzprüfung.
