15.5 Cloud-Sicherheit, IAM und Shared Responsibility

Cloud-Sicherheit bedeutet nicht nur, dass der Cloud-Anbieter sichere Rechenzentren betreibt.

Cloud-Sicherheit umfasst auch:

- Identitäten
- Benutzerkonten
- Rollen
- Berechtigungen
- MFA
- Netzwerksicherheit
- Verschlüsselung
- Logging
- Monitoring
- Backup
- sichere Konfiguration
- Datenschutz
- Compliance

Merksatz:

Cloud-Sicherheit ist gemeinsame Verantwortung von Anbieter und Kunde.

Warum Cloud-Sicherheit wichtig ist

Cloud-Ressourcen sind oft schnell erstellt und über Netzwerke erreichbar.

Dadurch entstehen typische Risiken:

zu breite Berechtigungen
öffentliche Speicherfreigaben
offene Managementports
fehlende MFA
falsch konfigurierte Security Groups
öffentliche Datenbanken

ungeschützte API-Schlüssel
fehlende Logs
keine Kostenkontrolle
falscher Datenstandort

Merksatz:

In der Cloud entstehen viele Risiken durch Fehlkonfiguration.

Shared Responsibility Model

Shared Responsibility Model bedeutet:

Anbieter und Kunde teilen sich die Verantwortung.

Der Anbieter ist je nach Dienst verantwortlich für:

Rechenzentrum
physische Sicherheit
Hardware
Grundinfrastruktur
Plattformbetrieb
Verfügbarkeit der angebotenen Dienste

Der Kunde bleibt je nach Dienst verantwortlich für:

Benutzer
Rollen
Daten
Berechtigungen
sichere Konfiguration
Netzwerkfreigaben
Anwendungssicherheit
Backup-Konzept
Compliance

Merksatz:

Cloud bedeutet geteilte Verantwortung,
nicht abgegebene Verantwortung.

Verantwortung hängt vom Service-Modell ab

Die Verantwortung ist bei IaaS, PaaS und SaaS unterschiedlich verteilt.

Bereich	IaaS	PaaS	SaaS
physisches Rechenzentrum	Anbieter	Anbieter	Anbieter
Hardware	Anbieter	Anbieter	Anbieter
Virtualisierung	Anbieter	Anbieter	Anbieter
Betriebssystem	Kunde	Anbieter	Anbieter
Anwendung	Kunde	Kunde	Anbieter
Daten	Kunde	Kunde	Kunde
Benutzer und Rechte	Kunde	Kunde	Kunde
sichere Konfiguration	Kunde	Kunde	Kunde

Merksatz:

Daten,
Benutzer
und Rechte bleiben fast immer Kundenthema.

Cloud-Irrtum: Anbieter macht alles sicher

Falsch:

Der Anbieter betreibt die Cloud,
also ist automatisch alles sicher.

Richtig:

Der Anbieter schützt die Plattform.
Der Kunde muss seine Nutzung sicher konfigurieren.

Beispiel:

```
Wenn ein Kunde einen Speicher öffentlich freigibt,
ist das meist ein Konfigurationsfehler des Kunden.
```

Merksatz:

```
Sichere Plattform plus falsche Konfiguration bleibt unsicher.
```

IAM

IAM steht für:

```
Identity and Access Management
```

IAM regelt, wer auf welche Cloud-Ressourcen zugreifen darf.

IAM umfasst:

```
Benutzer
Gruppen
Rollen
Berechtigungen
Richtlinien
Servicekonten
API-Schlüssel
MFA
Zugriffsprotokolle
```

Merksatz:

```
IAM entscheidet,
wer was in der Cloud darf.
```

Identität

Eine Identität ist ein Konto oder Objekt, das Zugriff erhalten kann.

Beispiele:

```
Benutzerkonto
Administrator
Entwickler
Servicekonto
Anwendung
virtuelle Maschine
Containerdienst
Automatisierungsskript
```

Merksatz:

```
Nicht nur Menschen,
auch Dienste können Identitäten haben.
```

Benutzer

Ein Benutzer ist eine menschliche Identität.

Beispiele:

```
Administrator
Entwickler
Supportmitarbeiter
Fachbereich
externer Dienstleister
```

Benutzer sollten:

```
eindeutig zugeordnet sein
keine Sammelkonten nutzen
MFA verwenden
nur notwendige Rechte erhalten
bei Austritt deaktiviert werden
```

Merksatz:

```
Jeder Benutzer braucht ein eigenes Konto.
```

Gruppen

Gruppen fassen Benutzer zusammen.

Beispiel:

```
Cloud-Admins
Entwickler
Leser
Sicherheitsprüfer
Datenbankadministratoren
Netzwerkadministratoren
```

Vorteil:

```
Rechte werden nicht einzeln pro Benutzer vergeben,
sondern über Gruppen verwaltet.
```

Merksatz:

```
Gruppen vereinfachen Rechteverwaltung.
```

Rollen

Eine Rolle beschreibt, welche Aufgaben und Berechtigungen eine Identität hat.

Beispiele:

```
Leser
Administrator
Netzwerkadministrator
Sicherheitsadministrator
Datenbankadministrator
Abrechnungsadministrator
Backup-Operator
```

Merksatz:

```
Rollen ordnen Rechte nach Aufgabe.
```

Berechtigungen

Berechtigungen legen fest, was erlaubt ist.

Beispiele:

```
virtuelle Maschine starten
virtuelle Maschine löschen
Speicher lesen
Speicher schreiben
Firewall-Regel ändern
Benutzer anlegen
Logs anzeigen
Backup wiederherstellen
```

Merksatz:

```
Berechtigungen sind konkrete Erlaubnisse.
```

Richtlinien

Richtlinien beschreiben, welche Berechtigungen gelten.

Sie können festlegen:

```
wer etwas darf
was erlaubt ist
auf welche Ressource es gilt
unter welchen Bedingungen es gilt
was verboten ist
```

Merksatz:

```
Richtlinien verbinden Identitäten,
Aktionen
und Ressourcen.
```

Least Privilege

Least Privilege bedeutet:

```
nur so viele Rechte wie nötig,
so wenige wie möglich.
```

In der Cloud ist das besonders wichtig, weil viele Aktionen große Auswirkungen haben können.

Beispiele für riskante Rechte:

```
alle Ressourcen löschen
Firewall-Regeln ändern
Speicher öffentlich freigeben
Benutzerrechte vergeben
API-Schlüssel erstellen
Backups löschen
```

Merksatz:

```
Cloud-Rechte immer minimal vergeben.
```

Need to Know

Need to Know bedeutet:

```
Zugriff nur auf Daten oder Systeme,
die für die Aufgabe benötigt werden.
```

Beispiel:

```
Entwickler braucht Zugriff auf Testsysteme,
aber nicht automatisch auf Produktionsdaten.

Abrechnung braucht Kostenübersicht,
aber keine Server-Adminrechte.
```

Merksatz:

```
Rechte nach Aufgabe,
nicht nach Bequemlichkeit vergeben.
```

Administratorrechte

Administratorrechte sind besonders kritisch.

Risiken:

```
versehentliches Löschen
falsche Firewall-Regeln
öffentliche Freigaben
Zugriff auf sensible Daten
Rechteausweitung
Änderung von Logs
Manipulation von Backups
```

Merksatz:

```
Administratorrechte nur gezielt und kontrolliert vergeben.
```

Privileged Access Management

Privileged Access Management wird oft abgekürzt:

```
PAM
```

PAM bedeutet:

```
besonders privilegierte Zugriffe werden kontrolliert,
begrenzt
überwacht
und dokumentiert.
```

Beispiele:

```
zeitlich begrenzte Adminrechte
Genehmigungsprozess
MFA
Session Logging
Notfallkonto
regelmäßige Rechteprüfung
```

Merksatz:

```
PAM schützt besonders mächtige Zugriffe.
```

Just-in-Time-Zugriff

Just-in-Time-Zugriff bedeutet:

```
Rechte werden nur für einen begrenzten Zeitraum vergeben.
```

Beispiel:

```
Admin braucht für 2 Stunden erhöhte Rechte,
um eine Wartung durchzuführen.
```

Nach Ablauf werden die Rechte automatisch entzogen.

Merksatz:

```
Just-in-Time reduziert dauerhafte Adminrechte.
```

Sammelkonten vermeiden

Sammelkonten sind gemeinsame Konten, die mehrere Personen nutzen.

Problem:

```
keine eindeutige Zuordnung
schlechte Nachvollziehbarkeit
Passwortweitergabe
```

schwieriges Offboarding

Sicherheitsvorfälle schwer aufklärbar

Merksatz:

> Cloud-Zugriffe müssen personengebunden nachvollziehbar sein.

Servicekonto

Ein Servicekonto ist eine Identität für einen Dienst oder eine Anwendung.

Beispiele:

Backup-Dienst

Automatisierung

CI/CD-Pipeline

Monitoring

Anwendung, die auf Speicher zugreift

Skript, das Ressourcen erstellt

Servicekonten sollten ebenfalls nur minimale Rechte erhalten.

Merksatz:

> Servicekonten sind Maschinenidentitäten und brauchen genauso Rechtebegrenzung.

API-Schlüssel

API-Schlüssel erlauben Programmen oder Skripten Zugriff auf Cloud-Dienste.

Risiken:

Schlüssel wird versehentlich veröffentlicht

Schlüssel liegt im Quellcode

Schlüssel hat zu viele Rechte

Schlüssel wird nie rotiert

Schlüssel wird nach Projektende nicht gelöscht

Merksatz:

API-Schlüssel wie Passwörter behandeln.

Secrets

Secrets sind geheime Informationen.

Beispiele:

Passwörter
API-Schlüssel
private Schlüssel
Tokens
Datenbankzugangsdaten
Zertifikate

Secrets sollten nicht liegen in:

Quellcode
öffentlichen Repositories
Klartextdateien
Chatnachrichten
ungeschützten Wikiseiten
unverschlüsselten Backups

Merksatz:

Secrets gehören in geschützte Secret-Verwaltung.

Secret Management

Secret Management bedeutet:

geheime Informationen sicher speichern,
verteilen
rotieren
und widerrufen.

Wichtig:

Zugriff begrenzen
Nutzung protokollieren
Rotation ermöglichen
keine Klartextspeicherung
Notfallzugriff regeln
alte Secrets entfernen

Merksatz:

Secret Management verhindert unkontrollierten Umgang mit Zugangsdaten.

MFA in der Cloud

MFA steht für:

Multi-Faktor-Authentifizierung

MFA sollte besonders gelten für:

Administratoren
externe Benutzer
Zugriff auf sensible Daten
Zugriff auf Abrechnung
Zugriff auf IAM
Zugriff auf Produktion
Zugriff von unbekannten Geräten

Merksatz:

Cloud-Adminzugänge ohne MFA sind ein hohes Risiko.

Conditional Access

Conditional Access bedeutet:

Zugriff wird von Bedingungen abhängig gemacht.

Bedingungen können sein:

Benutzerrolle
Gerätetyp
Gerätezustand
Standort
Risiko des Logins
Anwendung
MFA erfüllt
Uhrzeit
Netzwerk

Beispiel:

Adminzugriff nur mit MFA und verwaltetem Gerät.

Merksatz:

Conditional Access prüft Kontext vor Zugriff.

Zero Trust in der Cloud

Zero Trust bedeutet:

keinem Zugriff automatisch vertrauen.

Auch innerhalb der Cloud wird geprüft:

Wer greift zu?
Von welchem Gerät?
Auf welche Ressource?
Mit welchem Risiko?
Mit welcher Rolle?
Ist MFA erfüllt?
Ist Zugriff ungewöhnlich?

Merksatz:

Zero Trust prüft jeden Zugriff kontextbezogen.

Rollenbasierte Zugriffskontrolle

Rollenbasierte Zugriffskontrolle wird oft abgekürzt:

RBAC

RBAC bedeutet:

Rechte werden über Rollen vergeben.

Beispiel:

Rolle Leser:
darf Ressourcen ansehen

Rolle Netzwerkadministrator:
darf Netzwerke verwalten

Rolle Besitzer:
darf fast alles verwalten

Merksatz:

RBAC macht Rechteverwaltung strukturierter.

Attributbasierte Zugriffskontrolle

Attributbasierte Zugriffskontrolle wird oft abgekürzt:

ABAC

ABAC entscheidet anhand von Attributen.

Beispiele für Attribute:

Abteilung
Projekt
Umgebung
Datenklasse
Standort
Gerätestatus
Tag
Uhrzeit

Merksatz:

ABAC nutzt Eigenschaften für Zugriffsentscheidungen.

RBAC und ABAC vergleichen

Merkmal	RBAC	ABAC
Grundlage	Rollen	Attribute
Beispiel	Admin, Leser, Entwickler	Projekt, Tag, Standort, Datenklasse
Vorteil	übersichtlich	sehr flexibel
Nachteil	Rollen können zu grob werden	komplexer zu planen
Einsatz	klassische Rechtevergabe	feinere Kontextregeln

Merksatz:

RBAC arbeitet mit Rollen.
ABAC arbeitet mit Eigenschaften.

Mandant und Tenant

Ein Tenant ist ein logisch getrennter Bereich in einer Cloud- oder SaaS-Plattform.

Er enthält typischerweise:

Benutzer
Gruppen
Rollen
Richtlinien

Anwendungen
Einstellungen
Ressourcen
Abrechnung

Merksatz:

Tenant = eigener Verwaltungsbereich in einer Cloud-Plattform.

Mandantentrennung

Mandantentrennung bedeutet:

Daten und Ressourcen verschiedener Kunden oder Organisationseinheiten werden logisch getrennt.

Wichtig bei:

Public Cloud
SaaS
Hosting
Multi-Tenant-Anwendungen
Dienstleisterplattformen

Merksatz:

Mandantentrennung verhindert Vermischung fremder Kundenbereiche.

Single Sign-On

Single Sign-On wird abgekürzt:

SSO

SSO bedeutet:

Benutzer melden sich einmal an
und können mehrere Dienste nutzen.

Vorteile:

```
weniger Passwörter
zentrale Anmeldung
bessere Kontrolle
einfacheres Offboarding
MFA zentral möglich
```

Merksatz:

```
SSO vereinfacht Anmeldung und zentrale Zugriffskontrolle.
```

Identity Provider

Identity Provider wird oft abgekürzt:

```
IdP
```

Ein Identity Provider stellt Identitäten und Anmeldungen bereit.

Er prüft zum Beispiel:

```
Benutzername
Passwort
MFA
Richtlinien
Gruppen
Rollen
```

Merksatz:

```
IdP ist die zentrale Stelle für Anmeldung.
```

Föderation

Föderation bedeutet:

Eine Organisation vertraut der Anmeldung einer anderen Identitätsquelle.

Beispiel:

Benutzer meldet sich mit Unternehmensidentität bei einem Cloud-Dienst an.

Der Cloud-Dienst muss das Passwort nicht selbst verwalten, sondern vertraut dem Identity Provider.

Merksatz:

Föderation verbindet Identitätswelten.

SAML

SAML steht für:

Security Assertion Markup Language

SAML wird häufig für Single Sign-On genutzt.

Grundidee:

Identity Provider bestätigt dem Dienst,
dass der Benutzer erfolgreich angemeldet ist.

Merksatz:

SAML ermöglicht SSO zwischen Identitätsanbieter und Dienst.

OAuth 2.0

OAuth 2.0 ist ein Autorisierungsstandard.

Er wird genutzt, damit Anwendungen Zugriff auf Ressourcen erhalten können, ohne direkt das Benutzerpasswort zu kennen.

Beispiel:

```
Eine Anwendung darf auf Kalenderdaten zugreifen,
nachdem der Benutzer zugestimmt hat.
```

Merksatz:

```
OAuth 2.0 regelt delegierte Autorisierung.
```

OpenID Connect

OpenID Connect baut auf OAuth 2.0 auf und ergänzt Authentifizierung.

Es wird häufig für moderne Logins genutzt.

Merksatz:

```
OpenID Connect ergänzt OAuth 2.0 um Identitätsinformationen.
```

Authentifizierung und Autorisierung in der Cloud

Authentifizierung:

```
Wer bist du?
```

Autorisierung:

```
Was darfst du?
```

Beispiele:

```
Benutzer meldet sich erfolgreich an.
Das ist Authentifizierung.

Benutzer darf eine VM löschen.
Das ist Autorisierung.
```

Merksatz:

Anmeldung und Berechtigung immer unterscheiden.

Cloud-Netzwerksicherheit

Cloud-Netzwerksicherheit umfasst:

VPC oder VNet
Subnetze
Security Groups
NSGs
Firewalls
private Endpunkte
VPN
Peering
Routing
DNS
WAF
DDoS-Schutz

Merksatz:

Cloud-Sicherheit besteht aus IAM und Netzwerkschutz.

Private Endpoint

Ein Private Endpoint macht einen Cloud-Dienst über eine private IP im eigenen Cloud-Netz erreichbar.

Vorteil:

Zugriff muss nicht über das öffentliche Internet erfolgen.

Beispiel:

Anwendung greift auf Cloud-Datenbank über private Adresse zu.

Merksatz:

Private Endpoint hält Cloud-Dienste intern erreichbar.

Public Endpoint

Ein Public Endpoint ist öffentlich über das Internet erreichbar.

Beispiele:

öffentliche API
Webanwendung
öffentliches SaaS-Portal
Storage-URL mit öffentlichem Zugriff

Wichtig:

Public Endpoints brauchen starke Zugriffskontrolle,
TLS,
Logging
und Schutzregeln.

Merksatz:

Public Endpoint nur bewusst und abgesichert nutzen.

WAF

WAF steht für:

Web Application Firewall

Eine WAF schützt Webanwendungen vor typischen Angriffen.

Beispiele:

SQL Injection
Cross-Site Scripting
bösartige Requests

ungewöhnliche Muster
bekannte Angriffssignaturen

Merksatz:

WAF schützt Webanwendungen auf Anwendungsebene.

DDoS-Schutz

DDoS steht für:

Distributed Denial of Service

Dabei versuchen viele Systeme, einen Dienst durch massenhafte Anfragen zu überlasten.

Cloud-Anbieter bieten oft Schutzfunktionen gegen DDoS-Angriffe.

Merksatz:

DDoS-Schutz soll Dienste trotz Massenangriffen verfügbar halten.

Verschlüsselung in der Cloud

Verschlüsselung ist wichtig für:

Daten bei Übertragung
Daten im Ruhezustand
Backups
Datenbanken
Speicher
Logs
Schlüsselverwaltung

Merksatz:

Verschlüsselung schützt Daten,
ersetzt aber keine Rechteverwaltung.

Verschlüsselung während der Übertragung

Daten während der Übertragung sollten verschlüsselt werden.

Typische Technik:

```
TLS
```

Beispiele:

```
HTTPS
API-Aufrufe
Datenbankverbindungen
Verwaltungsschnittstellen
SaaS-Zugriffe
```

Merksatz:

```
Daten unterwegs mit TLS schützen.
```

Verschlüsselung im Ruhezustand

Daten im Ruhezustand sind gespeicherte Daten.

Beispiele:

```
Datenbankdaten
Dateien im Storage
Backups
Snapshots
Logs
virtuelle Festplatten
```

Diese Daten sollten verschlüsselt gespeichert werden.

Merksatz:

```
Gespeicherte Daten ebenfalls verschlüsseln.
```

Schlüsselverwaltung

Verschlüsselung braucht Schlüssel.

Wichtige Fragen:

```
Wer erstellt Schlüssel?
Wer verwaltet Schlüssel?
Wer darf Schlüssel nutzen?
Werden Schlüssel rotiert?
Wo werden Schlüssel gespeichert?
Was passiert bei Schlüsselverlust?
Wer kann Daten entschlüsseln?
```

Merksatz:

```
Verschlüsselung ist nur so sicher wie die Schlüsselverwaltung.
```

KMS

KMS steht für:

```
Key Management Service
```

Ein KMS verwaltet kryptografische Schlüssel.

Aufgaben:

```
Schlüssel erzeugen
Schlüssel speichern
Schlüssel rotieren
Zugriff auf Schlüssel steuern
Nutzung protokollieren
Schlüssel deaktivieren oder löschen
```

Merksatz:

```
KMS verwaltet Schlüssel für Cloud-Verschlüsselung.
```

Kundenverwaltete Schlüssel

Bei kundenverwalteten Schlüsseln kontrolliert der Kunde stärker, welche Schlüssel für Verschlüsselung genutzt werden.

Vorteile:

```
mehr Kontrolle
eigene Richtlinien
Schlüsselrotation steuerbar
Zugriff besser begrenzbar
```

Risiko:

```
Schlüsselverlust kann Daten unbrauchbar machen.
```

Merksatz:

```
Mehr Schlüsselhoheit bedeutet auch mehr Verantwortung.
```

Cloud-Logging

Cloud-Logging ist sicherheitskritisch.

Wichtige Logarten:

```
Anmeldungen
API-Aufrufe
Rechteänderungen
Netzwerkzugriffe
Firewall-Entscheidungen
Datenzugriffe
Adminaktionen
Fehlermeldungen
Sicherheitsereignisse
Kostenereignisse
```

Merksatz:

```
Cloud-Logs zeigen,
wer was wann getan hat.
```

Audit-Logs

Audit-Logs dokumentieren administrative und sicherheitsrelevante Aktionen.

Beispiele:

```
Benutzer erstellt
Rolle geändert
Firewall geöffnet
VM gelöscht
Speicher öffentlich gemacht
API-Schlüssel erstellt
MFA deaktiviert
Backup gelöscht
```

Merksatz:

```
Audit-Logs sind wichtig für Nachvollziehbarkeit.
```

Cloud-Monitoring

Cloud-Monitoring überwacht Betrieb und Sicherheit.

Wichtige Werte:

```
Verfügbarkeit
CPU
RAM
Speicher
Datenbanklast
Netzwerkverkehr
Loginfehler
ungewöhnliche Zugriffe
Kosten
Zertifikatsablauf
```

Backupstatus

Merksatz:

Monitoring erkennt technische und sicherheitsrelevante Probleme.

SIEM

SIEM steht für:

Security Information and Event Management

Ein SIEM sammelt und analysiert Sicherheitslogs aus verschiedenen Quellen.

Ziel:

Angriffe erkennen
Auffälligkeiten korrelieren
Alarmierungen erzeugen
Sicherheitsvorfälle untersuchen
Nachweise bereitstellen

Merksatz:

SIEM hilft,
Sicherheitsereignisse zentral auszuwerten.

Cloud-Backup

Auch Cloud-Dienste brauchen Backup.

Wichtige Fragen:

Welche Daten werden gesichert?
Wie oft?
Wie lange?
Wo werden Backups gespeichert?
Wer darf wiederherstellen?

Sind Backups verschlüsselt?
Sind Backups vor Löschung geschützt?
Wurde Wiederherstellung getestet?

Merksatz:

Cloud ist kein Ersatz für Backup.

Ransomware-Schutz in der Cloud

Auch Cloud-Daten können durch Ransomware betroffen sein.

Risiken:

synchronisierte verschlüsselte Dateien
gelöschte Backups
kompromittierte Adminzugänge
manipulierte Datenbanken
missbrauchte API-Schlüssel

Schutz:

MFA
getrennte Adminrollen
unveränderliche Backups
Versionierung
Least Privilege
Monitoring
schnelles Offboarding

Merksatz:

Ransomware-Schutz braucht Backup,
Rechtebegrenzung
und Monitoring.

Immutable Backup

Immutable bedeutet:

```
unveränderlich
```

Ein Immutable Backup kann für einen festgelegten Zeitraum nicht verändert oder gelöscht werden.

Vorteil:

```
Schutz vor versehentlicher Löschung
Schutz vor Ransomware
bessere Wiederherstellungschancen
```

Merksatz:

```
Unveränderliche Backups schützen vor Manipulation und Löschung.
```

Datenschutz in der Cloud

Cloud-Datenschutz fragt:

```
Welche Daten werden verarbeitet?
Wo werden Daten gespeichert?
Wer hat Zugriff?
Gibt es Auftragsverarbeitung?
Sind Daten verschlüsselt?
Gibt es Löschkonzepte?
Wie werden Betroffenenrechte erfüllt?
Werden Logs personenbezogen?
Welche Unterauftragnehmer gibt es?
```

Merksatz:

```
Cloud-Dienste brauchen Datenschutzprüfung.
```

Datenklassifizierung

Datenklassifizierung bedeutet:

Daten werden nach Schutzbedarf eingeteilt.

Beispiele:

öffentlich
intern
vertraulich
streng vertraulich
personenbezogen
geschäftskritisch

Je höher der Schutzbedarf, desto strenger müssen Zugriff, Verschlüsselung, Logging und Speicherort geregelt sein.

Merksatz:

Schutzmaßnahmen richten sich nach Datenklasse.

Compliance in der Cloud

Compliance bedeutet:

Einhaltung von Regeln,
Gesetzen,
Standards
und internen Vorgaben.

Cloud-relevant:

Datenschutz
Informationssicherheit
Aufbewahrung
Löschung
Auditierbarkeit
Zugriffskontrolle
Datenstandort
Vertragsprüfung
Branchenvorgaben

Merksatz:

```
Cloud muss zu rechtlichen und organisatorischen Vorgaben passen.
```

Cloud-Sicherheitsrichtlinie

Eine Cloud-Sicherheitsrichtlinie sollte festlegen:

```
erlaubte Dienste
erlaubte Regionen
Rollenmodell
MFA-Pflicht
Logging-Pflicht
Verschlüsselung
Backup-Vorgaben
Tagging
Kostenkontrolle
Freigabeprozesse
Umgang mit externen Benutzern
Lösch- und Aufbewahrungsregeln
```

Merksatz:

```
Cloud-Sicherheit braucht klare Regeln.
```

Cloud-Governance

Cloud Governance bedeutet:

```
Steuerung und Kontrolle der Cloud-Nutzung.
```

Ziele:

```
Sicherheit
Kostenkontrolle
Compliance
Standardisierung
```

klare Verantwortlichkeiten
Vermeidung von Schatten-IT
Nachvollziehbarkeit
Ordnung in Ressourcen

Merksatz:

Governance sorgt dafür,
dass Cloud kontrolliert genutzt wird.

Typische Cloud-Sicherheitsfehler

Häufige Fehler:

MFA nicht aktiviert
Adminrechte zu breit
öffentliche Speicherfreigaben
Datenbank öffentlich erreichbar
Security Group erlaubt 0.0.0.0/0 auf Adminport
API-Schlüssel im Quellcode
Servicekonto mit Vollzugriff
Logs deaktiviert
Backups nicht getestet
alte Benutzerkonten aktiv
keine Kostenalarme
kein Offboarding
falsche Region
keine Verschlüsselung
keine Rechteprüfung

Merksatz:

Cloud-Sicherheitsfehler sind oft Konfigurationsfehler.

Checkliste: Cloud-IAM sicher gestalten

MFA für Admins erzwingen.
Keine Sammelkonten nutzen.
Benutzer eindeutig zuordnen.
Gruppen und Rollen verwenden.
Least Privilege umsetzen.
Adminrechte zeitlich begrenzen.
Servicekonten minimal berechtigen.
API-Schlüssel schützen.
Secrets nicht im Quellcode speichern.
Regelmäßige Rechteprüfung durchführen.
Offboarding konsequent umsetzen.
Audit-Logs aktivieren.

Merksatz:

IAM ist die wichtigste Sicherheitsbasis in der Cloud.

Checkliste: Cloud-Ressourcen sicher konfigurieren

Öffentliche Erreichbarkeit prüfen.
Managementports nicht öffentlich öffnen.
Datenbanken privat bereitstellen.
Security Groups eng setzen.
Verschlüsselung aktivieren.
Backups einrichten.
Logs aktivieren.
Monitoring einrichten.
Tags setzen.
Kostenalarme setzen.
Region bewusst auswählen.
Änderungen dokumentieren.

Merksatz:

Cloud-Ressourcen sicher konfigurieren,
bevor sie produktiv genutzt werden.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was bedeutet Shared Responsibility Model?
- Was ist IAM?
- Warum ist IAM in der Cloud wichtig?
- Was ist der Unterschied zwischen Authentifizierung und Autorisierung?
- Was bedeutet Least Privilege?
- Was ist RBAC?
- Was ist ABAC?
- Was ist ein Tenant?
- Was ist Mandantentrennung?
- Warum sollte MFA für Cloud-Admins Pflicht sein?
- Warum sind API-Schlüssel kritisch?
- Was ist Secret Management?
- Was ist ein Private Endpoint?
- Was ist eine WAF?
- Was ist ein KMS?
- Warum ersetzt Verschlüsselung keine Rechteverwaltung?
- Warum braucht Cloud Logging und Monitoring?
- Warum ist Cloud kein Ersatz für Backup?
- Was ist ein Immutable Backup?
- Warum ist Datenklassifizierung wichtig?

Typische Prüfungsfallen

Cloud-Sicherheit ist gemeinsame Verantwortung.

Anbieter ist nicht automatisch für Kundendatenrechte verantwortlich.

Daten,
Benutzer
und Rechte bleiben fast immer Kundenthema.

IAM ist zentral für Cloud-Sicherheit.

Authentifizierung ist nicht Autorisierung.

MFA für Admins ist besonders wichtig.

Adminrechte nicht dauerhaft und breit vergeben.

Servicekonten sind ebenfalls Identitäten.

API-Schlüssel wie Passwörter behandeln.

Secrets nicht im Quellcode speichern.

RBAC arbeitet mit Rollen.

ABAC arbeitet mit Attributen.

Tenant ist ein Verwaltungsbereich.

Mandantentrennung schützt Kundenbereiche.

SSO vereinfacht zentrale Anmeldung.

OAuth 2.0 ist Autorisierung.

OpenID Connect ergänzt Authentifizierung.

Private Endpoint vermeidet öffentlichen Zugriff.

Public Endpoint braucht besonderen Schutz.

WAF schützt Webanwendungen.

Verschlüsselung ersetzt keine Zugriffsrechte.

KMS verwaltet Schlüssel.

Cloud-Logs müssen aktiv sein.

Backup muss auch in der Cloud geplant werden.

Immutable Backup schützt vor Löschung und Manipulation.

Datenschutz und Compliance müssen geprüft werden.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Shared Responsibility	geteilte Verantwortung zwischen Anbieter und Kunde
IAM	Identity and Access Management
Identität	Konto oder Dienst mit Zugriff
Benutzer	menschliche Identität
Gruppe	Zusammenfassung von Benutzern
Rolle	Aufgabenbezogene Rechte
Berechtigung	konkrete Erlaubnis
Richtlinie	Regel für Zugriff
Least Privilege	minimale notwendige Rechte
Need to Know	Zugriff nur bei Bedarf
PAM	Kontrolle privilegierter Zugriffe
Just-in-Time	zeitlich begrenzte Rechte
Servicekonto	Identität für Dienst oder Anwendung
API-Schlüssel	Zugriffsschlüssel für Programme
Secret	geheime Information
Secret Management	Verwaltung geheimer Informationen
MFA	Multi-Faktor-Authentifizierung
Conditional Access	Zugriff abhängig von Bedingungen
Zero Trust	kein automatisches Vertrauen
RBAC	rollenbasierte Zugriffskontrolle
ABAC	attributbasierte Zugriffskontrolle
Tenant	logisch getrennter Verwaltungsbereich
Mandantentrennung	Trennung verschiedener Kundenbereiche
SSO	Single Sign-On
IdP	Identity Provider
Föderation	Vertrauen zwischen Identitätsquellen
SAML	SSO-Standard
OAuth 2.0	delegierte Autorisierung

Begriff	Kurze Erklärung
OpenID Connect	Authentifizierung auf Basis von OAuth 2.0
Private Endpoint	privater Zugriff auf Cloud-Dienst
Public Endpoint	öffentlicher Zugriffspunkt
WAF	Web Application Firewall
DDoS	Überlastungsangriff
KMS	Key Management Service
Audit-Log	Nachweis sicherheitsrelevanter Aktionen
SIEM	zentrale Sicherheitslog-Auswertung
Immutable Backup	unveränderliches Backup
Datenklassifizierung	Einteilung nach Schutzbedarf
Compliance	Einhaltung von Vorgaben
Cloud Governance	Steuerung der Cloud-Nutzung

IHK-sichere Kurzformulierung

Cloud-Sicherheit basiert auf dem Shared Responsibility Model. Der Anbieter schützt je nach Service-Modell die Plattform, Infrastruktur und den Dienstbetrieb, während der Kunde für Benutzer, Rollen, Berechtigungen, Daten, sichere Konfiguration, Zugriffsschutz, Backup, Logging, Monitoring und Compliance verantwortlich bleibt. IAM, also Identity and Access Management, ist ein zentraler Bestandteil der Cloud-Sicherheit, da es regelt, wer welche Ressourcen nutzen oder verändern darf. Wichtige Prinzipien sind MFA, Least Privilege, rollenbasierte Rechtevergabe, sichere Servicekonten, Schutz von API-Schlüsseln, Secret Management, Logging, Verschlüsselung und regelmäßige Rechteprüfung. Cloud-Sicherheit entsteht durch Technik, Prozesse und klare Verantwortlichkeiten.

Merksätze

Cloud-Sicherheit ist gemeinsame Verantwortung.

Anbieter schützt Plattform,
Kunde schützt Nutzung und Daten.

Daten,
Benutzer
und Rechte bleiben fast immer Kundenthema.

IAM entscheidet,
wer was darf.

Nicht nur Menschen haben Identitäten.

Servicekonten brauchen minimale Rechte.

API-Schlüssel wie Passwörter behandeln.

Secrets nicht im Quellcode speichern.

MFA für Admins erzwingen.

Authentifizierung = Wer bist du?

Autorisierung = Was darfst du?

Least Privilege gilt immer.

Adminrechte zeitlich und fachlich begrenzen.

Sammelkonten vermeiden.

RBAC nutzt Rollen.

ABAC nutzt Attribute.

Tenant ist ein Cloud-Verwaltungsbereich.

SSO vereinfacht zentrale Anmeldung.

IdP prüft Identitäten.

OAuth 2.0 ist Autorisierung.

OpenID Connect ergänzt Authentifizierung.

Private Endpoint hält Zugriff intern.

Public Endpoint besonders schützen.

WAF schützt Webanwendungen.

DDoS-Schutz schützt Verfügbarkeit.

Verschlüsselung ersetzt keine Rechte.

KMS verwaltet Schlüssel.

Audit-Logs zeigen Adminaktionen.

SIEM wertet Sicherheitsereignisse zentral aus.

Cloud ist kein Ersatz für Backup.

Immutable Backup schützt vor Manipulation.

Datenklassifizierung bestimmt Schutzbedarf.

Cloud Governance schafft Regeln.

Fehlkonfiguration ist eines der größten Cloud-Risiken.