

20.10 Trainer - Cloud, Bereitstellungsmodelle, IAM und Shared Responsibility

Diese Trainer-Seite wiederholt Cloud-Grundlagen, Bereitstellungsmodelle, Servicemodelle, Cloud-Netzwerke, IAM, Sicherheit und typische Prüfungsfragen zur Cloud.

Ziel ist, IaaS, PaaS, SaaS, Public Cloud, Private Cloud, Hybrid Cloud, Multi Cloud und Shared Responsibility sicher zu unterscheiden.

Merksatz:

Cloud bedeutet:
IT-Ressourcen werden flexibel über ein Netzwerk bereitgestellt.
Die Verantwortung ist dabei geteilt.

Lernziele

Nach dieser Seite solltest du sicher können:

- Cloud Computing erklären
- IaaS,
PaaS
und SaaS unterscheiden
- Public Cloud,
Private Cloud,
Hybrid Cloud
und Multi Cloud unterscheiden
- Shared Responsibility erklären
- IAM einordnen
- Cloud-Netzwerke grob verstehen
- Security Groups,
VPCs
und Subnetze einordnen
- typische Cloud-Fehlerbilder erkennen
- Cloud-Kosten und Skalierung fachlich erklären

Kurzüberblick

Begriff	Bedeutung
Cloud Computing	Bereitstellung von IT-Ressourcen über ein Netzwerk
IaaS	virtuelle Infrastruktur
PaaS	verwaltete Plattform
SaaS	fertige Software
Public Cloud	Cloud eines öffentlichen Anbieters
Private Cloud	Cloud nur für eine Organisation
Hybrid Cloud	Kombination aus lokal und Cloud
Multi Cloud	Nutzung mehrerer Cloud-Anbieter
IAM	Identitäts- und Zugriffsverwaltung
Shared Responsibility	geteilte Verantwortung zwischen Anbieter und Kunde

Merksatz:

IaaS = Infrastruktur.

PaaS = Plattform.

SaaS = Software.

Aufgabe 1

Was bedeutet Cloud Computing?

Antwort anzeigen

Cloud Computing bedeutet:

IT-Ressourcen werden über ein Netzwerk bereitgestellt
und können flexibel genutzt,
skaliert
und abgerechnet werden.

Beispiele:

virtuelle Server

Speicher

Datenbanken

Anwendungen

Plattformdienste

Netzwerkdienste

Merksatz:

Cloud = IT-Ressourcen flexibel über Netzwerk nutzen.

Aufgabe 2

Nenne typische Vorteile von Cloud Computing.

Antwort anzeigen

Typische Vorteile:

flexible Skalierung

schnelle Bereitstellung

nutzungsabhängige Abrechnung

weniger eigene Hardware

weltweite Verfügbarkeit

verwaltete Dienste

hohe Automatisierbarkeit

schnelle Erweiterbarkeit

Merksatz:

Cloud ist besonders stark bei Flexibilität,
Skalierung
und schneller Bereitstellung.

Aufgabe 3

Nenne typische Nachteile oder Risiken von Cloud Computing.

Antwort anzeigen

Typische Nachteile oder Risiken:

Abhängigkeit vom Anbieter

Datenschutzanforderungen

falsche Konfigurationen

Kostenkontrolle notwendig

Netzwerkabhängigkeit

Vendor Lock-in

geteilte Verantwortung kann missverstanden werden

Zugriffsschutz muss sauber geplant werden

Merksatz:

Cloud nimmt Arbeit ab,
aber nicht die Verantwortung für sichere Nutzung.

Aufgabe 4

Was ist IaaS?

Antwort anzeigen

IaaS steht für:

Infrastructure as a Service

Bedeutung:

Der Anbieter stellt grundlegende Infrastruktur bereit.

Beispiele:

virtuelle Maschinen

virtuelle Netzwerke

Speicher

Firewalls

Load Balancer

Der Kunde verwaltet häufig selbst:

Betriebssystem

Anwendungen

Patches im Gastbetriebssystem

Konfiguration

Merksatz:

IaaS = virtuelle Infrastruktur.

Aufgabe 5

Was ist PaaS?

Antwort anzeigen

PaaS steht für:

Platform as a Service

Bedeutung:

Der Anbieter stellt eine verwaltete Plattform für Anwendungen bereit.

Beispiele:

App-Plattform

verwaltete Datenbank

Laufzeitumgebung

Containerplattform

Entwicklungsplattform

Der Kunde kümmert sich eher um:

Anwendung

Daten

Konfiguration

Zugriffsrechte

Merksatz:

PaaS = Plattform für Anwendungen.

Aufgabe 6

Was ist SaaS?

Antwort anzeigen

SaaS steht für:

Software as a Service

Bedeutung:

Der Anbieter stellt eine fertige Anwendung bereit,
die der Kunde nutzt.

Beispiele:

E-Mail-Dienst

Office-Anwendung im Browser

CRM-System

Ticketsystem

Cloud-Speicheranwendung

Der Kunde verwaltet meist:

Benutzer

Rollen

Daten

Einstellungen

Zugriffsrechte

Merksatz:

SaaS = fertige Software nutzen.

Aufgabe 7

Ordne zu.

Modell	Bedeutung
IaaS	?
PaaS	?
SaaS	?

Antwort anzeigen

Modell	Bedeutung
IaaS	virtuelle Infrastruktur
PaaS	verwaltete Plattform
SaaS	fertige Anwendung

Merksatz:

IaaS unten,
PaaS in der Mitte,
SaaS oben.

Aufgabe 8

Welche Aussage passt zu IaaS?

A: Fertige Anwendung im Browser

B: Virtuelle Maschine mit eigenem Betriebssystem

C: Nur E-Mail-Postfach ohne Serververwaltung

D: Kein Netzwerk notwendig

Antwort anzeigen

Richtig ist:

B: Virtuelle Maschine mit eigenem Betriebssystem

Begründung:

IaaS stellt Infrastruktur bereit,
zum Beispiel virtuelle Maschinen,
Speicher
und Netzwerke.
Das Betriebssystem und Anwendungen werden oft vom Kunden verwaltet.

Merksatz:

Virtuelle Maschine = typisches IaaS-Beispiel.

Aufgabe 9

Welche Aussage passt zu SaaS?

A: Der Kunde installiert und patcht das Betriebssystem selbst.

B: Der Kunde nutzt eine fertige Anwendung.

C: Der Kunde baut ein eigenes Rechenzentrum.

D: Der Kunde verwaltet die Hardware des Anbieters.

Antwort anzeigen

Richtig ist:

B: Der Kunde nutzt eine fertige Anwendung.

Begründung:

SaaS bedeutet,
dass eine fertige Software als Dienst bereitgestellt wird.

Merksatz:

SaaS = benutzen statt betreiben.

Aufgabe 10

Was ist der Unterschied zwischen IaaS, PaaS und SaaS?

Antwort anzeigen

IaaS:

virtuelle Infrastruktur,
viel Verantwortung beim Kunden

PaaS:

verwaltete Plattform,
Kunde bringt Anwendung und Daten

SaaS:

fertige Anwendung,
Kunde verwaltet hauptsächlich Nutzung,
Daten,
Benutzer
und Rechte

Merksatz:

Je mehr Richtung SaaS,
desto mehr übernimmt der Anbieter.

Aufgabe 11

Was ist Public Cloud?

Antwort anzeigen

Public Cloud bedeutet:

Cloud-Ressourcen werden von einem öffentlichen Cloud-Anbieter bereitgestellt
und von vielen Kunden getrennt genutzt.

Eigenschaften:

hohe Skalierbarkeit

nutzungsabhängige Abrechnung

Anbieter betreibt Infrastruktur

Mandantentrennung wichtig

Merksatz:

Public Cloud = Cloud eines öffentlichen Anbieters.

Aufgabe 12

Was ist Private Cloud?

Antwort anzeigen

Private Cloud bedeutet:

Cloud-Umgebung wird nur für eine Organisation betrieben.

Möglich:

im eigenen Rechenzentrum

bei einem Dienstleister

dediziert für eine Organisation

Vorteile:

mehr Kontrolle

individuelle Anpassung

besondere Compliance-Anforderungen leichter steuerbar

Merksatz:

Private Cloud = Cloud nur für eine Organisation.

Aufgabe 13

Was ist Hybrid Cloud?

Antwort anzeigen

Hybrid Cloud bedeutet:

lokale IT oder Private Cloud wird mit Public-Cloud-Ressourcen kombiniert.

Beispiele:

lokales Rechenzentrum plus Cloud-Backup

lokale Anwendung plus Cloud-Datenbank

lokales Firmennetz plus Cloud-VPC über VPN

Merksatz:

Hybrid Cloud = lokal und Cloud kombiniert.

Aufgabe 14

Was ist Multi Cloud?

Antwort anzeigen

Multi Cloud bedeutet:

Eine Organisation nutzt mehrere Cloud-Anbieter.

Beispiel:

Anbieter A für Infrastruktur

Anbieter B für Datenanalyse

Anbieter C für Office-Dienste

Gründe:

Vermeidung von Abhängigkeit

passende Dienste verschiedener Anbieter nutzen

Ausfallsicherheit

Kostenoptimierung

Merksatz:

Multi Cloud = mehrere Cloud-Anbieter.

Aufgabe 15

Ordne zu.

Modell	Bedeutung
Public Cloud	?
Private Cloud	?
Hybrid Cloud	?
Multi Cloud	?

Antwort anzeigen

Modell	Bedeutung
Public Cloud	Cloud eines öffentlichen Anbieters
Private Cloud	Cloud nur für eine Organisation
Hybrid Cloud	Kombination aus lokal oder privat und Public Cloud
Multi Cloud	Nutzung mehrerer Cloud-Anbieter

Merksatz:

Hybrid beschreibt Kombination von Umgebungen.

Multi beschreibt mehrere Anbieter.

Aufgabe 16

Was bedeutet Shared Responsibility?

Antwort anzeigen

Shared Responsibility bedeutet:

Cloud-Anbieter und Kunde teilen sich die Verantwortung für Sicherheit und Betrieb.

Der Anbieter ist typischerweise verantwortlich für:

physische Infrastruktur

Rechenzentrum

Grundplattform

Hardware

Der Kunde ist typischerweise verantwortlich für:

Daten

Benutzer

Berechtigungen

Konfigurationen

Anwendungen je nach Modell

Merksatz:

Cloud-Sicherheit ist geteilte Verantwortung.

Aufgabe 17

Warum ist Shared Responsibility wichtig?

Antwort anzeigen

Shared Responsibility ist wichtig, weil Kunden oft fälschlich glauben, der Cloud-Anbieter sei für alles verantwortlich.

In Wirklichkeit bleiben viele Aufgaben beim Kunden, zum Beispiel:

Benutzerrechte

Datenklassifizierung

Zugriffsschutz

sichere Konfiguration

Backup

Verschlüsselung

Monitoring

Merksatz:

Cloud-Anbieter schützt die Cloud.

Kunde schützt seine Nutzung der Cloud.

Aufgabe 18

Wer ist bei SaaS typischerweise für Benutzer und Rechte verantwortlich?

Antwort anzeigen

Typischerweise:

der Kunde

Begründung:

Auch wenn der Anbieter die Anwendung betreibt,
muss der Kunde seine Benutzer,
Gruppen,
Rollen,
Daten
und Freigaben korrekt verwalten.

Merksatz:

SaaS nimmt Betrieb ab,
aber nicht Rechteverwaltung.

Aufgabe 19

Wer ist bei IaaS typischerweise für das Gastbetriebssystem verantwortlich?

Antwort anzeigen

Typischerweise:

der Kunde

Begründung:

Bei IaaS stellt der Anbieter die virtuelle Infrastruktur bereit.
Betriebssystem,
Patches,
Dienste
und Anwendungen in der virtuellen Maschine werden häufig vom Kunden verwaltet.

Merksatz:

IaaS bedeutet mehr Kundenverantwortung als SaaS.

Aufgabe 20

Was ist IAM?

Antwort anzeigen

IAM steht für:

Identity and Access Management

Bedeutung:

Verwaltung von Identitäten,
Rollen,
Rechten
und Zugriffen.

Typische Aufgaben:

Benutzer verwalten

Rollen definieren

Berechtigungen vergeben

MFA erzwingen

Service Accounts verwalten

Zugriff protokollieren

Merksatz:

IAM entscheidet,
wer was darf.

Aufgabe 21

Warum ist IAM in der Cloud besonders wichtig?

Antwort anzeigen

Cloud-Ressourcen sind oft über das Internet erreichbar und können schnell erstellt, geändert oder gelöscht werden.

Fehlerhafte Berechtigungen können zu:

Datenabfluss

Missbrauch von Ressourcen

Kostenexplosion

unberechtigtem Zugriff

Manipulation

führen.

Merksatz:

In der Cloud sind Identitäten oft der wichtigste Sicherheitsperimeter.

Aufgabe 22

Was bedeutet Least Privilege im Cloud-Kontext?

Antwort anzeigen

Least Privilege bedeutet:

Benutzer,

Rollen,

Dienste

und Anwendungen erhalten nur die Berechtigungen,
die sie wirklich benötigen.

Beispiele:

Entwickler darf Logs lesen,
aber keine Produktionsdatenbank löschen.

Anwendung darf in einen Speicher schreiben,
aber keine Benutzer verwalten.

Dienstkonto darf nur auf benötigte Ressourcen zugreifen.

Merksatz:

In der Cloud keine pauschalen Adminrechte vergeben.

Aufgabe 23

Was ist MFA im Cloud-Kontext?

Antwort anzeigen

MFA steht für:

Multi-Faktor-Authentifizierung

Bedeutung:

Anmeldung benötigt mehr als nur ein Passwort.

Beispiele für Faktoren:

Wissen:
Passwort

Besitz:
Smartphone,
Token,

Smartcard

Sein:

biometrisches Merkmal

Merksatz:

MFA schützt Cloud-Konten gegen Passwortmissbrauch.

Aufgabe 24

Was ist ein Service Account?

Antwort anzeigen

Ein Service Account ist ein Konto, das von Diensten, Anwendungen oder Automatisierungen genutzt wird.

Risiken:

zu viele Rechte

Schlüssel liegen unsicher

Zugriff wird nicht überwacht

Konto wird nach Projektende nicht entfernt

Schutzmaßnahmen:

Least Privilege

Schlüsselrotation

kurze Laufzeiten

Logging

keine geteilten Geheimnisse im Klartext

Merksatz:

Service Accounts brauchen besonders saubere Rechteverwaltung.

Aufgabe 25

Was ist eine VPC?

Antwort anzeigen

VPC steht für:

Virtual Private Cloud

Bedeutung:

logisch getrenntes virtuelles Netzwerk in einer Cloud-Umgebung.

Typische Bestandteile:

Subnetze

Routing-Tabellen

Security Groups

Gateways

Firewalls

VPN-Anbindungen

Merksatz:

VPC = virtuelles Cloud-Netzwerk.

Aufgabe 26

Was ist ein Cloud-Subnetz?

Antwort anzeigen

Ein Cloud-Subnetz ist ein IP-Adressbereich innerhalb eines virtuellen Cloud-Netzwerks.

Typische Unterscheidung:

öffentliches Subnetz

privates Subnetz

Öffentliches Subnetz:

Ressourcen können über passende Regeln und öffentliche Adresse aus dem Internet erreichbar sein.

Privates Subnetz:

Ressourcen sind nicht direkt öffentlich erreichbar.

Merksatz:

Subnetze strukturieren Cloud-Netzwerke.

Aufgabe 27

Was ist eine Security Group?

Antwort anzeigen

Eine Security Group ist eine regelbasierte Zugriffskontrolle für Cloud-Ressourcen.

Sie steuert typischerweise:

eingehenden Verkehr

ausgehenden Verkehr

Ports

Protokolle

Quellen

Ziele

Merksatz:

Security Group ist wie eine ressourcennahe Firewall-Regelgruppe.

Aufgabe 28

Was ist der Unterschied zwischen Security Group und klassischer Netzwerkfirewall?

Antwort anzeigen

Security Group:

häufig direkt an Cloud-Ressourcen gebunden

regelt Zugriff auf einzelne Ressourcen oder Gruppen

Klassische Firewall:

oft zentrale Netzwerkkomponente oder Appliance

kontrolliert Verkehr zwischen Netzen oder Zonen

Wichtig:

Beide kontrollieren Verkehr,
aber an unterschiedlichen Stellen.

Merksatz:

Security Groups sind Cloud-nahe Zugriffskontrolle.

Aufgabe 29

Warum sollte eine Cloud-Datenbank nicht öffentlich erreichbar sein?

Antwort anzeigen

Eine Datenbank enthält oft sensible Daten und ist ein attraktives Angriffsziel.

Risiken:

Brute Force

Exploits

Datenabfluss

Manipulation

Kosten oder Last durch Missbrauch

Besser:

privates Subnetz

Zugriff nur von Anwendungsservern

Security Group einschränken

starke Authentifizierung

Verschlüsselung

Logging

Merksatz:

Datenbanken nicht öffentlich freigeben.

Aufgabe 30

Was bedeutet Skalierung?

Antwort anzeigen

Skalierung bedeutet:

Ressourcen werden an Bedarf angepasst.

Vertikale Skalierung:

eine Ressource wird größer gemacht

Beispiel:

mehr CPU oder RAM für eine VM

Horizontale Skalierung:

mehrere Instanzen werden hinzugefügt

Beispiel:

mehrere Webserver hinter einem Load Balancer

Merksatz:

Vertikal = größer.

Horizontal = mehr.

Aufgabe 31

Was ist Auto Scaling?

Antwort anzeigen

Auto Scaling bedeutet:

Ressourcen werden automatisch erhöht oder reduziert,
abhängig von definierten Bedingungen.

Beispiele:

CPU-Auslastung hoch:
zusätzliche Instanz starten

Last niedrig:
Instanz entfernen

Vorteile:

bessere Verfügbarkeit

flexible Leistung

Kostenkontrolle bei richtiger Konfiguration

Merksatz:

Auto Scaling passt Ressourcen automatisch an Last an.

Aufgabe 32

Was ist ein Load Balancer?

Antwort anzeigen

Ein Load Balancer verteilt Anfragen auf mehrere Ziele.

Beispiele:

mehrere Webserver

mehrere Anwendungsserver

Vorteile:

bessere Verfügbarkeit

Lastverteilung

Wartung einzelner Instanzen leichter möglich

Skalierung

Merksatz:

Load Balancer verteilt Verkehr.

Aufgabe 33

Was bedeutet Cloud-Kostenkontrolle?

Antwort anzeigen

Cloud-Kostenkontrolle bedeutet:

Nutzung,
Ressourcen
Speicher
Datenverkehr
Lizenzen
und laufende Dienste überwachen.

Maßnahmen:

Budgets

Alarme

Tags

Abschalten ungenutzter Ressourcen

passende Größen wählen

Reservierungen oder Pläne prüfen

Speicherklassen nutzen

Merksatz:

Cloud ist flexibel,
aber nicht automatisch günstig.

Aufgabe 34

Warum sind Tags in der Cloud nützlich?

Antwort anzeigen

Tags sind Metadaten an Ressourcen.

Nutzung:

Kostenstellen zuordnen

Besitzer erkennen

Umgebung kennzeichnen

Projektzuordnung

Automatisierung

Compliance

Beispiele:

Projekt = Webshop

Umgebung = Produktion

Besitzer = IT-Team

Merksatz:

Tags helfen bei Ordnung,
Kosten
und Automatisierung.

Aufgabe 35

Was ist Vendor Lock-in?

Antwort anzeigen

Vendor Lock-in bedeutet:

starke Abhängigkeit von einem Anbieter,
weil Dienste,
Schnittstellen
oder Datenformate schwer wechselbar sind.

Risiken:

Wechsel wird teuer

Migration wird schwierig

Preiserhöhungen schwer vermeidbar

technische Abhängigkeiten

Merksatz:

Vendor Lock-in erschwert Anbieterwechsel.

Aufgabe 36

Was ist ein Cloud-Backup?

Antwort anzeigen

Cloud-Backup bedeutet:

Daten oder Systeme werden in einer Cloud-Umgebung gesichert.

Wichtig:

Zugriffsschutz

Verschlüsselung

Retention

Restore-Test

Schutz gegen Ransomware

regionale Speicherung

Kosten

Merksatz:

Auch Cloud-Backups müssen getestet und geschützt werden.

Aufgabe 37

Warum ersetzt Cloud-Synchronisation kein Backup?

Antwort anzeigen

Synchronisation gleicht Datenstände ab.

Problem:

Löschungen

Verschlüsselung durch Ransomware

Fehländerungen

beschädigte Dateien

können nicht synchronisiert werden.

Backup braucht:

alte Versionen

Retention

Restore-Möglichkeit

Schutz vor Manipulation

Merksatz:

Sync hält gleich.

Backup stellt alte Stände wieder her.

Aufgabe 38

Welche Antwort ist besser?

Aufgabe:

Wer ist in der Cloud für Sicherheit verantwortlich?

Antwort A:

Nur der Cloud-Anbieter.

Antwort B:

Die Verantwortung ist geteilt.
Der Anbieter schützt die Cloud-Infrastruktur,
der Kunde bleibt je nach Modell für Daten,
Benutzer,
Rechte,
Konfigurationen
und Anwendungen verantwortlich.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort beschreibt das Shared-Responsibility-Modell korrekt.

Merksatz:

Cloud-Sicherheit ist geteilte Verantwortung.

Aufgabe 39

Welche Antwort ist besser?

Aufgabe:

Warum ist eine öffentlich erreichbare Cloud-Datenbank kritisch?

Antwort A:

Weil Datenbanken wichtig sind.

Antwort B:

Eine öffentlich erreichbare Datenbank erhöht die Angriffsfläche erheblich.

Es drohen Brute-Force-Angriffe,

Ausnutzung von Schwachstellen,

Datenabfluss

und Manipulation.

Besser ist der Betrieb in einem privaten Subnetz mit Zugriff nur durch benötigte Anwendungen.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort nennt konkrete Risiken
und eine bessere Schutzmaßnahme.

Merksatz:

Sicherheitsantwort:
Risiko,
Maßnahme,
Wirkung.

Aufgabe 40

Welche Antwort ist besser?

Aufgabe:

Was ist der Unterschied zwischen IaaS und SaaS?

Antwort A:

SaaS ist irgendwie mehr fertig.

Antwort B:

Bei IaaS stellt der Anbieter virtuelle Infrastruktur bereit,
zum Beispiel virtuelle Maschinen,
Speicher
und Netzwerke.
Der Kunde verwaltet häufig Betriebssystem und Anwendung.
Bei SaaS nutzt der Kunde eine fertige Anwendung
und verwaltet hauptsächlich Benutzer,
Daten,
Rechte
und Einstellungen.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort grenzt beide Modelle fachlich sauber voneinander ab.

Merksatz:

Modelle immer über Verantwortlichkeit und Bereitstellung erklären.

Mini-Prüfung: schnelle Zuordnung

Frage	Antwort
Was bedeutet IaaS?	Infrastructure as a Service
Was bedeutet PaaS?	Platform as a Service
Was bedeutet SaaS?	Software as a Service
Was ist IaaS?	virtuelle Infrastruktur
Was ist PaaS?	verwaltete Plattform
Was ist SaaS?	fertige Anwendung
Was ist Public Cloud?	Cloud eines öffentlichen Anbieters
Was ist Private Cloud?	Cloud nur für eine Organisation
Was ist Hybrid Cloud?	lokal oder privat plus Public Cloud
Was ist Multi Cloud?	mehrere Cloud-Anbieter
Was ist IAM?	Identitäts- und Zugriffsverwaltung
Was ist VPC?	virtuelles Cloud-Netzwerk
Was ist Security Group?	ressourcennahe Firewall-Regelgruppe
Was ist Auto Scaling?	automatische Anpassung von Ressourcen
Was ist Vendor Lock-in?	starke Anbieterabhängigkeit

Mini-Prüfung: Fehlerbild erkennen

Fehlerbild	Wahrscheinliches Thema
------------	------------------------

Benutzer sieht zu viele Cloud-Ressourcen	IAM / Rechte zu breit
Cloud-Datenbank öffentlich erreichbar	Security Group oder Netzwerk falsch
Kosten steigen unerwartet	Kostenkontrolle, ungenutzte Ressourcen
Anwendung langsam bei Lastspitzen	Skalierung oder Load Balancer prüfen
VM nicht erreichbar	Security Group, Route, Subnetz, Firewall
SaaS-Dateien falsch geteilt	Freigaben und Berechtigungen prüfen
Cloud-Backup nicht wiederherstellbar	Restore-Test fehlt
gelöschte Datei verschwindet überall	Sync statt Backup
Anbieterwechsel sehr schwierig	Vendor Lock-in
Cloud-Ressource ohne Besitzer	fehlende Tags oder Dokumentation

IHK-sichere Kurzformulierung

Cloud Computing bezeichnet die Bereitstellung von IT-Ressourcen über ein Netzwerk. Bei IaaS stellt der Anbieter virtuelle Infrastruktur wie Server, Speicher und Netzwerke bereit. Bei PaaS nutzt der Kunde eine verwaltete Plattform für Anwendungen. Bei SaaS wird eine fertige Anwendung bereitgestellt. Public Cloud ist die Cloud eines öffentlichen Anbieters, Private Cloud eine Cloud für eine Organisation, Hybrid Cloud kombiniert lokale oder private IT mit Public Cloud und Multi Cloud nutzt mehrere Anbieter. Beim Shared-Responsibility-Modell teilen sich Anbieter und Kunde die Verantwortung: Der Anbieter schützt die Cloud-Infrastruktur, der Kunde bleibt je nach Modell für Daten, Identitäten, Rechte, Konfigurationen und Anwendungen verantwortlich.

Merksätze

Cloud = IT-Ressourcen über Netzwerk.

Cloud ist flexibel,
aber nicht automatisch sicher.

Cloud ist flexibel,
aber nicht automatisch günstig.

IaaS = Infrastruktur.

PaaS = Plattform.

SaaS = Software.

Virtuelle Maschine ist typisch IaaS.

Verwaltete Plattform ist typisch PaaS.

Fertige Anwendung ist typisch SaaS.

Public Cloud = öffentlicher Anbieter.

Private Cloud = nur für eine Organisation.

Hybrid Cloud = lokal oder privat plus Cloud.

Multi Cloud = mehrere Anbieter.

Hybrid beschreibt Kombination von Umgebungen.

Multi beschreibt mehrere Anbieter.

Shared Responsibility = geteilte Verantwortung.

Anbieter schützt die Cloud.

Kunde schützt seine Nutzung der Cloud.

IAM entscheidet,
wer was darf.

Cloud-Identitäten sind besonders wichtig.

MFA schützt Cloud-Konten.

Least Privilege gilt auch in der Cloud.

Service Accounts brauchen minimale Rechte.

VPC = virtuelles Cloud-Netzwerk.

Subnetze strukturieren Cloud-Netze.

Security Groups kontrollieren Zugriff.

Datenbanken nicht öffentlich freigeben.

Vertikal skalieren = größer machen.

Horizontal skalieren = mehr Instanzen.

Auto Scaling passt Ressourcen automatisch an.

Load Balancer verteilt Verkehr.

Tags helfen bei Kosten,
Ordnung
und Automatisierung.

Vendor Lock-in erschwert Anbieterwechsel.

Cloud-Sync ist kein Backup.

Auch Cloud-Backups brauchen Restore-Tests.
